

Image Authentication and Rightful Ownership Watermarking Method for the Cloud Environment

REZA KHALEGHPARAST

BCS, MSc (Hons)

A thesis submitted to Auckland University of Technology

in fulfillment of the requirements for the degree of

Doctor of Philosophy (PhD)

2017

School of Engineering, Computer and Mathematical Sciences

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Reza Khaleghparast

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies of the AUT University in the New Zealand. Throughout the research duration the researcher received valuable support from many people who in one way or another, contributed immensely to the success of the research. It is with utmost pleasure and gratefulness the researcher would like to take this opportunity to thank all those people for their support, inspiration and motivation, which without, it would not have been possible to complete the research.

First and foremost the researcher wishes to thank the primary supervisor Dr. Brian Cusack for his constant non-stop support, motivation and advice throughout the whole research from day 1 to the end of this research. The contribution of Dr. Cusack will be a very long-term asset in shaping the researcher and in assisting him to attain a higher academic level and professional work style. In addition, the research would like to thank Prof. Ajit Narayanan, the secondary supervisor, for his support and reviewing the research outcomes and providing a valuable feedback that helped immensely in improving the research deliverables. Secondly, the researcher would like to thank the people who used, tested and evaluated the models designed in the research. Thirdly, would like to thank family members who patiently helped and motivated the researcher throughout the research and without their help and support, this journey would not be possible.

The assistance of AUT administrators, in particular the Computing department administrators. AUT Postgraduate office is also acknowledged with gratitude. Various other people have helped the researcher in many ways to accomplish required tasks, including but not limited to staff at IT service and library, these are all acknowledged with appreciation.

Publications

Khaleghparast, R., & Cusack, B. (2015). Using Design Science to Build a Watermark System for Cloud Rightful Ownership Protection. *Proceedings of Australian Conference on Information Systems (ACIS)*.

Khaleghparast, R., & Cusack, (2014). Securing identity information with image watermarks. *Proceedings of 12th Australian Information Security Management Conference*.

Khaleghparast, R., & Cusack, (2016). A privacy gap around the internet of things for open-source projects. In Johnstone, M. (Ed.). *The Proceedings of 14th Australian Information Security Management Conference* on (pp. 14-20).

Ghazizadeh, E., Shams Dolatabadi, Z., Khaleghparast, R., Zamani, M., Manaf, A. A., & Abdullah, M. S. (2014). Secure OpenID authentication model by using trusted computing *Hindawi Publishing Corporation*. Symposium conducted at the IEEE meeting of the Abstract and Applied Analysis

Moghaddam, F. F., Varnosfaderani, S. D., Mobedi, S., Ghavam, I., & Khaleghparast, R. (2014, April). GD2SA: Geo detection and digital signature authorization for secure accessing to cloud computing environments. In *Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on* (pp. 39-42). IEEE.

Abstract

Cloud computing has evolved in the last five years from being an abstract idea and proposal, and into services that people use every day. In particular services that relate to mobile phone technologies have expanded in proportion to the number of users, so that for example the use of cloud drop boxes for photos, videos, and audio recordings is done on a daily basis. In the bigger picture businesses have found it economical to exploit the new opportunities and to migrate much of their previous business computing capability and storage facilities into the cloud.

With opportunity there always comes the positive and negative aspects of risk. With cloud computing the economic advantages and the ease of access have outweighed the risk of unplanned information disclosure. Cloud computing spans a multitude of technologies, is multi-layered, and crosses the boundaries of different legal jurisdictions. As a consequence it is possible for an end user to commit their information and/or the information processing into cloud services with a trusted supplier. However, the cloud service supplier interacts with many other service suppliers who may not share the same legal compliance or understanding of the service level agreements. The complication of service agreements also extends to the ability of anyone service level agreement to adequately protect digital property rights.

In this thesis the problem of rightful ownership is raised and research questions developed to explore the potential positive and negative risks around property ownership in the cloud. The three research questions are asked:

- What preparation methods improve ownership protection in cloud environments?
- What could be a suitable management framework to increase ownership protection in a cloud environment?
- What tests show the reliability of a proposed method in a cloud environment?

The literature analysis identified both watermarking and watermarking technologies as being relevant to the key issue of privacy protection. Consequently the researcher chose to build a watermarking application and to introduce unique security features and implementation schema as a working solution to the problem.

A design science approach is adopted as being relevant to an exploratory investigation and the development of software artefacts that are open to revision and continuous improvement. The researcher builds a watermarking software artefact (see Appendix B for the code, and chapter 4 for the demonstration) and submits to industry experts for naturalistic feedback. Comprehensive statistical analysis is also performed on the artefact to know and to understand the value of the implementation. It was found that this particular solution to the rightful ownership problem is a working solution that can be further developed in theory and in practice. The significant innovation proposed in this thesis is that the service supplier takes responsibility for watermarking all objects submitted to the cloud in the interests of standardisation, performance, and security of information in the cloud.

The nature and approach of this research has been to address the theoretical problem by reasoning and then to deliver a solution by demonstrating a relevant software artefact. The software artefact for watermarking has performed well and passed naturalistic scrutiny but it requires further development and maturity before it can be generalised across the Cloud services industry. The suggestions for further research arising from this thesis are:

- examination of watermarking potential for all information submitted to the cloud
- further research and intellectual property protection in the Cloud
- further exploration of industry sector specific requirements for watermarking
- the development of policies and law that applies to ownership issues in the cloud
- standardisation procedures for all cloud service suppliers
- the availability of watermarking tools on every cloud service suppliers site

Table of Contents

Declaration	i
Acknowledgements	ii
Publications	iii
Abstract	iv
Table of Contents	vi
List of Figures	xi
List of Tables	xiii
List of Abbreviations	xiv

Chapter One - Introduction

1.0 INTRODUCTION	1
1.1 MOTIVATION	2
1.2 RESEARCH METHODOLOGY	4
1.3 FINDINGS	5
1.4 RESEARCH ORGANISATION	6
1.5 CONCLUSION	8

Chapter Two - Literature Review

2.0 INTRODUCTION	9
2.1 BACKGROUND	9
2.2 RESEARCH METHOD FOR LITERATURE SELECTION	11
2.3 REVIEW METHOD	13
2.4 CLASSIFYING AND USING A MODEL FOR PRIVACY REQUIREMENTS	14
2.4.1 Data Integrity	15
2.4.2 Data Segregation	16
2.4.3 Data Availability	16
2.4.4 Network Availability	16
2.4.5 Backup Strategy	17
2.4.6 Provider's Transparency	17

2.4.7 Organisational Policies	17
2.4.8 Legal Compliance.....	18
2.4.9 Data Protection	18
2.5 QUALITY APPRAISAL	19
2.6 RESPONSE TO THE GAP	25
2.6.1 Watermarking	25
2.6.2 Spatial Domain and Frequency Domain.....	30
2.6.3 Image Watermarking	30
2.6.3.1 Robust, Fragile and Semi-fragile Image Watermarking.....	30
2.6.3.2 Requirements for Digital Image Watermarking	31
Imperceptibility	32
Robustness.....	32
Capacity	33
Security.....	33
2.6.4 Processing methods in frequency domain	34
2.6.4.1 Singular Value Decomposition.....	34
2.6.4.2 Distributed Discrete Wavelet Transformation.....	34
2.6.5 Attacks on watermarking.....	35
2.6.5.1 Watermarking attacks classification	36
2.6.5.2 Benchmarking.....	37
Stirmark	37
Certification for watermarking techniques.....	38
Checkmark.....	38
Optimark.....	39
2.7 CLOUD WATERMARKING	40
2.7.1 Virtualisation in cloud	40
2.8 SUMMARY	41

Chapter Three - Research Methodology

3.0 INTRODUCTION	42
3.1 PROBLEM REVIEW	43
The Research Questions	45
The Hypotheses	46
3.2 RESEARCH METHODOLOGY	46
3.3 RESEARCH DESIGN	49

3.3.1	Research Design Steps	50
3.4	DESIGN EVALUATION REQUIREMENTS	52
3.4.1	Data Collection Methods	53
3.4.2.1	Find appropriate methods for watermarking to use in cloud environment (Phase1).....	56
3.4.2.2	Implement the artefact in a virtualized environment as a cloud (Phase2)	58
3.4.2.3	Implementation Diagram	59
3.4.2.4	Analysing and testing different performance characteristics of the watermark method in the virtualized cloud (Phase3).....	61
3.5	RESEARCH METHODOLOGY LIMITATIONS	64
3.5.1	Reliability	64
3.5.2	Validity	66
3.5.3	Generalisation.....	67
3.6	FORECASTED RESEARCH OUTCOMES	68
3.7	CONCLUSION	69
 Chapter Four - Artefact Design and Implementation		
4.0	INTRODUCTION	70
4.1	ARTEFACT DESIGN	71
4.2	PROCESSES FOR IMPLEMENTING ARTEFACT DESIGN	74
4.2.1	Embedding Algorithm	74
4.2.2	Feature Extraction Process	76
4.2.2.1	Sample Acquisition	76
4.2.2.2	Fix Password Acquisition	76
4.2.2.3	DYN Password Request.....	77
4.2.2.4	Hash Extraction.....	77
4.2.3	Image Authentication Process	77
4.2.3.1	Watermark Existence Check (WECH)	77
4.2.3.2	Image Similarity Checking	79
4.2.3.3	Watermark Embedding Process	81
4.3	ARTEFACT DEVELOPMENT (RIGHTFUL OWNERSHIP DETECTION SYSTEM DEVELOPMENT)	82

4.3.1 Login	83
4.3.2 Upload Image	84
4.3.3 WECH Process	87
4.3.4 ISCH Process.....	89
4.3.5 Watermarking Process.....	90
4.4 SUMMARY	95

Chapter Five - Artefact Evaluation and Analysis

5.0 INTRODUCTION.....	96
5.1 NATURALISTIC EXPERT EVALUATION.....	97
5.1.1 Fieldwork Activities	97
5.1.2 Evaluation Preparation Activities.....	98
5.1.3 Experts' Evaluation.....	99
5.1.3.1 Expert1	99
5.1.3.2 Expert2	101
5.1.3.3 Expert 3	102
5.1.4 Critical Reflection on Experts' Evaluation Results	104
5.1.4.1 Suggested Changes	107
5.2 ARTEFACT STATISTICAL EVALUATION	108
5.2.1 Cover Images	108
5.2.2 Experimental Results for Watermark Existence Check.....	110
5.2.3 Experimental Results for Hash Existence Checking	111
5.2.4 Experimental Results for Image Authentication	113
5.2.4.1 Quality Test on ISCH	114
5.2.5 All Tested images Differentiation Recognition	128
5.2.6 ISCH output results.....	131
5.3 Experimental Results for the Watermarking phase	136
5.3 SUMMARY	140

Chapter Six - Research Contribution

6.0 INTRODUCTION.....	141
6.1 HYPOTHESIS EVALUATION.....	141
6.2 ANSWER TO THE RESEARCH QUESTION	145
6.2.1 Question 1	145
6.2.2 Question 2	146
6.2.3 Question 3	146

6.3	DISCUSSION OF FINDINGS	147
6.4	RESEARCH CONTRIBUTION	149
6.4.1	Contribution to Theory	150
6.4.2	Contribution to Practice	151
6.5	CONCLUSION	153

Chapter Seven - Conclusion

7.0	INTRODUCTION	154
7.1	THE RESEARCH JOURNEY	154
7.1.1	Initiation.....	155
7.1.2	Challenges.....	155
7.1.3	Methodology	156
7.1.4	Discovery and Innovation	157
7.1.5	Where to from Here	157
7.2	LIMITATION.....	157
7.3	FUTURE WORK	159
	REFERENCES	160
	APPENDIX A	167
	APPENDIX B.....	168

List of Figures

Figure 2.1: Systematic Review Steps.....	12
Figure 2.2: Cloud Privacy Issues Considered in this Research	15
Figure 2.3: A typical watermark embedding process	27
Figure 2.4: A typical blind watermark detection	27
Figure 2.5: Watermarking Scenario	29
Figure 2.6: Schematic diagram for robust watermarking.....	32
Figure 2.7: Trade-off among the imperceptibility, robustness and capacity.....	33
Figure 2.8: 3-scale DDWT transform.....	35
Figure 3.1: Cloud Computing Services	43
Figure 3.2: Cloud Service Architecture	44
Figure 3.3: DS research methodology	47
Figure 3.4: Research Stages	49
Figure 3.5: Research design	51
Figure 3.6: Modified design Science methodology diagram displaying process for each phase of this research	52
Figure 3.7: Some of the watermarking methods related to the research	56
Figure 3.8: Illustration of the cloud environment focused on the research goal...	58
Figure 3.9: Implementation Diagram	60
Figure 3.10: CIA Triad	61
Figure 3.11: Proposed Artefact Architecture	63
Figure 4.1: Proposed Artefact explained....	73
Figure 4.2: Preparation Flowchart.....	75
Figure 4.3: Watermark extraction process	78
Figure 4.4: Watermark embedding process	81
Figure 4.5: Amazon Web Services Console	82
Figure 4.6: User registration form	83
Figure 4.7: Login window	84
Figure 4.8: Successful transaction of uploading the image	85
Figure 4.9: DYN sample code	86
Figure 4.10: Notification of successful features sending	87
Figure 4.11: Notification of user clearance to continue to next step	88

Figure 4.12: Image existence notification in hash existence check system	89
Figure 4.13: Image Similarity Check (ISCH)	90
Figure 4.14: Watermarking with extracted features	91
Figure 4.15: Bit stream code built for watermarking purpose	92
Figure 4.16: Embedding process	92
Figure 4.17: Notification of successful watermarking	93
Figure 4.18: Embedding algorithm.....	94
Figure 5.1: Standard-watermarking images	109
Figure 5.2: Message extraction	110
Figure 5.3: Cloud database capture of table "Full" which shows the stored output of SHA256.....	111
Figure 5.4: Result of Hash Check if the hash exists	112
Figure 5.5: Result of Hash Check if the hash could not be found	113
Figure 5.6: Lena ISCH results	115
Figure 5.7: Cameraman ISCH results	117
Figure 5.8: House ISCH results	118
Figure 5.9: Jet Plane ISCH results	120
Figure 5.10: Lake ISCH results.....	121
Figure 5.11: Living Room ISCH results	123
Figure 5.12: Mandrill ISCH results	124
Figure 5.13: Pepper ISCH results	125
Figure 5.14: Pirate ISCH results	126
Figure 5.15: Walking bridge ISCH results	128
Figure 5.16: ISCH test results for each manipulation	130
Figure 5.17: Camera Man under format changing manipulation	131
Figure 5.18: Resize manipulation results of ISCH	134
Figure 5.19: Text manipulation results of ISCH	135
Figure 5.20: Format changing manipulation results of ISCH	136
Figure 5.21: output result of the PSNR quality test of embedding the CFDH in tested images	138

List of Tables

Table 2.1: Key data risks in the cloud	19
Table 2.2: Literature analysis of related studies	21
Table 2.3: Watermarking attacks classification	36
Table 3.1: Expert Evaluation Criteria	54
Table 4.1: Similarity Process between uploaded image and existence image Pseudo Code	80
Table 4.2: Extracting the embedded message Pseudo Code	88
Table 5.1: Artefact list provided for experts evaluation	98
Table 5.2: Expert 1 respond to the questions asked	100
Table 5.3: Expert 2 respond to the questions asked	101
Table 5.4: Expert 3 respond to the questions asked.....	103
Table 5.5: Critical Reflection on Expert Evaluation Results	105
Table 5.6: Result of comparison between tested images in ISCH system	132
Table 5.7: PSNR result of embedded images with CFDH	137
Table 5.8: PSNR Calculation Pseudo code	138
Table 6.1: Hypothesis Evaluation	142

List of Abbreviations

API	Application Programming Interface
AWS	Amazon Web Services
CFDH	Cloud Fixpass, DynamicPass, Hash
CSP	Cloud Service Provider
CU	Cloud User
DS	Design Science
DSRM	Design Science Research Methodology
DSR	Design Science Roadmap
DWT	Discrete Wavelet Transformation
DYN	Dynamic
DRM	Digital Right Management
HECH	Hash Existence Check
IaaS	Infrastructure as a Service
IS	Information System
ISCH	Image Similarity Check
NIST	National Institute of Standards and Technology
PSNR	Peak Signal-to-Noise Ratio
PaaS	Platform as a Service
RDS	Relational Database Service
RODS	Rightful Ownership Detection System
RQ	Research Question
SLA	Service Level Agreement
SaaS	Software as a Service

SR	Systematic Review
SVD	Singular Value Decomposition
WECH	Watermark Existence Check

Chapter 1

Introduction

1.0 INTRODUCTION

With the dramatic development and reach of technology, a global village of users has been created. This place is in the hands of many and diverse people who have new opportunities services at affordable and accessible rates. The introduction of Cloud computing in the last few years is one of the opportunities that has made computing and storage processes available without the requirement own expensive equipment and support personnel. It is economical, accessible and flexible for use; and presents a great opportunity to many people to increase their computing and information management capability. However, the risk analysis for the user identifies vulnerabilities. In particular for intellectual property ownership and vulnerabilities for the identification of rightful property owners when cloud services are used (Liu *et al.*, 2011b; Yuhan and En-hui, 2009).

One of the important issues of cloud computing is user loss of control. The system architecture for services posits multiple layers of inter-related services for which no one supplier has control (Tek, et al., 2010, p.684). In the first instance a user interacts with a sales agent (human or machine) to purchase the services opportunity. The sales agent may be selling on behalf of one or more service suppliers. In turn these suppliers have supply agreements with many sub-service suppliers or brokers. Sub-service suppliers also have inter-related arrangements for services that may migrate data and service without notice (Lombardi and Di Pietro, 2011). The net result is that a cloud service user may not know the storage and processing place or places of the data and may not be assured of ownership protection. Hence, the consequences are for security, privacy and legally enforceable agreements.

The essence of cloud computing is that a user entrusts their own digital information to a second party who exploits multiple third parties to deliver the user a service. The user has technology and information, which are hosted in the cloud by the provider, and the services to store information, to create further

information, and to transact business are made available by the provider. Inevitably, the protection of ownership rights can be problematic and the many related vulnerabilities require risk treatment in a secure service system (O'Ruanaidh, 1996; Cayre, 2005).

The aim of this research is to design and develop an artefact to improve the rightful ownership protection in the cloud environment. To achieve this goal, the research will look for possible solutions by raising questions, trying answers, building artefacts, testing artefacts, and soliciting expert feedback. Chapter 1 introduces the research aspects in the following sections: section 1.1 explores the motivation and the problem focus of the research; section 1.2 identifies the research methodology; while section 1.3 introduces the research findings. In section 1.4 the theses organisation is presented, and concluded in section 1.5.

1.1 MOTIVATION

The researcher finished an MSc in information security with first class honours in Malaysia before taking on this doctor of philosophy degree. Towards the end of that time the cloud computing innovation started to become a major study area in computer science and the researcher was reading the various commercial and academic publications in the area. Some of the glaring contradictions regarding security and open systems that have been in computer science for decades became very obvious. The development of cloud computing was all about giving people economical access to resources. There was very little or no consideration of matters such as protecting the integrity of the content beyond simple technical matters that could not address concerns such as privacy and ownership.

The most serious concerns the researcher read regarded privacy issues. In the cloud environment there seemed to be little concern about protecting the ownership of intellectual property when the major thrust in cloud computing was to provide a ubiquitous system that was distributed without consideration of jurisdictions or security, law and controls. This to me, was a big problem. For example with copyright protection there seemed to be little concern beyond what the end user could contribute to their artefacts before everything gets uploaded into the different cloud environments. For businesses such as photographic studios, this is a major problem. Their business is images and yet these images could be taken

without permission and reused in other jurisdictions because of the reach of the cloud. Hence, it seemed sensible to me, to develop tools and techniques that will begin to address these problems.

In cloud computing the instrument that was being used to manage the legal requirements of ownership was the service level agreement (SLA). These SLAs were in general little more than the end user signing away their rights for the ownership of the intellectual property and for the cloud service supplier to guarantee the technical performance of their system. The researcher's concern was that there is a big gap in understanding of the nature of the information content represented in these SLA documents. In the first instance the end user committed their intellectual property to the cloud but was not guaranteed the content would not be disclosed. In the second instance the service supplier guaranteed system performance, access and often the speed of access, and the fees required for the service. Together the mutual assurances left a huge gap where neither party could gain recourse for compensation when the content of a program, document, and image, or any other object in the cloud was wrongfully disclosed or compromised. To me this did not seem right when many of the information elements committed to the cloud or processed in the cloud have considerable value based on their creativity and content protection.

The researcher's thinking ran that the solution to the problem could be found in a two pronged attack. First by improving the policies governing cloud contracts - including the contents of SLAs; and, secondly by building software applications that would protect the rightful ownership of intellectual properties in the cloud. The situation appeared to me that both elements had been missing from the arrangements being put in place for cloud usage. Consequently, the researcher have to narrow the targets for research but the problem of privacy in cloud environments and the identification of rightful ownership to objects in the cloud environment stands out as a feasible research topic.

The final motivation the researcher had was that he likes challenges. He has always enjoyed the use and the study of technology, and he could see that there are ways to improve the current situation. It would probably be an easier task to simply theorise solutions but he also wanted to build solutions and software applications which could be used not only to prove the theory but also to influence practice in cloud environments. The outcome of such research would be to satisfy two

customers. One customer would be the end user who at the moment is left with their own resources to protect their intellectual properties when they put them into the cloud, but often these resources are inadequate against the managerial attacks the cloud environment has with respect to the host. The second customer is the cloud service supplier who is at the mercy of the markets and may not be able to sufficiently control every situation so that the end user can be assured of their digital rights. With these two customers in mind the researcher have to design a solution that bridges the interests and delivers a secure solution that will protect intellectual property rights in the cloud.

1.2 RESEARCH METHODOLOGY

The research subject domain is a complex network of tensions that are dynamic and interrelate with human and technical constraints. It has many aspects and various levels, which require a pragmatic research approach to attempt to solve the defined problem. Thus the Design Science (DS) methodology is used to build the artefact and answer the research question: How can rightful ownership be protected in the Cloud? In DS, guidelines and roadmaps as well as artefacts evaluation criteria are adopted. According to Berndtsson, Hansson, Olsson and Luncell (2008, p. 10) to ensure the defined problem is researched in a systematic way, a methodology has to be defined and applied, to enable a researcher to obtain relevant data and to analyse it accordingly. IT research often, concerns complex systems, where technologies, people and organisations are interconnected and required to comply with various regulations (Berndtsson et al., 2008; Vaishnavi & Kuechler, 2008). IT research should be based on multi- paradigms, and a pragmatic approach to produce a tentative solution. A researcher may not always have a full understanding of the whole system (Oates, 2006; Vaishnavi & Kuechler, 2008). Peffers et al. (2007) claimed that the use of the interpretive research paradigm has been accepted in IS research, however, “the resulting research outcome is mostly exploratory and, it could be argued, not often applicable to the solution of the problem encountered” (p. 1). On the contrary, “design, is the act of creating an explicitly applicable solution to the problem” (p. 1), is accepted as a research paradigm in faculties such as engineering (Peffers et al., 2007). DS has been progressively, albeit slowly, accepted by IS researchers since 1990s, to

improve effectiveness and utility of the produced IT artefacts (Alturki, Gable, & Bandara, 2011a). According to Hevner et al. (2004) a researcher adapting DS must further the existing knowledge that would help resolve the identified problem, and to develop and communicate findings to a target audience. However, adding new knowledge through developing validated artefacts is not an easy exercise to undertake and could require a number of iterations (Hevner et al., 2004). IT artefacts developed and implemented in an organisation context, require, behavioural-science research validation to explain the artefact's use, usefulness, and impact on practitioners and organisations (DeLone & McLean, 1992, 2003; Seddon, 1997). The experts' evaluation and insight are paramount to test the theoretical assertions in order to gain a wider view of the problem in any DS research.

Peffer et al. (2007) developed the DS Research Methodology (DSRM) along with a framework (shown in Figure 3.3), to aid researchers in conducting of DS based IS research. However, some authors have indicated that the DS guidelines and the questions, are all deemed too abstract to follow (Peffer et al., 2007; Alturki et al., 2011a). Furthermore, the lack of specificity could cause conflicting issues (Alturki et al., 2011a; Alturki, Gable, & Bandara, 2013). To streamline tasks and activities at each stage, Alturki et al. (2011a) have developed a roadmap and further refined the roadmap, aligned with the three DS cycles.

The researcher believes that the best approach to achieve the research objectives is by adopting DS research methodology and following the DSR guidelines (Hevner et al., 2004) and DSR roadmap (Alturki, Gable, & Bandara, 2011b) to ensure deliverables are obtained according to the DS guidelines and roadmap. Data will be collected from experts' oral and written feedback as well as the statistical results of testing the artefact in the lab environment. Answers to a number of question sets formed around the usability of the developed artefacts and other aspects such as functionality, efficacy, performance, and fit for purpose; will be addressed. Furthermore, the researcher's critical reflection, notes and observations will be used for further analysis.

1.3 FINDINGS

The research delivers a design that reengineers the current cloud service and user

supplier relationship, and shifts the responsibility for security mechanisms from the end user onto the cloud service supplier. The cloud service supplier is also provided with the knowledge component built into the software artefact of this research that will adequately watermark all incoming information to the cloud service. Watermarking was chosen as the ideal mechanism for the protection of intellectual property and the identification of rightful ownership in the cloud environment (see chapter 2).

The matters of digital rights have been largely overlooked in the cloud computing literature. An assumption is made that computing services are neutral. However computing services carry content that is valuable and can be accessed in a multitude of legitimate and illegitimate ways. The theoretical research has confirmed that there is a general dearth of literature covering privacy and the protection of content ownership within the cloud environments. These observations are part of the findings of this thesis that have been substantiated by literature analysis and the assessment of cloud security options in practice.

The strongest contribution this thesis makes is in its evaluation of theory and demonstration in practice that feasible solutions to a vexing problem may be obtained. The utilisation of the design science framework and methodology is a contribution in itself. Many people argue that design science cannot be used for theoretical work. The researcher disagrees with this point of view and would counter the position by suggesting it is a matter of the depth of critical reflection, testing and evaluation that is undertaken in any research project that substantiates its value. Design science has all of these features in the statistical and naturalistic evaluation schema. The considerations of theory and practice provide a much more comprehensive understanding of any situation and in particular the solution to problems that are found in different situations. This study can be taken as a use case for the application of design science methodology and as a contribution to further theoretical development of the framework. Design science has been found adequate and a valuable tool for resolving these theoretical and real-world problems confronting cloud computing (see chapter 3).

1.4 RESEARCH ORGANISATION

The thesis is structured in the following way: Chapter 2 establishes the literature

foundation, where the theoretical model for cloud watermarking is assessed. A fundamental definition of cloud computing and its privacy concerns are reported and tabulated into Table 2.1 of the literature analysis. Three literature questions are selected to organise the literature review and focus the elibrary database search onto potential research targets. The literature review compares similar works, seeking the answers to the identified gap in the literature coverage. The chapter then continues with the response to the gap and a full review of the possible solutions for watermarking that can be used in the cloud environment.

Chapter 3 specifies the research methodology that is taken from and derived from reviewing other similar research studies. Then, the challenge of developing and selecting researchable questions to the problem is taken up. The focus problem is examined again to select a workable research question. Furthermore, aspects from the selected research method, industry practices, data reporting and presentation methods, will be examined to identify the justification for the chosen methodology. That leads to justifying the grounds for selecting the research methods, which were derived and reasoned from literature. Part of the research method is to define the data collection methods and to propose analysis, evaluation and reporting criteria. The task of developing an artefact is then facilitated by the DS methods and a plan made for building and evaluating the artifact.

In Chapter 4, the design of the artefact and its steps following the design science road map is presented. A full review of the preparatory activities that are needed to be done before designing the algorithm is made. The text elaborates the artefact design process and the implementation processes and demonstrates the working software. An experimental and modeling approach is used to build the artefact with the aim of designing a Rightful Ownership Detection System (RODS) to enhance the copyright protection of the cloud users in the cloud environment.

Chapter 5 has been designed to evaluate the implantation of the demonstrated artefact in chapter 4 by following the DS methodology road map explained in chapter 3. The RODS has been shown working and is made ready for the evaluation. According to the DS roadmap adapted in the research, artefacts will be subject to the two types of evaluation: Naturalistic evaluation from experts' feedback and statistical evaluation by putting the artefact under the

evaluation techniques discussed in Chapter 3. The experts' evaluation has been tabulated and the researcher's critical reflections to respond to the experts' feedback has been discussed. The chapter then continues by the statistical results of the artefact's evaluation. The RODS has been tested for each implementation section by establishing unique feature selections for the watermarking resilience and robustness qualities.

Chapter 6 focuses on the research contribution. It is structured to take the evidence presented in chapter 5 and use it for qualitative hypothesis testing. In addition the research question is answered by considering the outcomes of the hypotheses tests and other evidences accrued during the research process. The chapter then concludes with the critical review and evaluation of the design science methodology considering the artefact's contribution to the theory as well as the business practice.

In Chapter 7 the research is summarised and concluded with recommendations and suggestions for further research and related topics.

1.5 CONCLUSION

The security challenges that are apparent in the new cloud technologies require new strategies and approaches to protect information in the cloud environments. This thesis is to address the issue of privacy and the subsequent rightful ownership of information in the cloud. A design science approach has been selected as being a proven way of tackling exploratory investigations and open-ended problems. Chapter 2 will now review the relevant literature in order to establish a basis for the theoretical problem area.

Chapter 2

Literature Review

2.0 INTRODUCTION

Chapter 2 provides a review of relevant literature as a background to watermarking and the cloud environment. The chapter is structured to first provide a background to cloud computing and its definitions. This is then followed by the selection and definition of a methodology with which to choose the relevant literature. Okoli's (2010) eight-step methodology is applied to guide the literature choice and to justify the inclusions and the exclusions of works. The matters of Cloud privacy issues and quality appraisal are documented from the selected literature. In table 2.1 a comprehensive summary of the literature available at the date of this research, and is tabulated and analysed with regard to its contribution. From the analysis a significant gap is found in the literature regarding watermarking applications and use for security in cloud technologies. The potential for research in this area is summarised in figure 2.5 and the technicality of watermarking for the cloud detailed. Chapter 2 achieves the theoretical foundation that the literature provides and the opportunity to focus the research onto key matters of interest.

2.1 BACKGROUND

The National Institute of Standards and Technology (NIST), defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell, 2011). Cloud computing is a general term for something which is involved in delivering hosted services over the Internet. These services are divided into three categories, Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). “The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in diagrams or tables” (Zissis *et al.*, 2011). Cloud computing as a new systems technology that has

challenged traditional ways of approaching security. Cloud service providers have made tangible progress in securing their environments and protecting the customer but little progress is made on issues of control and ownership once the data is protected (Zissis *et al.*, 2011). Providers are reluctant to sign off assurances because the risk assessment suggests that breaches will occur and that in the multiplicity of arrangements for storage and processing privacy may not be protected. In this regard, there is a breakdown of roles and responsibilities between cloud service providers and customers when moving sensitive and proprietary data to third-party service providers. Maintaining control and ownership of data in the cloud is not currently in many service contracts (Liu *et al.*, 2011; Yuhua and En-hui, 2009).

Storage service providers assure the user data's security in two aspects. They promised data cannot be modified, compromised, lost or damaged. This was the traditional way to protect the user's data, which could be solved by using data backup, recovering, virus killing or firewalls. On the other hand, all data owners care about, is that, if service providers are modifying their data or revealing information without authorisation. This is a trust management issue regarding protection and privacy (Liu *et al.*, 2011). While users increasingly embrace cloud computing, data privacy advocates, regulators, and lawyers are not so quick to change and adopt new contexts. Critics often raise concerns due to perceived risks for privacy and security of personal data. To them, cloud computing means primarily that users transfer data to far away systems that they do not understand, own, or control (Xia, Z., *et al.*, 2016a). As it is often the case with respect to legally and technologically complex topics, oversimplifications, over-generalizations, buzz words, and slogans are quickly established and abused to pursue various policy and competitive agendas. The agendas include keeping jobs in-country, protecting local industries, and shielding established business models from disruptive alternatives. Data is often secure and protected in some clouds better than in traditional systems but trust remains an issue (Liu *et al.*, 2011).

With these concerns, chapter 2 will be reviewing relevant studies with four main focuses – Cloud Privacy (Data Protection in cloud), ownership protection, Watermarking and Image Authentication. Chapter 2 will follow a systematic literature review method and the steps will be followed according to the literature research method shown in figure 2.1. First, an evaluation on Cloud privacy classification will be conducted, followed by an in depth of data protection, which

leads to rightful ownership protection concerns in the cloud. Second, the chapter continues with dividing the similar research works in to a tabular form, followed by an analysis of the similar research. Finally, the chapter ends with a response to the existent gap resulted in the analysis of the literature review.

2.2 RESEARCH METHOD FOR LITERATURE SELECTION

The scope of the literary review includes a variety of purposes. It includes providing a theoretical background for subsequent research; learning the breadth of research on a topic of interest; and answering practical questions by understanding what existing research has to say on the matter. As such, research reviews are most often published as the introductory section of an article reporting a specific research study, or as one of the early sections of an academic thesis or dissertation. Rather than just providing a base for the researcher's own endeavours, it creates a solid starting point for all other members of the academic community interested in a particular topic.

An eight step Systematic Review has been adapted from Okoli (2010) as the operative Research Method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners. The eight steps are as follows:

1. Purpose of the literature review: The first step in any review requires the reviewer to clearly identify the purpose and intended goals of the review. This is necessary for the review to be explicit to its readers.
2. Protocol and training: For any review that employs more than one reviewer, it is critical that the reviewers be completely clear and in agreement about the detailed procedure to be followed. The review requires both a written, detailed protocol document, and training for all reviewers to ensure consistency in the execution of the review.
3. Searching for the literature: The reviewer needs to be explicit in describing the details of the literature search, and needs to explain and justify how the comprehensiveness of the search was assured.
4. Practical screen: Also known as screening for inclusion, this step requires that the reviewer be explicit about what studies were considered for review, and

which ones were eliminated without further examination (a necessary part of any literature review). For excluded studies, the reviewer must state what the practical reasons were for their non-consideration, and justify how the resulting review can still be comprehensive given the practical exclusion criteria.

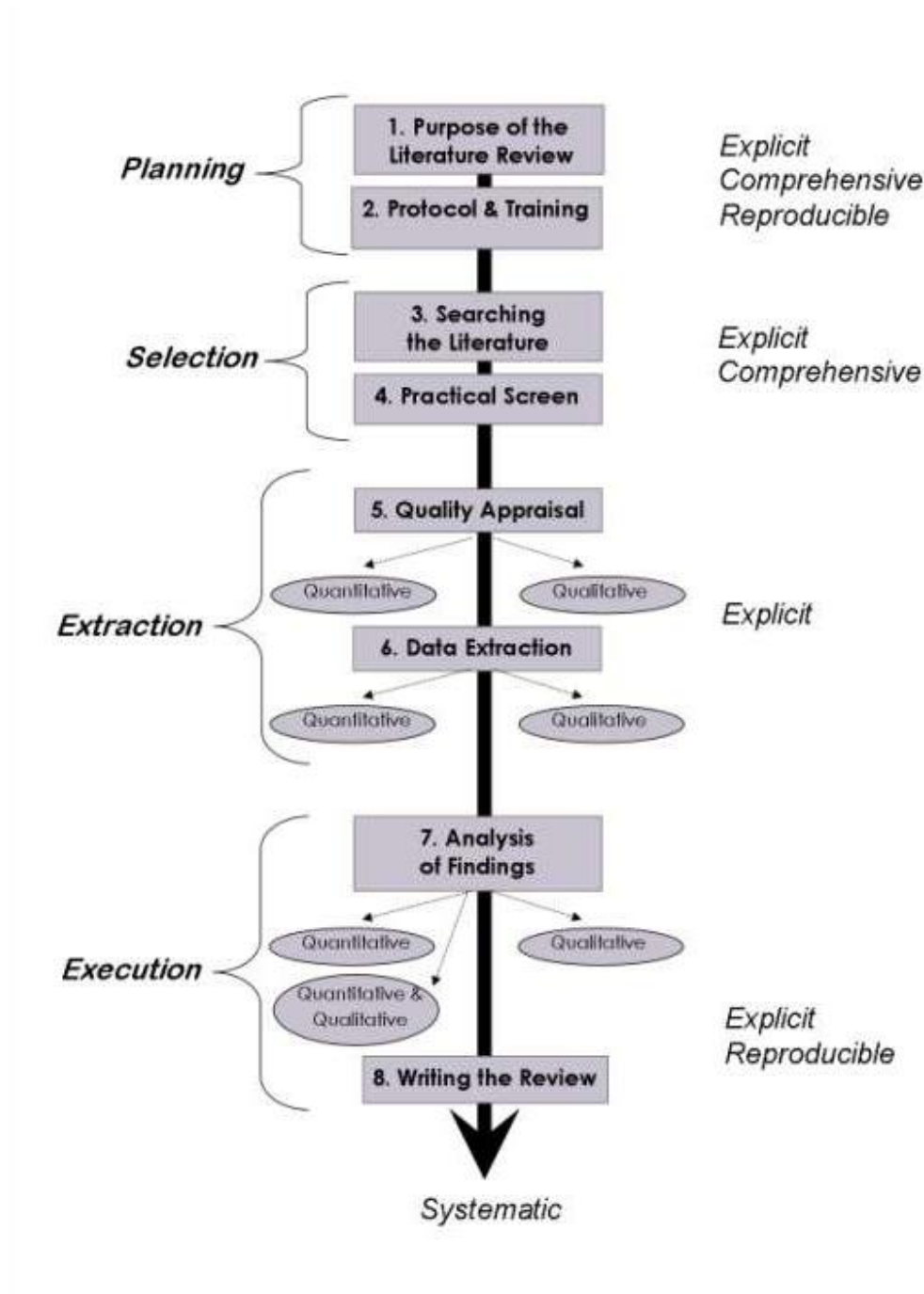


Figure 2.1: Systematic Review Steps (Okoli C., 2010)

5. Quality appraisal: Also known as screening for exclusion, the reviewer needs to explicitly spell out the criteria for judging which articles are of insufficient quality

- to be included in the review synthesis. All included articles need be scored for their quality, depending on the research methodologies employed by the articles.
6. Data extraction: After all the studies that should be included in the review have been identified, the reviewers need to systematically extract the applicable information from each study.
 7. Synthesis of studies: Also known as analysis, this step involves combining the facts extracted from the studies using appropriate techniques, whether quantitative, qualitative, or both.
 8. Writing the review: In addition to the standard principles to be followed in writing research articles, the process of a systematic literature review needs to be reported in sufficient detail that the results of the review can be independently reproduced.

2.3 REVIEW METHOD

The following research questions (RQs) are used to guide the literature analysis:

(1) What kind of requirements in Cloud privacy have been treated in the assessed published literature? (2) Which parts of cloud requirement have been under represented? (3) What would be response to the gap resulting from RQ2.

RQs have been used for determining the content and structure of the systematic review (SR), for designing strategies, for locating and selecting primary studies, for critically evaluating the studies, and for analyzing their results. The research literature review is concept-centric as it classifies and presents the publications according to the privacy area they address. In this section, boundaries of the work and the scope of the literature review has been set.

A variety of providers such as Scopus and IEEE as initial source has been selected, because they contain publications from major journals and conference proceedings, which has a diverse sample that is representative of the current state of the knowledge in the area of cloud computing security. The initial search in Scopus was on ‘security AND ({software as a service} OR SaaS)’ in the article title, abstract or keywords. Later the search string was refined to also include materials with ‘cloud AND security’ in the article title. The revision was done after manual review of some of the excluded articles by the initial search. Such publications discuss security challenges for cloud computing in general and sometimes do not refer explicitly to SaaS. The composition of the search string is

the result of a learning process including experimentation with a variety of combinations of key words in order to test synonyms used in literature and to cover the variety of cloud security requirements concepts. The following restrictions to define the boundaries of the study have been applied: (i) limit by source type (i.e. conference papers and journal articles), (ii) limit by publication year - before and including the first quarter of 2016, and (iii) limit by Scopus' subject area, i.e. Computer Science, Information System, Cloud Computing and Watermarking. The returned records by Scopus were 172 and two interesting observations have been made. First, about 66% of the articles were published in 2010 and 2011, which suggests that this is a fairly new and quickly developing area of research. Second, only 31 articles (approximately 18%) were from conferences on cloud computing or security which indicates that cloud computing cannot yet be separated from other IS disciplines. The 172 articles were manually reviewed for relevance to our RQs. As relevant all publications that comply with the following criteria have been considered:

- Cloud Computing Security and Privacy
- Ownership Protection
- Authentication
- Watermarking

2.4 CLASSIFYING AND USING A MODEL FOR PRIVACY REQUIREMENTS

Security and privacy from a holistic perspective based on the extracted data from the literature have been considered (Rittinghouse, J. W., *et al.*, 2016). The term holistic considers both technical issues, such as data integrity, availability of service, and accountability of provider activities and non-technical issues such as compliance, and policies (Islam et al., 2012b, Islam et al., 2010). Comparing to the other software system paradigms, cloud computing has some unique features in terms of service and deployment models. Therefore these issues require adequate attention for supporting the systematic identification of security and privacy issues in the context of cloud computing. At the same time all types of proactive counter measure such as monitoring, patch management, and hardening virtual machine instances should be implemented (Rosado et al., 2012). The

following security and privacy issues fall within the context of cloud computing:

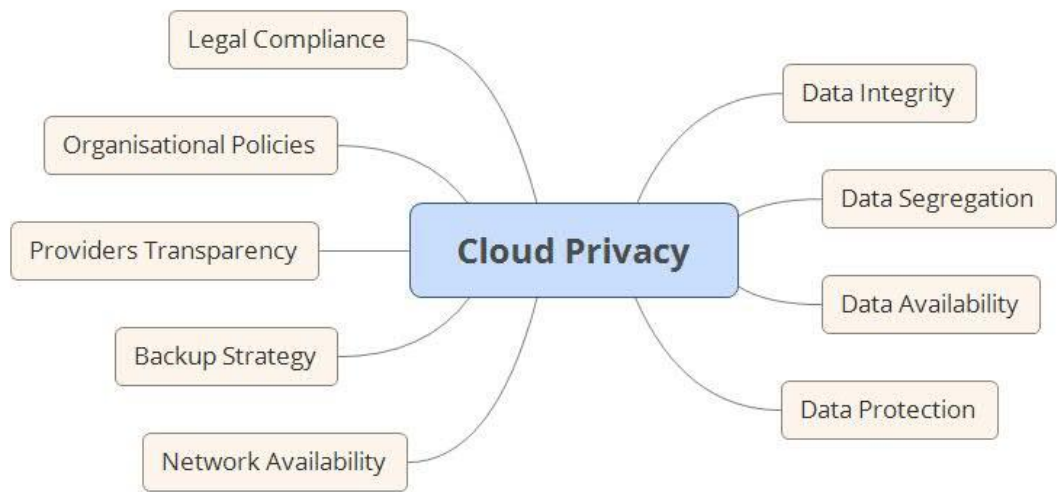


Figure 2.2: Cloud Privacy Issues Considered in this Research

2.4.1 Data Integrity

Data integrity is one of the most important factors when considering security in the cloud. Data integrity can be easily achieved in a standalone system, but because in a cloud solution multiple databases are used to store multiple tenants' data (Xia, Z., *et al.*, 2017b). The structure is complex to ensure transaction durability and consistency. As the cloud environment is virtualised at some level, standard methods, such as HTTP, of maintaining guaranteed transactions are not possible. The way to assure transactions is at the Application Programming Interface (API) level (Subashini and Kavitha, 2011). Sometimes this introduces extra complexity, and, through complexity, possible security vulnerabilities in the API stack itself or the technology handling the API calls. Vulnerabilities in API stack could allow an attacker to dump transaction data, intercept and provide false or corrupt data to the transaction destination which would lead to further data corruption, data theft and service breakdown leading to financial loss. Data integrity is measured by the level of secure channels in place for handling transactions. This is why data have to be transferred among servers and databases through secure channels. Hence, every transaction has to be verified for legitimacy (e.g. checksums), have a certain level atomicity, isolation and be durable. APIs handling the transactions have to be reliable, well recognised and time-tested (e.g.

the Simple Object Access Protocol)

2.4.2 Data Segregation

One of the major cloud characteristics is multi-tenancy. In multi-tenancy environment several users' data might be stored at the same physical location using the hypervisor techniques under the concept of virtualisation. An organization's data may be mingled in various ways with other users' data causing confidential data leakages; while users of other organisations might be exposed with the data of other organisations (Rosenberg and Mateos, 2011). For example, in 2009 a security flaw was discovered in Google Docs, which exposed documents to users that belonged to other users. That security problem happened because of the user session allocation. The problem was patched within hours, but it showed that users' data storage has to be separated to prevent accidental data leaks.

2.4.3 Data Availability

Providers must provide on-request and reliable service with highest up-times (it depends on the type and importance of corporate data and processes, but it might be up to 99.9999%, which is equivalent to 31.56s of downtime per year (Rosenberg and Mateos, 2011). If an organization's data gets locked-in and providers fail to provide access, this service disruption could pose potential financial damage to the organisation and its clients.

2.4.4 Network Availability

Cloud usage mostly depends on network connectivity and bandwidth. It is vital that the cloud is available whenever needed and that bandwidth throughput is able to handle the volume of data for an organisation, and retrieving the data from the cloud effectively. If these conditions are not met, the consequences will be similar to poor data availability. One strategy that could be deployed to attain high availability is obtaining the services of multiple cloud computing providers, other than a single provider (Armbrust *et al.*, 2010). A Provider could speed the scale-up in case of disruption of network bandwidth. In terms of availability, quality of service requirements relating to response time, throughput, reliability, scalability, and availability require negotiation with the service provider (Ferretti *et al.*, 2010).

2.4.5 Backup Strategy

An Organization's data might be backed-up and encrypted by the provider but it might be better, in some cases, for an organisation to backup their data on the cloud and then encrypt it. Backup and recovery is essential in case of failure. Data backups and recovery require regular testing, and as another security measure backed-up data should be encrypted and stored in several different locations. Encryption keys also require protection by the organisation and strong security management controls.

2.4.6 Provider's Transparency

A Cloud provider should provide the details of how client data will be handled, what types of security they already apply to the cloud infrastructure, what happens in case the system was compromised, if and how they will participate in the investigation and prosecution. If some details about the internal policies and technology implementation are kept in secret, clients must not blindly trust the provider's claims about security in their environment (Cachin and Schunter, 2011). In this case the provider must be investigated by the organisation to establish the level trust that may be imputed. The starting point of any investigation is to first assume that provider's environment is insecure and after investigation make corrections to the initial assumption. A Cloud provider might give all the important details when contacted directly, but it is important to triangulate this information with other independent sources.

2.4.7 Organisational Policies

Customer data protection is a core concern of security and privacy measures in cloud computing. Privacy is a moral and legal right of individuals. A Data owner needs to be assured that their data is not shared with any third party (Takabi et al., 2010). Storing data and applications that reside outside the organization's premises poses the potential risk of unauthorised access and processing of the data and application (Chen et al., 2010). Customers may lose control over their critical assets. Data confidentiality and privacy risks may be more critical when providers reserve the right to change their terms and conditions. Apart from the data theft from external attackers, data leakage is also carried out by the employees of the service providers. Therefore, measures such as privacy policy, data subject

consent and control, un-linkability, transparency of data, data operations, and assurance of data protection are necessary and should be included in the service level agreement (SLA).

2.4.8 Legal Compliance

Legal compliance is a significant challenge for cloud-based systems. Although a large number of information security and data privacy laws exist, depending on the country and location, there is no single, comprehensive legal framework in which the legal rights, liabilities, and obligations of cloud providers and cloud users are formulated (Islam et al., 2011). Both providers and customers need to comply with existing regulatory requirements and SLAs. SLAs are agreements between the cloud service providers and the cloud service users. A SLA should be complete, as well as well structured, taking into consideration the right to audit such as quality of service attributes and monitoring continuously and enforced by a SLA (Dawoud et al., 2010). On the one hand, customers may have to give their private data and important processes into the hands of personnel and out of their control. On the other hand, providers may be obliged to search the data due to national security or to comply with the local jurisdiction. The law is enforced at the place the data is stored as well as the place from where data are transmitted. Customers should take note of the jurisdictions in which their data may be stored or processed. Therefore, it is necessary to identify and analyse issues such as legal rights and alignment of SLA with legal obligations, protection and enforcement requirements before deploying a cloud computing solution.

2.4.9 Data Protection

Customer data protection is a core concern of security and privacy measures in cloud computing (Almorsy, M., *et al.*, 2016). People expect to have their information protected and within their ownership. This means that it is not accessible to third parties and that went to similar objects are retrieved, then the rightful ownership of each may be established (Takabi et al., 2010). Storing data and applications that reside outside the organization's control introduce new vulnerabilities and concerns regarding digital rights (Chen et al., 2010). Data confidentiality and privacy risks may be more critical when providers reserve the right to change their terms and conditions. Apart from the data theft from external

attackers, data leakage can also be carried out by the employees of the service providers. Therefore, measures such as privacy policy, data subject consent and control, unlinkability, transparency of data, data operations, and assurance of data protection are necessary and should be included in the SLA. Table 2.1 shows some of the data risks and vulnerabilities that can occur in a cloud environment.

Table 2.1: Key data risks in the cloud

Harm: Threat:	Data Loss	Data Inaccessibility	Data Modification	Data Access	Data Replication
1st Party					
Business Process Error	Y	Y	Y	Y	Y
Abuse of Privilege	Y	Y	Y	Y	Y
2nd Party					
Storage Error	Y	Y	Y	Y	Y
Availability Failure	Y	Y	Y		
Network Malfunction		Y	Y	Y	Y
Interception				Y	Y
Abuse of Privilege	Y	Y	Y	Y	Y
Data Incompatibility	Y	Y	Y		
3rd Party					
Hacking	Y	Y	Y	Y	Y
Injunction	Y	Y	Y	Y	Y
Government Powers	Y	Y	Y	Y	Y
DoS Attack		Y			

2.5 QUALITY APPRAISAL

The comparison in section 2.5 on different aspects of cloud privacy shows that the data protection and the critical need to protect the true ownership of the data is one of the most overlooked topics in cloud environments, in both the customer and the cloud service provider (CSP) side. Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. While cloud computing is expanding rapidly and used by many individuals and organisations internationally, data protection issues in the cloud have not been carefully addressed. In the cloud environment, users' data is usually processed remotely in unknown machines that users do not own or operate. Hence, users' fear of confidential data leakage and loss of privacy in the cloud becomes a significant barrier to the wide adoption of cloud services. This research, has conducted a

significant literature review that results in an analysis table at considers the current use of different techniques for responding to the third research question of this chapter. Table 2.2 shows a full analysis of the related works that form the basis for this research. The table has been divided into four categories of analysis based on the guiding literature research questions. It gives the relates solution and techniques that other researchers have used to tackle the cloud privacy issues of: cloud privacy, ownership and watermarking and the image authentication. These categories structure the analysis of literature so that the key attributes for focusing the research are visible. In the ‘Propose’ column, the innovation or contribution of each paper is summarised. Overall weaknesses are found in matters relating to privacy of information but strengths are found in protecting the system and the information from damage.

The Table 2.1 represents a sizeable contribution to this research. Not only was it time-consuming searching the e-library for the relative documents but each of the selected articles then had to be read and analysed according to the categories presented in the table. The result is substantial evidence and justification for the identified gap in the literature and the selection of the target for this research.

Table 2.2: Literature analysis of related studies

No.	Author	Year	Title	Cloud Privacy	Ownership Protection	Watermarking	Image Auth.	Propose
1	Lin Gu	2009	Constructing and Testing Privacy-Aware Services in a Cloud Computing Environment – challenges and Opportunities					Focusing on privacy protection, discussing the research challenges in this unique design space, and explore potential solutions for enhancing privacy protection in several important components of the system (Gu & Cheung, 2009).
2	Jaime Anthony Bowen	2011	Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations					A cloud model composed of five essential characteristics, three service models, and four deployment models (Bowen, 2011).
3	Dimitrios Zissis	2010	Addressing cloud computing security issues					Proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. (Zissis & Lekkas, 2012).
4	Apoorva Rathi and Nilesh Parmar	2015	Secure Cloud Data Computing with Third Party Auditor Control					Provides secure centralized control and alert system to achieve the integration of storage correctness insurance and data error localization in cloud. (Rathi & Parmar, 2015).
5	Katzan	2011	On The Privacy Of Cloud Computing					Provides a conspectus of the major issues in cloud computing privacy. (Katzan, 2011).
6	Tiegang Gao	2009	A novel image authentication scheme based on hyper-chaotic cell neural network					Presents a new image authentication scheme based on cell neural network with hyper-chaos characteristics (HCCNN). (Gao, Gu & Emmanuel, 2009).
7	Chao-Tung Yang	2011	Implementation of Image Watermarking Processes on Cloud Computing Environments					Proposes a method that can process image watermarking based on a robust method which combines the Singular Value Decomposition (SVD) and Distributed Discrete Wavelet Transformation (DDWT) over cloud computing environments. (Yang, Lin & Chang, 2011).
8	Samarati	2016	Privacy protection and security in eHealth cloud platform for medical image sharing					Propose two mechanisms to solve this issue. First, a caching third party that prevent the cloud provider (CP) to link the records from their time of acquisition is proposed(Samarati, 2016).

No.	Author	Year	Title	Cloud Privacy	Ownership	Watermarking	Image Auth.	Propose
9	Jen-Sheng Tsai	2007	A Feature-Based Digital Image Watermarking for Copyright Protection and Content Authentication					A feature-based robust digital image watermarking algorithm is proposed to achieve the goal of image authentication and protection simultaneously. (Tsai, Huang, Chen & Kuo, 2007).
10	Congxu Zhu	2008	A Multipurpose Watermarking Scheme for Image Authentication and Copyright Protection					Present a novel multipurpose digital image watermarking scheme based on discrete wavelet transform (DWT) and chaotic map, which can be applied to image authentication and copyright protection. (Zhu & Hu, 2008).
11	Shunguo Yang	2011	Cloud Computing Security Issues and Mechanisms					Addresses cloud customers' significant concerns about and requirements of cloud security. (Yang, 2011).
12	Chuan-Yu Chang	2010	Copyright authentication for images with a full counter-propagation neural network					A full counter-propagation neural network (FCNN) is applied to copyright authentication, where the ownership information (watermark) is embedded and detected by a specific FCNN. (Chang, Wang & Su, 2010).
13	C.Chang	2002	Robust authentication scheme for protecting copyrights of images and graphics					A simple and robust watermark-like digital authentication scheme is proposed. (Chang, Hwang & Hwang, 2002).
14	Junning Fu	2010	A Watermark-aware Trusted Running Environment for Software Clouds					Implement the scheme which mainly contains two parts: 1) embedding watermark into the Java programs running in the cloud; 2) generating customized JVMs for recognizing the watermarked programs. (Fu, Wang, yu, Wang & Sun, 2010).
15	Yu-Chao Liu	2011	A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking					Propose a data colouring method based on cloud watermarking to recognize and ensure mutual reputations. (Liu, Ma, Zhang & Chen, 2011).

No.	Author	Year	Title	Cloud Privacy	Ownership	Watermarking	Image Auth.	Propose
16	Khaled Loukhaoukha	2015	Security of ownership watermarking of digital images based on singular value decomposition					Watermarking algorithms of digital images based on singular value decomposition (SVD) have been proposed. (Loukhaoukha & Chouinard, 2010).
17	Guofu Gui	2006	Watermarking for joint ownership verification of digital images					A new watermarking scheme for joint owner- ship verification of digital images. (Gui, Jiang & He).
18	Min-Jen Tsai	2008	A wavelet-based semi- fragile watermarking with recovery mechanism.					Propose a novel image authentication and recovery scheme based on discrete wavelet transform (DWT). (Tsai & Chien, 2008)...
19	Gaofeng Zhang	2011	A trust-based noise injection strategy for privacy protection in cloud					Present a novel trust-based noise injection strategy for privacy protection in cloud. (Zhang, Yang, Yuan & Chen, 2012)
19	Husev T. Sencar	2005	Watermarking and Ownership Problem: A Revisit					Address the security weaknesses common to most watermarking techniques and assess the role of watermarking in construction of owner- ship assertion systems. (Sencar & Memon, 2005)
20	PW Wong	2001	Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification					Describe a watermarking scheme for ownership verification and authentication. (Wong & Memon, 2001)..
21	Chuanxian Jiang	2009	Watermarking Relational Databases for Ownership Protection Based on DWT					Focuses on the analysis of the wavelet high frequency coefficients of corresponding data and gives the definition of the intensive factor. (Jiang, Chen & Li, 2009)
22	Raja's Alomari	2005	A Robust Watermarking Algorithm for Copyright Protection					A New Robust Watermarking Algorithm for Copyright Protection. (Omari & Al-Jaber, 2005).

No.	Author	Year	Title	Cloud Privacy	Ownership	Watermarking	Image Auth.	Propose
23	Mr. Manjunatha Prasad R	2010	A Robust Wavelet Based Watermarking Scheme for Copyright Protection of Digital Images					Presents a novel robust invisible watermarking scheme for embedding and extracting a digital watermark in an image to protect its copyrights. (Prasad & Koliwad, 2010).
24	Zhiwei Yu	2011	A novel watermarking method for software protection in the cloud					Identify an insider threat to access control which is not completely eliminated by the usual techniques of encryption, cryptographic hashes, and access-control labels. (Yu, Wang, Thomborson, Wang, Lian & Vasilakos, 2011).
25	Shuguo Yang	2011	Cloud Computing Security Issues and Mechanisms					Addresses cloud customers' significant concerns about and requirements of cloud security. (Yang, 2011).
26	Satwan Mahmud Khan and Kevin	2012	A Data Ownership Privacy Provider Framework in Cloud Computing					Concealing ownership of cloud data without impeding computation over the data is presented and evaluated. (Khan & Hamlen, 2012).
27	Peng Jing	2015	A New Model of Data Protection on Cloud Storage					Studying cloud storage data protection model and implementing encrypted storage of user data in double- key form. (Peng, 2015).
28	Ruiying Du, Ian Deng	2014	Proofs of Ownership and Retrievability in Cloud Storage					Introduce a framework called Proofs of Ownership and Retrievability (PoOR) considering the requirement of mutual validation. (Du, Deng, Chen, He & Zheng, 2014).
29	Ali Gholami	2016	Design and implementation of the advanced cloud privacy threat modeling					describes an extension of Cloud Privacy Threat Modeling (CPTM) methodology for privacy threat modeling in relation to processing sensitive data in cloud computing environments (Gholami et al., 2016).

Table 2.1 shows a range of studies with focus mainly in cloud security, some of which addresses ownership protection, Some directly address the data protection in cloud concerns, however just a few scholars concentrate on using watermarking methods or authentication techniques to achieve rightful ownership in the cloud environments. None of these texts has shown to pinpoint the ownership protection issue by prescribing the most crucial authentication methods among with watermarking techniques. This research is to be informed by the analysis of literature presented in table 2.1.

2.6 RESPONSE TO THE GAP

Digital watermarking is a technology for copyright protection, which embeds the copyright information into digital production to avoid being tampered, peculated, and illegally copied (Johnson et al., 2001). The main idea of watermarking is to introduce small images or patterns in the data to be watermarked without affecting the data subject to normal use. If an illegal copy occurs, the owner of the data can therefore get watermarks from the illegal data to verify his ownership of the data. Cloud watermarking is a digital watermarking technology based on a cloud model, which has widely been applied in text and relation database media (Li, 2004; Liu et al., 2011). Currently similar research has been done for specific aspects of the Cloud security environment, watermarking and privacy protection, but few focused on privacy protection in the cloud (Refer Table 2.1). None has the focus of a privacy protection framework based on watermarking attributes and the cloud environment. Hence, a significant gap is identified for this research to address.

2.6.1 Watermarking

The concept of watermarking has been used in many different forms and can be traced back to thousands of years ago. For instance, in the late 13th century in Italy, a thin, translucent layer was sewn with wire onto a paper mold to form a watermark. With the growth of the Internet and data separation methods Digital watermarking is used to implement data security and ownership marking. Watermarking can be implemented to make a safer way for data transfer protection (Yang *et al.*, 2011; Yu *et al.*, 2011). A major problem faced by content providers and owners is protection of their content. They are concerned about copyright protection and other forms of abuse of their digital content. Unlike

copies of analogue tapes, copies of digital information are identical to the original and suffer no quality degradation, and there is no limit to the number of exact copies that can be made. In addition, duplication equipment is widely available and inexpensive. One approach to content security uses cryptographic techniques, but those encryption systems do not completely solve the problem of unauthorized copying. All encrypted content needs to be decrypted before it can be used. Once encryption is removed, there is no way to prove the ownership or copyright of the content. As a solution to this problem, digital watermark technology is now drawing attention as a new method of protection against unauthorized copying of digital content. A digital watermark is a signal added to the original digital data itself (namely, audio, video, or image), which can later be extracted or detected.

A watermark imprint is intended to be permanently embedded into the digital data so that authorized users can easily access it. At the same time, the watermark should not tamper with the quality or authenticity of the digital media file. In general, digital watermark techniques must satisfy the following requirements (Jong Won and Jin Woo, 2001). A digital watermark can be either visible or invisible. An example of visible digital watermark is the translucent logos that are often seen embedded in the corner of videos or images, in an attempt to prevent copyright infringement. However, these visible watermarks can be targeted and removed rather simply by cropping the media, or overwriting the logos. Subsequently, the field of digital watermarking is primarily focused on embedding invisible watermarks, which operate by adjusting the content of the media imperceptibly. As the watermark cannot be seen, there must exist a robustness property that ensures the watermark data survives if the image is altered (Jong Won and Jin Woo, 2001).

Typical applications of digital watermarking can include broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control legacy enhancement and content description. Figure 2.3 illustrates a typical watermark embedding process. The Watermarked work is produced from an embedding algorithm that is traditionally comprised of three inputs: the Original work, the Watermark and a Key. A blind watermark detection process is shown in Figure 2.3. The watermark is extracted from the Watermarked work by using a detection algorithm in conjunction with the same key that was originally used to embed the watermark.

Here, the Original work has to be provided as a reference source in order for the detection algorithm to function (Zhao and Ho, 2010).

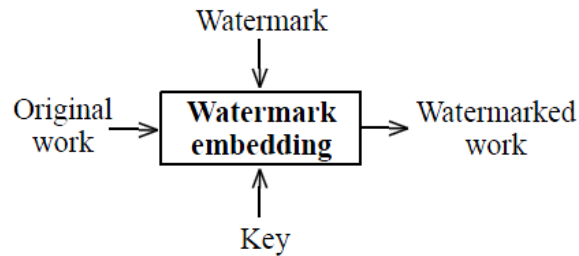


Figure 2.3. A typical watermark embedding process (Zhao and Ho, 2010)

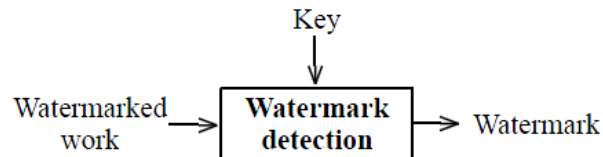


Figure 2.4. A typical blind watermark detection (Zhao and Ho, 2010, p.14)

Therefore, the selection of a blind or non-blind watermarking detection system typically depends on whether the original work is accessible or not. The original work is the host signal which is employed into diverse forms such as video (Jing *et al.*, 2007), audio (Kirovski and Malvar, 2003), image (Yuhan and En-hui, 2009), halftone image, binary text, 3D meshes, holography, optical and network protocol (Zander *et al.*, 2007). The watermark is a binary sequence of data produced from a logo image, fingerprint, serial number, owner's name or ID, or indeed anything that could identify the ownership of the media. The key is used to increase the security of the procedure; it prevents the possibility of an attacker modifying or removing the watermark as this can only be achieved if the key is known (Zhao and Ho, 2010). One of the main applications of watermarking is for copyright defence. An image, video, text document or audio sample may be embedded with a watermark and registered with a copyright authority. Watermarks are a legally recognized method of proof of ownership and if copyright is infringed then the matter can be presented to a court of law (Zhao and Ho, 2010).

There are three types of watermark and their appropriate keys. These are private-key, detection- key and public-key. A private-key is available only to the author and can be thought of as a flair or the signature of the product, for example points being snapped to grid spacing in 3D objects or certain colours used in images. This type of watermark should not be detectable by anyone other than the original author. In this project authorized user to the cloud and his/her cloud provider will use this method, because of the need for privacy and the capability of detecting the compromised uploaded image. Public-key watermarks are those that can be extracted from the public. An example of this type of key is the RSA Algorithm used in cryptography. These are used for verification purposes – perhaps to ensure the seller is the rightful owner. Finally, the detection-key is the method that is recognized in the court of law. This key is available only to the author and a trusted copyright authority and can be used to bring justice to copyright infringement. The key can be used to extract the watermark and this should uniquely identify the author. It is illegal to use copyrighted files for unauthorized distribution or for the watermark to be intentionally removed (Barker, 2004).

Another application for watermarking is to trace the route of the certain files during the distribution. Multiple watermarks can be embedded in the media as long as saturation does not occur. At each server or router in a network, a simple watermark may be embedded in real-time. These watermarks may contain an IP address or DNS name. Once a file is obtained using this method it is possible to trace the route of the file between clients (Zhao and Ho, 2010). The watermark within a file may be modified or removed so that the original owner cannot be uniquely identified. Such methods are known as attacks. The following figure is an illustration of the watermarking scenario that has been included the image as the carrier of the watermark and the potential watermarking methods to be used in cloud environment for robustness as well as invisibility. Figure 2.5 shows each classification followed by the explanation of the main watermarking methods and attributes.

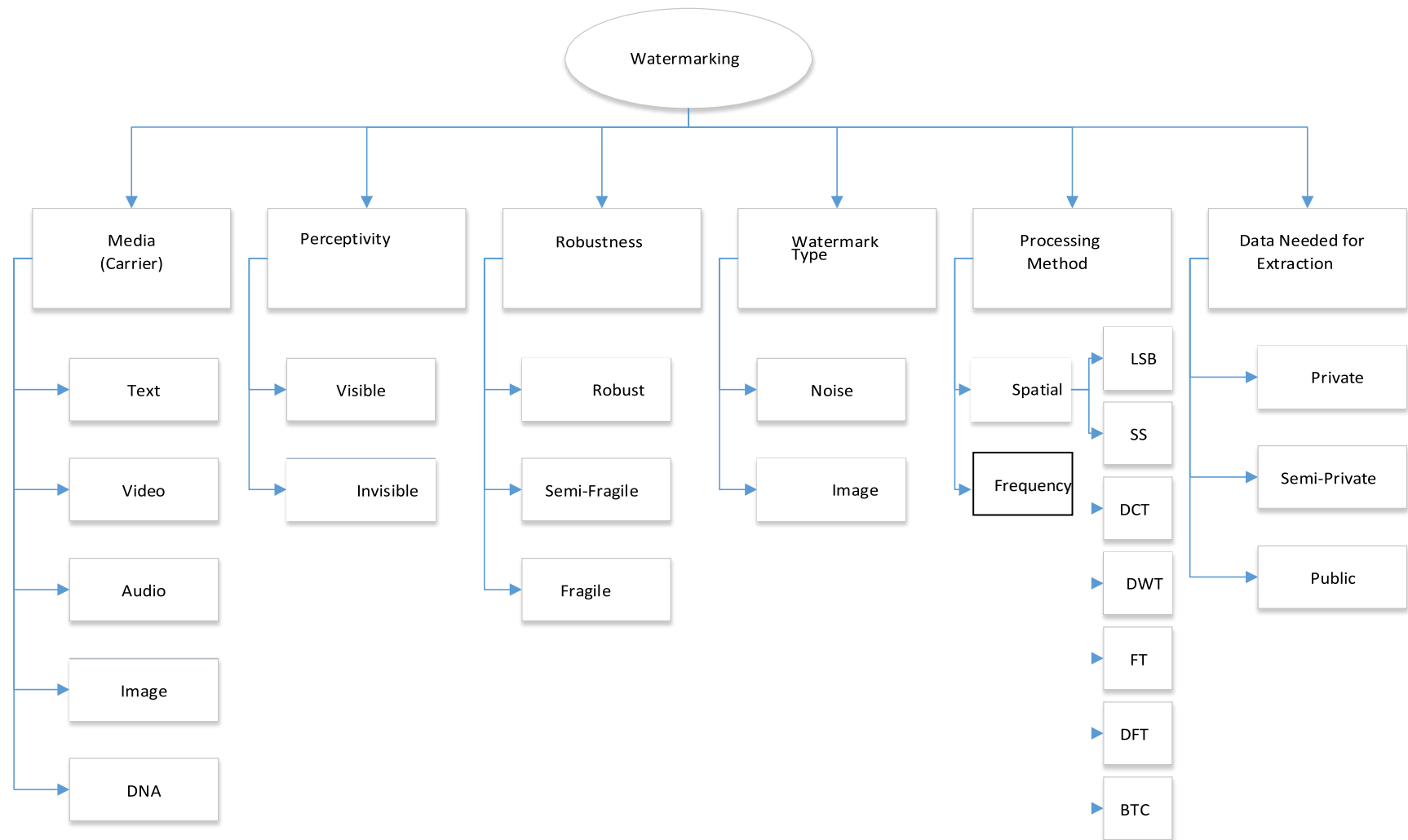


Figure 2.5: Watermarking Scenario

2.6.2 Spatial Domain and Frequency Domain

Digital watermarking schemes are usually classified into two categories: one is in the spatial domain (Hernandez Martin and Kutter, 2001). It directly changes digital data to hide the watermark. The advantage of this kind is low computational complexity. But, it has weak defense against digital signal processing. Another is in the frequency domain. It must first process digital data to be in the frequency domain with a transformation (such as Fast Fourier Transformation or Discrete Cosine Transformation or Discrete Wavelet Transformation). Then, it changes the coefficients which are obtained by transformation to hide watermarks. Finally, it inversely transforms these changed coefficients to be in the spatial domain. Compared with the spatial domain, it needs more computation, but it can provide better robustness (Bruce, 2001).

2.6.3 Image Watermarking

Image watermarking is becoming more effective due to its extensive research. Original algorithms were calculated in the spatial domain. In images, not much information can be embedded in flat featureless regions without being detected (O'Ruanaidh *et al.*, 1996). Some algorithms attempt to incorporate most of the information into textured or on definite edges but care must be taken to maintain the integrity of the original. A common method of watermarking was to alter the least significant bit of each pixel in a pseudo-random manner. This offers a poor robustness as it is very susceptible to noise and also requires the original image for detection of the watermark (Bruce, 2001).

2.6.3.1 Robust, Fragile and Semi-fragile Image Watermarking

There are three different classifications associated with digital watermarking, depending on the applications: robust, fragile and semi-fragile. Each is now defined.

Robust watermarking has been used extensively in the past decade, and is primarily designed to provide copyright protection and proof of ownership for digital images. The most important property of robust watermarking is its ability to tolerate certain signal processing operations that usually occur during the lifetime of a media object. The sender watermarks the original work via a watermark embedding process, and then sends the watermarked work to the receiver. The

receiver extracts the watermark via a watermark detection process. During the transmission of the watermarked work, the image is open to attack, meaning the integrity of the watermark data is in jeopardy. Examples of common attacks include JPEG compression, additive noise, and filtering, and geometric distortions such as rotation and scaling (Zhao and Ho, 2010).

In contrast to the applications of robust watermarking, fragile and semi-fragile techniques are geared towards image authentication and localization of tampered regions. Fragile watermarking can be used to detect any small manipulations made to the original image. Hence, any attacks that ultimately alter the pixel values of an image can be detected, and the tampered regions can be located accurately when applying fragile watermarking schemes. Many fragile watermarking algorithms are intentionally designed for use in the spatial domain (typically by altering the Least Significant Bits (LSB) of the image), as this domain is widely documented as being relatively fragile and sensitive to small changes (Zhu *et al.*, 2009).

Semi-fragile watermarking techniques for image content authentication have recently attracted much attention. This is due to the fact that comparing to fragile watermarking, semi-fragile watermarking is not as sensitive as fragile watermarking. Semi-fragile schemes make it possible to verify the content of the original image, as well as permitting alterations caused by non-malicious (unintentional) modifications such as system processes. Moreover, semi-fragile watermarking is more focused on detecting intentional attacks than validating the originality of the image. During the image transmission, the mild signal processing errors caused by signal reconstruction and storage, such as transmission noise or JPEG compression, are permissible. However, image content tampering effects such as a ‘copy and paste’ attack are identified as a malicious attack (Zhao and Ho, 2010).

2.6.3.2 Requirements for Digital Image Watermarking

Four important properties for digital watermarking are discussed here. These are imperceptibility, robustness, capacity and security (Zhao and Ho, 2010).

- **Imperceptibility**

The embedded watermark should be imperceptible from the watermarked work. The degradation of original work to watermarked work is permitted with the rule of maintaining image fidelity of the original work. Therefore, in order to evaluate the similarity between original and the watermarked image, objective and subjective evaluation methods are required.

- **Robustness**

Robustness is an important property for robust watermarking schemes. The watermark that is embedded into the image should be robust (to varying degrees according to the application) to tolerate different forms of attack or image processing operations when the watermarked image is transmitted. These image manipulations or attacks can be categorized into non-geometrical and geometrical groups. Non-geometrical distortion is derived from lossy compression algorithms such as Jpeg as well as noise addition, image filtering and contrast stretching, while geometrical distortion includes rotation, scaling, cropping, translation, and shifting pixels. These distortions are often implemented to simulate possible attacks to analyse the performance trade-off of the proposed algorithms by the researchers in the community. Maintaining the robustness of the watermark is much more difficult and challenging when considering geometrical attacks. This is due to the fact that each individual pixel location of the watermarked image is likely to be shifted or translated. A possible approach is to find an invariant property of an image that can be used in the watermark embedding process to enhance the robustness against different attacks (Zheng *et al.*, 2007).

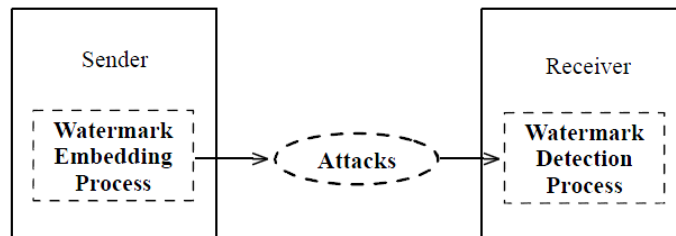


Figure 2.6: Schematic diagram for robust watermarking (Zheng *et al.*, 2007)

- **Capacity**

Zheng *et al.* (2007) also believe Capacity refers to the maximum amount of watermark bits that can be embedded into the original image. The number of watermark bits embedded into the image data can affect the overall perceptual quality of the image. Figure 2.7 illustrates the performance tradeoffs concerned with watermarking; specifically, the imperceptibility of the watermarked image, the robustness of the watermark, and the capacity of the watermark data.

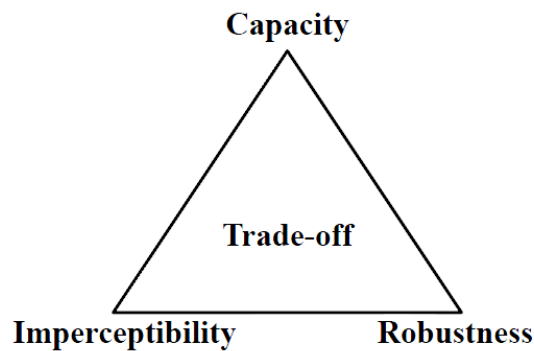


Figure 2.7: Trade-off among the imperceptibility, robustness and capacity (Zheng *et al.*, 2007)

According to Zhao and Ho (2010), if the quality of watermarked image is high, then the robustness and capacity of the watermark data will be degraded. Similarly, if the robustness is high, the quality of watermarked image is likely to be degraded, as a greater number of watermark bits will be used. Finally, if the capacity of watermark data is increased, the quality of the image and its robustness will decrease.

- **Security**

The approach to security in digital watermarking is mainly focused on malicious removal or modification of the watermark bits. The watermark security can be defined as “the inability by unauthorized users to have access to the raw watermarking channel” (Cayre *et al.*, 2005, p, 49). The watermarking systems could be compromised if an attacker manages to obtain the secret key. In this case,

the attacker will have access to parameters such as the watermark embedding locations, random frequency of the watermark bits, and the threshold for embedding the watermark bits. Gathering the characteristics of a set of watermarked images and analysing their similarities, to evaluate, can predict the secret key whether the same secret key and watermark bits have been used repeatedly. Some of the problems associated with secret key leakage have been studied by a number of researchers (Cayre *et al.*, 2005; Chuhong *et al.*, 2006).

2.6.4 Processing methods in frequency domain

The most important processing methods which have been used in frequency domain can be divided into two methods: Singular Value Decomposition and Discrete Wavelet Transformation. The following sub-sections discuss these issues.

2.6.4.1 Singular Value Decomposition

Singular Value Decomposition (SVD) based watermarking schemes are novel techniques, they are similar to frequency-domain-based schemes, and it can also be considered as a transformation, e.g. a SVD-based watermarking scheme. Although this scheme has good embedding quality and high robustness, it needs to store three matrices whose sizes are equal to these of the original image to extract the watermark. In addition, Chandra (2002) also proposed two SVD-based watermarking schemes. One is a global-based scheme, and another is a blocked-based scheme. Their robustness and embedding qualities are strong. However, Chandra's global-based scheme also needs to store three matrices to extract watermarks, while Chandra's block-based scheme needs the original images to extract the embedded watermarks. These schemes will add to the load for the watermarking system. In the next section, details of these related schemes will be shown (Chandra, 2002; Chang *et al.*, 2007).

2.6.4.2 Distributed Discrete Wavelet Transformation

Due to the shortcoming of the Discrete Wavelet Transformation (DWT) method, which embeds watermark information in the LL sub-band and is vulnerable to the cropping attack, Chang *et al.*, (2007), also proposed the Distributed Discrete Wavelet Transformation (DDWT) method to solve this problem. This method

transforms images from the spatial domain into the frequency domain by using the multi-scale DDWT, and embeds watermark information in the frequency domain and then performs the inverse DDWT to obtain the stego-image in the spatial domain. The DDWT method distributes hidden watermark information in spatial coefficients. The purpose of distributing information is to handle malicious depredations of the centre part of the image where the watermark information is located using the DWT method. Imperceptibility and distributed information are characteristics of DDWT watermarking so that it is very robust against the cropping attack. However, the DDWT watermarking technology is not robust against other geometric attacks such as rotation, scaling, transposition and non-geometric attacks such as sharpening, blurring, Gaussian noise. The example of a 3-scale DDWT transform is shown in Figure 2.8.

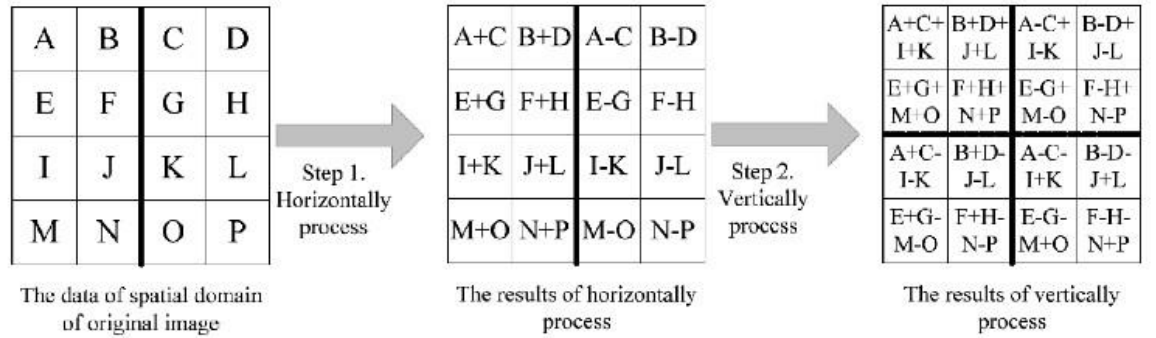


Figure 2.8: 3-scale DDWT transform Chang et al., (2007, p. 40)

2.6.5 Attacks on watermarking

Despite of these watermarking methods being well established, the watermark itself is still vulnerable to attacks. Sherekar *et al* (2011) details that a watermark attack could comprise of intentional or unintentional tampering which will impair the integrity of the data. Any alterations or manipulation during the processing of the original watermark is regarded as an attack. Processes could include lossy compression, signal enhancement, or digital-to-analogue (D/A) and analogue-to-digital (A/D) conversion. Processing of watermark data is often necessary and unavoidable when a file is to be transferred or made available in a cloud environment. In order to develop a concept that better protect the integrity of

watermarked work, first the different types of attacks and processes must be analysed and examined. These research aspects are reviewed in the following subsections.

2.6.5.1 Watermarking attacks classification

Categorization of the wide class of existing attacks contains many classes or attacks: e.g. removal attacks, geometric attacks, cryptographic attacks, and protocol attacks (Sherekar *et al.*, 2011). A summary is made in table 2.3. Accordingly, the research will focus on potential attacks that can be applied on the watermark to harm the purpose of robustness and visibility of it. The benchmark of the stability also provides a metric from which the robustness of the watermark can be measured after attack.

Table 2.3: Watermarking attacks classification

Active attacks	The Attacker tries deliberately to remove the watermark or simply make it undetectable. This is a prominent issue in copyright protection, fingerprinting or copy control (Sherekar <i>et al.</i> , 2011)
Simple attacks (waveform attacks or noise attacks)	Conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. Examples include linear and general nonlinear filtering, waveform-based compression (Jpeg, Mpeg), addition of noise, and the addition of an offset, cropping, quantization in the pixel domain, conversion to analogue, and gamma correction (Sherekar <i>et al.</i> , 2011).
Removal attacks	Removal attacks are attacks that attempt to analyse the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and dispose of only the watermark. Removal attacks aim at the complete discard of the watermark information from the watermarked data without cracking the security of the watermarking algorithm. This category includes de-noising, quantization (e.g., for compression), re-modulation and collusion attacks. (Sherekar <i>et al.</i> , 2011).

Protocol attacks:	Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data (Bangaleea and Rughooputh, 2002). It has been shown that for copyright protection applications, watermarks need to be noninvertible (Kuttera <i>et al.</i> , 2000; Sherekar <i>et al.</i> , 2011).
Copy attacks	The goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy (Huang and Wu, 2004).

2.6.5.2 Benchmarking

The results of experimental testing performed off benchmarks inform developers of watermarking algorithms. The developers require for the analysis and performance of the watermarking algorithm metrics with respect to different attacks. The benchmarking initiatives for image watermarking schemes can be elaborated through various benchmarking tools used for watermarking (Sherekar et al., 2008; Sherekar et al., 2011).

- **Stirmark**

Stirmark has been developed by Fabien Petitcolas at Cambridge University, UK. Since its first publication in 1997, Stirmark has gained large interest from the watermarking community and it is currently the most widely used benchmark suite for digital watermarking technologies. The Stirmark benchmark divides attacks into the following nine categories: signal enhancement, compression, scaling, cropping, shearing, rotation, linear transformations, other geometric transformations, and random geometric distortions. In the case of signal scaling, cropping, shearing, rotation, linear transformations, and other geometric transformations, the attacked images are obtained with and without a JPEG 90% quality factor compression. In order to produce a score relative to the benchmark, a score of 1 is assigned when

the watermark is decoded and 0 when it is not decoded. The average is then computed for each category, and the average of the results is computed to obtain an overall score. The benchmark should also average over several images. In order to ensure a fair comparison, Petitcolas (2001) suggests imposing a minimum PSNR of 38 dB for the watermarked image. However, this constraint is questionable since PSNR is not a meaningful measurement in the context of geometric distortions (Sherekar *et al.*, 2011).

- **Certification for watermarking techniques.**

For image watermarking, the best known benchmarking tools, Unzign and Stirmark, integrate a variety of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Stirmark introduces both global and local geometric distortions. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often rely on the use of either a transform-invariant domain (Fourier-Melline) or an additional template, or specially designed periodic watermarks whose auto covariance function (ACF) allows estimation of the geometric distortions. However, as discussed below, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is better resolved. However, resistance to the local random alterations integrated in Stirmark remains an open problem for most commercial watermarking tools. The so-called random bending attacks in Stirmark exploits the fact that the human visual system (HVS) is not sensitive to local shifts and engine modifications. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist this attack (Sherekar *et al.*, 2011).

- **Checkmark**

Checkmark is a benchmarking suite for digital watermarking technologies. Running on MATLAB under UNIX and Windows, it provides efficient and effective tools to evaluate and rate watermarking technologies. Checkmark contains some attacks, which are not present in Stirmark. It includes new classes of tests such as Wavelet compression (JPEG 2000 based on Jasper), Projective transformations, Modeling

of video distortions based on projective transformations, Warping, Copy, Template removal, De-noising (midpoint, trimmed mean, wiener filtering), De-noising followed by perceptual re-modulation, Non-linear line removal, Collage, and so on. In addition the following known test classes are re-programmed from Stirmark and included: Cropping, Flip, Rotation, Rotation-Scale, FMLR, sharpening, Gaussian filtering, Random bending, Linear transformations, Aspect ratio, Scale changes, Line removal, Color reduction, JPEG compression (Sherekar *et al.*, 2011).

- **Optimark**

Optimark is a benchmarking tool for image watermarking algorithms that was developed at the Artificial Intelligence and Information Analysis Laboratory at the Department of Informatics, Aristotle University of Thessaloniki, Greece. Its main features are as follows: Graphical user interface, Detection/decoding performance evaluation using multiple trials utilizing different watermarking keys and messages, Evaluation of the following detection performance metrics: For watermark detectors that provide a float output, i.e. the value of the test statistic used for detection. For watermark detectors that provide a binary output, i.e. a value that states whether the watermark has been detected or not: Evaluation of the following decoding performance metrics, for algorithms that allow for message encoding (multiple bit algorithms): Bit error rate, Percentage (probability) of perfectly decoded messages. Evaluation of the mean embedding and detection time. Evaluation of the algorithm payload (for multiple bit algorithms). Evaluation of the algorithm breakdown limit for a certain attack and a certain performance criterion, i.e., evaluation of the attack severity where algorithm performance exceeds (or falls below) a certain limit. Result summarization in multiple levels using a set of user-defined weights on the selected attacks and images. Option for both users defined and preset benchmarking sessions. Optimark was partially supported by EU Projects CERTIMARK & INSPECT. Optimark includes the following attacks: Cropping, Line and Column Removal, General Linear Transformation, Scaling, Shearing Horizontal Flip, Rotation, Rotation and Auto cropping, Rotation and Auto cropping and Auto scale Sharpening, Gaussian Filtering, Median, Jpeg, and so on (Sherekar *et al.*, 2011).

2.7 CLOUD WATERMARKING

Digital watermarking is a technology for ownership protection, which embeds the copyright information into digital production to avoid being tampered, peculated, and illegally copied (Johnson, Duric, Jajodia, & Memon, 2001). The main idea of watermarking is to introduce small images or patterns in the data to be watermarked without affecting the data subject to normal use. If an illegal copy occurs, the owner of the data can therefore get watermarks from the illegal data to verify his ownership of the data. Cloud watermarking is a digital watermarking technology based on cloud model, which has widely been applied in text and relation database (Li, 2004; Liu, Ma, Zhang, Li, & Chen, 2011).

2.7.1 Virtualisation in cloud

Tan and Ai (2011) illustrate that virtualization technology is a core technology of cloud computing, the virtual machine is the basic unit of the cloud computing platforms, cloud providers provided services to clients by virtual machines must ensure the security and isolation. Sometimes, however, because of the business needs, the virtual machine need communication with others, which destroys the isolation protection. The traffic between virtual machines is difficult to monitor, it will lead to malicious attacks between virtual machines when there exists a malicious virtual machine (Tan & Ai, 2011).

In virtualization technology, a hypervisor is a software program that manages multiple OS (or multiple instances of the same OS) on a single computer system. The hypervisor manages the system's processor, memory, and other resources to allocate what each OS requires. The hypervisor or VMM coordinates instructions between the guest and the host CPU. There are two types of hypervisors:

- Bare-Metal Hypervisor or Type 1 hypervisors are hypervisors that install directly on top of the physical server. Basically, it is a thin OS that controls the hardware, handles resource scheduling, and monitors the guest. Type 1 hypervisors are typically the preferred approach to virtualization because they deal directly with the hardware, so higher virtualization efficiency is achieved. Some examples of the type of hypervisor are VMware ESX, Citrix XenServer, and Microsoft Hyper-V (Tan & Ai, 2011).
- A hosted or Type 2 hypervisor is software that runs on top of an already installed standard OS environment, such as Linux or Windows. The guest OS runs at the

third level above the hardware. Examples of this type of environment are Parallels Workstation, Microsoft Virtual Server, VMware Server, and VMware Workstation. (Jasti, Shah, Nagaraj, and Pendse, 2010)

2.8 SUMMARY

Chapter 2 has responded to the three questions asked in 2.4 (Review Method) based on the systematic literature format. To answer the questions this chapter was divided into three main parts. The first part was Cloud computing and its privacy problems, that leads to the reason for choosing ownership protection as an under-developed topic in cloud privacy. A full analysis of how similar researchers tackle the ownership protection issue reveals one of the least researched topics in cloud privacy. In the second part, a brief scoping of watermarking capability has been evaluated as the main response to the gap. In the third part of this chapter 2, the relation between cloud computing and watermarking has been explained and clarified. Chapter 3 will now take up the concern of defining a suitable research methodology to explore the issues raised in chapter 2.

Chapter 3

Research Methodology

3.0 INTRODUCTION

Chapter 2 reviewed the literature that is relevant to Cloud privacy and specifically, ownership protection concerns, and identified researchable problems. The main problems affect both Cloud Service Providers (CSP) and Cloud Users (CUs) and requires solutions that give better efficiencies. Design Science (DS) has been chosen for the methodology for this research as its reliability for an information system investigation and artefact build is well-established. In this chapter the challenge of developing and selecting researchable questions to the problem is taken up. The task of developing an artefact is then facilitated by the DS methods and a plan made for building and evaluating the artifact.

In section 3.1 the outcomes of chapter 2 are brought forward to shape the context for the problem, the question development, and the hypothesis construction. In section 3.2 the research methodology is developed and justified. In section 3.3 the research design is elaborated in depth to identify ways to apply it and to answer the research question. Section 3.4 specifies the design evaluation and requirements. Section 3.5 evaluates the limitations of the research methodology. Section 3.6 forecasts the expected outcomes from the research. Chapter 4 then reports the findings of the first iteration of artefact building and the evaluation.

Contribution of Chapter 3	
Key Point	Page no.
3.1 Problem Review (RQ's & Hypothesis)	43
3.2 Research Methodology	46
3.3 Research Design	49
3.4 Design Evaluation Requirements	52
3.5 Research Methodology Limitations	64
3.6 Forecasted Research Outcomes	68

3.1 PROBLEM REVIEW

One of the important issues in cloud computing is user loss of control. The system architecture for services posits multiple layers of inter-related services for which no one supplier has control. Figure 3.1 shows the technical services stack (Tek, et al., 2010, p.684) and figure 3.2 the service architecture referred in the problem statement (Tek, et al., 2010, p.686). In the first instance, a user interacts with a sales agent (human or machine) to purchase the services opportunity. The sales agent may be selling on behalf of one or more service suppliers. In return these suppliers have supply agreements with many sub-service suppliers or brokers. Sub-service suppliers also have inter-related arrangements for services that may migrate data and service without notice (Lombardi and Di Pietro, 2011). The net result is that a cloud service user may not know the storage and processing place or places of the data and may not be assured of ownership protection. Hence, the consequences are for security, privacy and legal jurisdiction. The essence of cloud computing is that a user entrusts their own digital information to a second party who exploits multiple third parties to deliver the user a service.

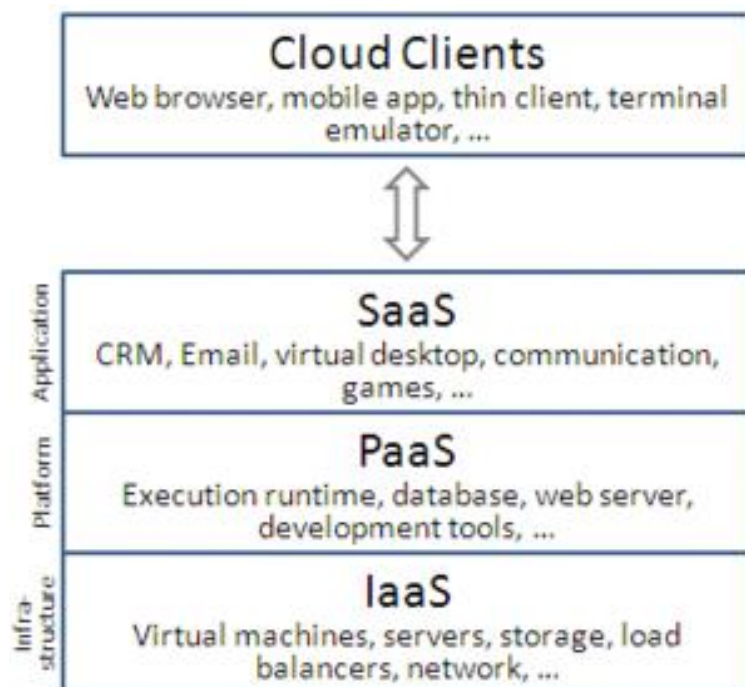


Figure 3.1: Cloud Computing Services (Based on: Tek, et al., 2010; Mel and Grace, 2011)

The user has technology and information, which are hosted in the cloud by the provider, and the services to store information, to create further information, and to transact business that are made available by the provider. Inevitably, the protection of ownership rights is an issue and the many related vulnerabilities require risk treatment in a secure service system (O'Ruanaidh, 1996; Cayre, 2005).

The results from Chapter 2 literature review shows a substantial gap for ownership protection in the cloud. The problem is addressed by reviewing the potential of watermarks to protect rightful ownership and to place the responsibility for that protection with the service provider. Another example of the service users losing control is the scope of service level agreements (SLAs) and the enforceability between cloud providers (Lombardi and Di Pietro, 2011).

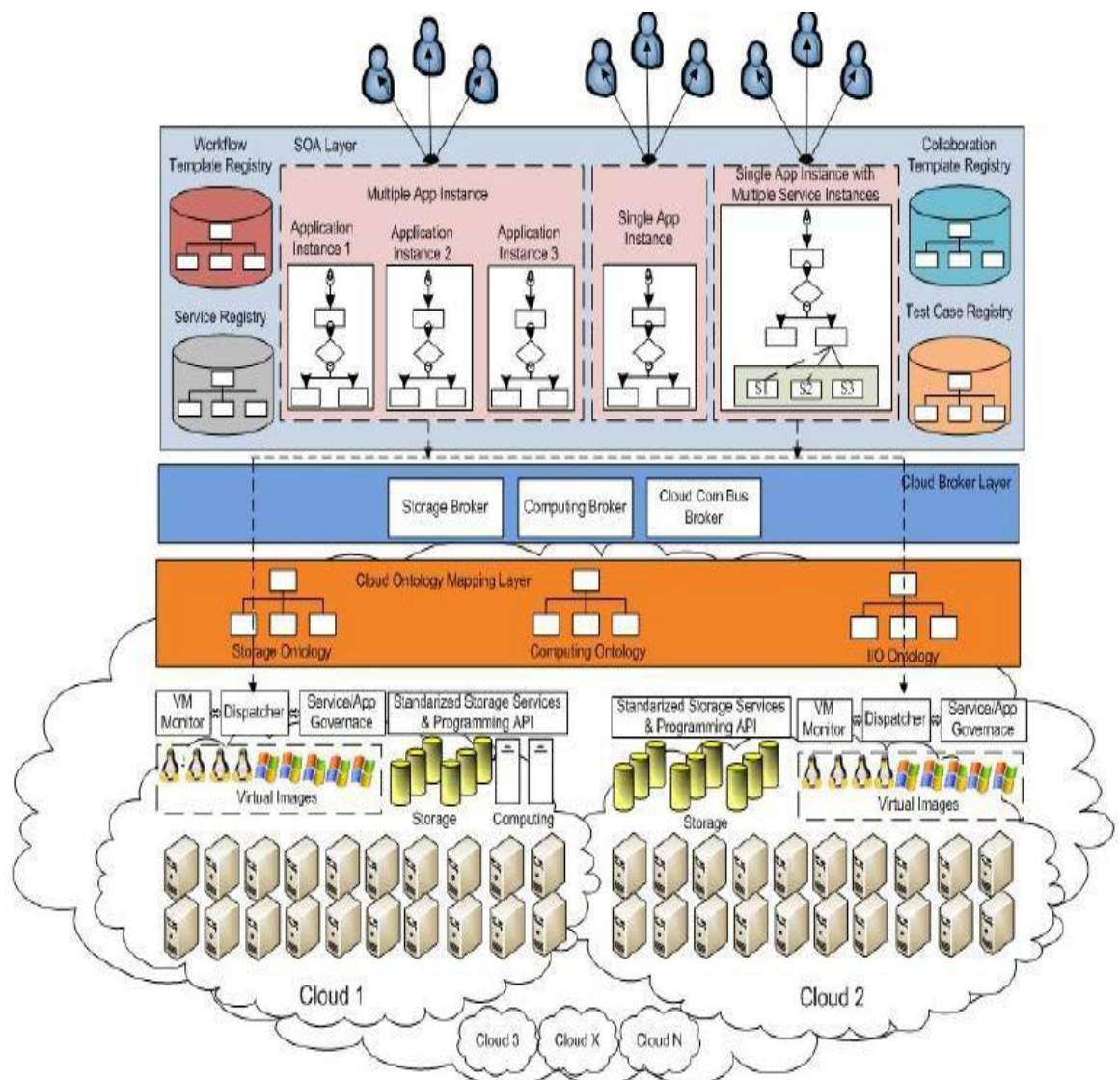


Figure 3.2: Cloud Service Architecture (Tek, et al., 2010, p.686)

Security of Cloud computing has been enhanced in many ways, and improved with for example with watermarking. Watermarking is a technology for copyright protection that mitigates illegally copying or tampered. It introduces small patterns in the digital data signal without changing the original source. If there is a breach of the original data then, the rightful owner can verify the ownership of that data (Liu et al., 2011). It is used to protect visibly or invisibly the ownership of artefacts such as images, audios and, videos. Currently there are many software packages available for users to insert digital watermarks in their media.

The substantial problem is that the user insertion of watermarks may have variable impact on the problem of verifying rightful ownership (Sherekar, 2008). The cloud environment is a torrid environment in which there are many possible attacks that may be on account of unintentional management of the data or intentional attacks on the data. The variation introduced by many different user watermarking tools can be reduced by requiring cloud service providers to insert watermarks.

The problem of, partial solution transfers responsibility to the service provider, is to have a robust and consistent capability for watermarking. Consequently, a secure information management service by a provider is required to test and prove watermarks' robustness to the environment in which the service is provided. Users applying generic watermark tools may not have the capability to anticipate the scope of attacks a property may be subjected and the management practices of multiple third parties. Hence, the innovation in this research is an advocacy for an architecture where the responsibility is with the service provider. The design solution is a tool design for provider information security management. This chapter is focused on a methodology selection that can demonstrate a design solution and justification to the problem.

The Research Questions

The aim of the study is to find a way for enhancing the ownership protection in the cloud by using appropriate watermarking methods on image files in a cloud environment. First, the appropriate method needs to be identified and tested. Second is to implement the method by using it in a cloud environment.

The research questions are as follows:

- i. What preparation methods improve ownership protection in cloud environments?
- ii. What could be a suitable management framework to increase ownership protection in a cloud environment?
- iii. What tests show the reliability of the proposed method in a cloud environment?

The Hypotheses

Three hypotheses were also developed to be tested as part of this study; these hypotheses are assertions derived from the literature reviewed in section 2.3.

- i. The DWT method in the transform domain is the most resilient and robust for the cloud environment.
- ii. The proposed novel artefact provides strong ownership protection.
- iii. The proposed Authentication method improves rightful ownership protection in a cloud environment.

These hypotheses are to be tested by collecting two sets of data: one from scenario tests on a selection of current frameworks; and, two on the new artefact to be developed from theory. The tests are to confirm (or otherwise) the validity of the gap identified in the literature review; and, the full scenario tests the validity (or otherwise) of the new artefact.

3.2 RESEARCH METHODOLOGY

Design Science (DS) is an organising framework and philosophy for making and building artefacts. It has been made relevant to Information Systems (IS) research as a methodology and the framework to IS security has been applied (Hevner, et al., 2004; Nunamaker, et al., 1990; Goes, 2014). The benefit of the approach is that an artefact may be investigated in context and the artefact improved through continuous iterations and testing (Pretorius, D., *et al.*, 2016). The purpose of the DS research methodology is not only to develop an artefact but also to answer research questions. Depending on the characteristics and the goals of the research, a researcher can shape

the processes to deliver innovative or confirmatory outcomes (Johannesson and Perjons, 2014). The DS research methodology consists of six main phases: problem identification and motivation, define the objectives for a solution, design and development, demonstration, evaluation and communication as it is shown in figure 3.3.

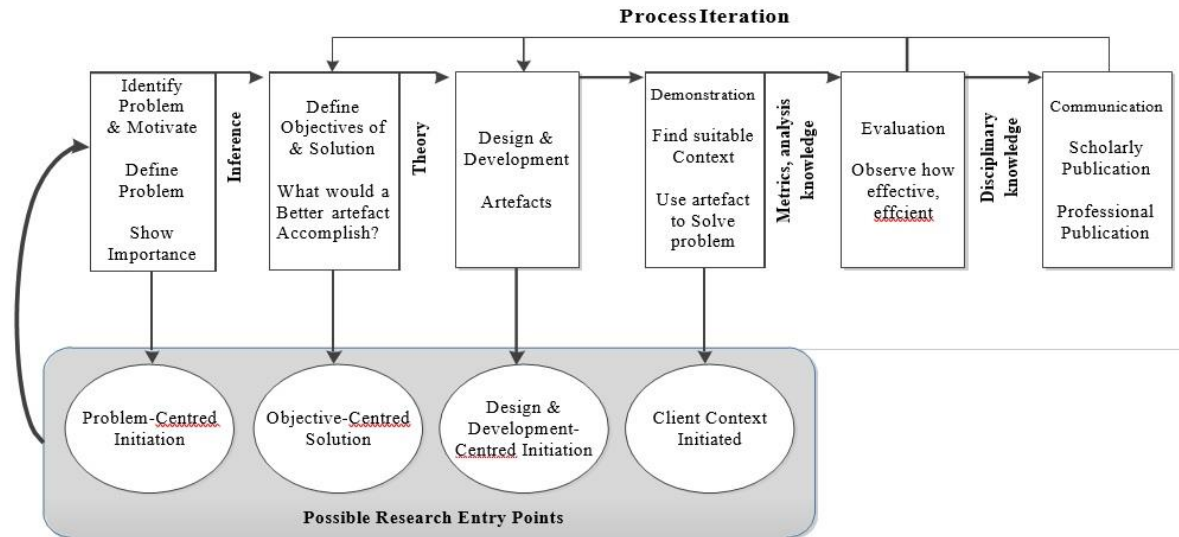


Figure 3.3: DS research methodology (Peffers, et al., 2007, p.54)

DS is solution oriented whereas the other research methodology such as Natural Science or Social Science, are problem oriented (Hevner and Chatterjee, 2010). Figure 3.3 shows four entry points for starting research and six phases that are linked by output loops and feedback loops (Thakurta, R., *et al.*, 2017). The consequence is that any action that is taken is balanced by evaluation and the outcome of the evaluation can deliver forward propagation to the next phase or a return to an earlier phase for improvement. The first four phases also offer the option of returning to the entry specification for improvement and then re-entry to the phases. Phases 5 and 6 have process iteration options for quality improvement that offer alternative pathways depending on the researcher objectives and intended delivery standard.

In this research the six phases in figure 3.3 are adopted as:

1. Identify the Problem
2. Define the Solution
3. Design and Develop the Artefact
4. Demonstrate in Context
5. Evaluate the Solution
6. Communicate the Story

Design Science is chosen for this study because it is solution oriented and not problem oriented. The problem specification in the Introduction and the literature analysed shows that the problem has two components. One technical and one managerial (Simonsohn, U., *et al.*, 2017). DS focuses on the creation process and refining of the artefact to get a working solution. The purpose of this study is to develop a solution for assuring the rightful ownership of a property in a cloud environment. According to Offermann, et al., (2009, p.2), design science refers to “an explicitly organised, rational and wholly systematic approach to design; not just the utilisation of scientific knowledge of artefacts”. Therefore, the solution defined is in two parts; one that addresses a requirement for information security and the other for an information security management design.

The design and development of the artefact concerns the technical solution for a robust watermark. The scope of the current research is to subject the solution to five attacks that represent information management policies in the Cloud. The two components of the solution are dependant whereby the managerial design solution solves the problem of user variation and the problem of watermark failure on account of user capability. The technical watermark artefact development is a proposed solution to technical failure. It has a reasoned layering of protection from information management attacks and a further scope for Cloud technical attacks. A server side rightful detection tool requires that every file coming to the server is assessed for consistency with the criteria for a robust watermark in the cloud environment. Any incoming file not meeting the requirement is then deleted and replaced by a service provider one. In this proposed research a context and a scope is selected that is feasible for testing. The scope of watermark research is narrowed to image media; JPG format; invisible perceptivity; robust requirements; image type; frequency domain processing; DWT format; and, private information for extraction. To satisfy the scope ten files were subjected to attack. The ten images were chosen as the cover objects for watermarks and were publicly available for free download. The scoping of the testing allowed the information management attacks of resizing, cropping, format change, text manipulation and flipping. Each of these attacks was chosen to represent standard policies applied by Cloud providers rather than for any complex malicious attacks that may exist in the cloud. Once attacked and entered into the cloud database the images were extracted and tested for responsiveness to the

original key and consistency against the original watermark. The PSNR scale was used for measuring the extracted watermark signal strength. The benchmark of less than 30 decibels is selected from the literature as a spoiled watermark (Oligeri et al., 2011).

The scope of the testing is to demonstrate the artefact in action in a simulated Cloud environment and in the context of information management attack. The simulation consisted of the artefact, the service provider policies, the information management attacks, a Cloud database, the embedding and extraction algorithms, and a PSNR measurement tool. As a consequence the demonstration provides a confirmation of the expectations an intellectual property owner may have for rightful ownership protection in similar circumstances. The evaluation is guided by the scope of the testing outlined here and cannot be generalised to matters outside of this scope. The final phase defined is the communication of the research findings and story. The phase is completed in the reporting of the results below and any other publications that may arise (Gregor and Hevner, 2013).

3.3 RESEARCH DESIGN

The research problem is about issues in cloud computing privacy and ownership protection. It is important to understand how problems happen and answer questions related to a researchable part of the problem. Designing a robust copyright protection artefact can be possible, if there is an understanding about attacks in the cloud and also of watermarked preparation. Figure 3.4 outlines the three phases that the implementation section part of the research will go through.

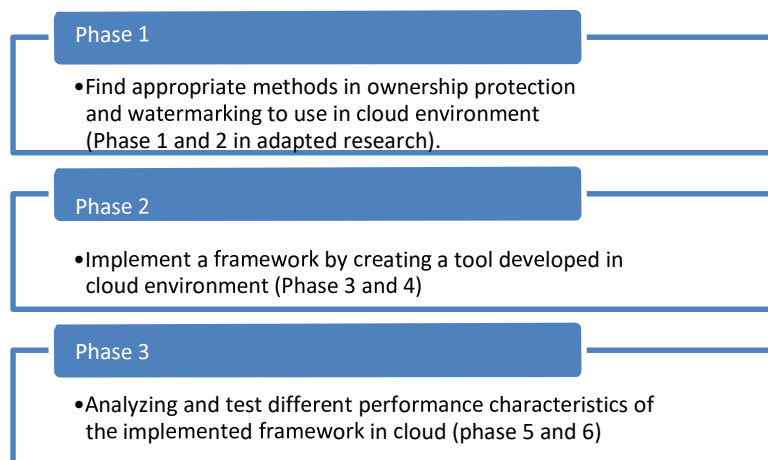


Figure 3.4: Research Stages

Phase one will find the most resilient and robust watermarking method to be used in cloud environment for ownership protection purposes. The second and the most important phase of this research is the design and implementation of a unique artefact that can result in a good solution to improve the copyright protection in a cloud environment. The research artefact will have a unique three-way Image authentication technique. It will be tested in a SaaS (Software as a Service) cloud environment. The artefact along with a research diagram of the implementation phase (Phase 2) will be explained in the rest of this section. Phase three will focus on the testing and evaluating of the implemented artefact to make sure that the proposed solution is the most practical one, and aligns with the theoretical expectations.

The research process will follow the advocated Design Science Methodology to build and be guided by the detailed steps involved. The research objective will be explored as a knowledge question (Wieringa, 2010), and each phase as stated above will be treated as an artefact and be put through rigorous testing cycles within the problem domain to generate the most effective outcome and solution (Hevner, 2007).

3.3.1 Research Design Steps

Figure 3.5 illustrates the research design according to the design science methodology. There are three phases in this research project, an output for each phase must be found before the next phase, for example ‘An appropriate watermarking method for image and ownership protection’ result must be successfully completed before moving to Phase 2. This phase will be conducted and compare all potential watermarking techniques to be used in cloud environment with the purpose of finding the more robust and resilience method. Only then the research would move to the second phase and start developing the artefact as a result of the gathered information from phase 1 and being capable of ‘Implementing the artefact in a virtualised environment as a cloud’. This will then continue with a complete analysis and report of the artefact based on the adopted methodology.

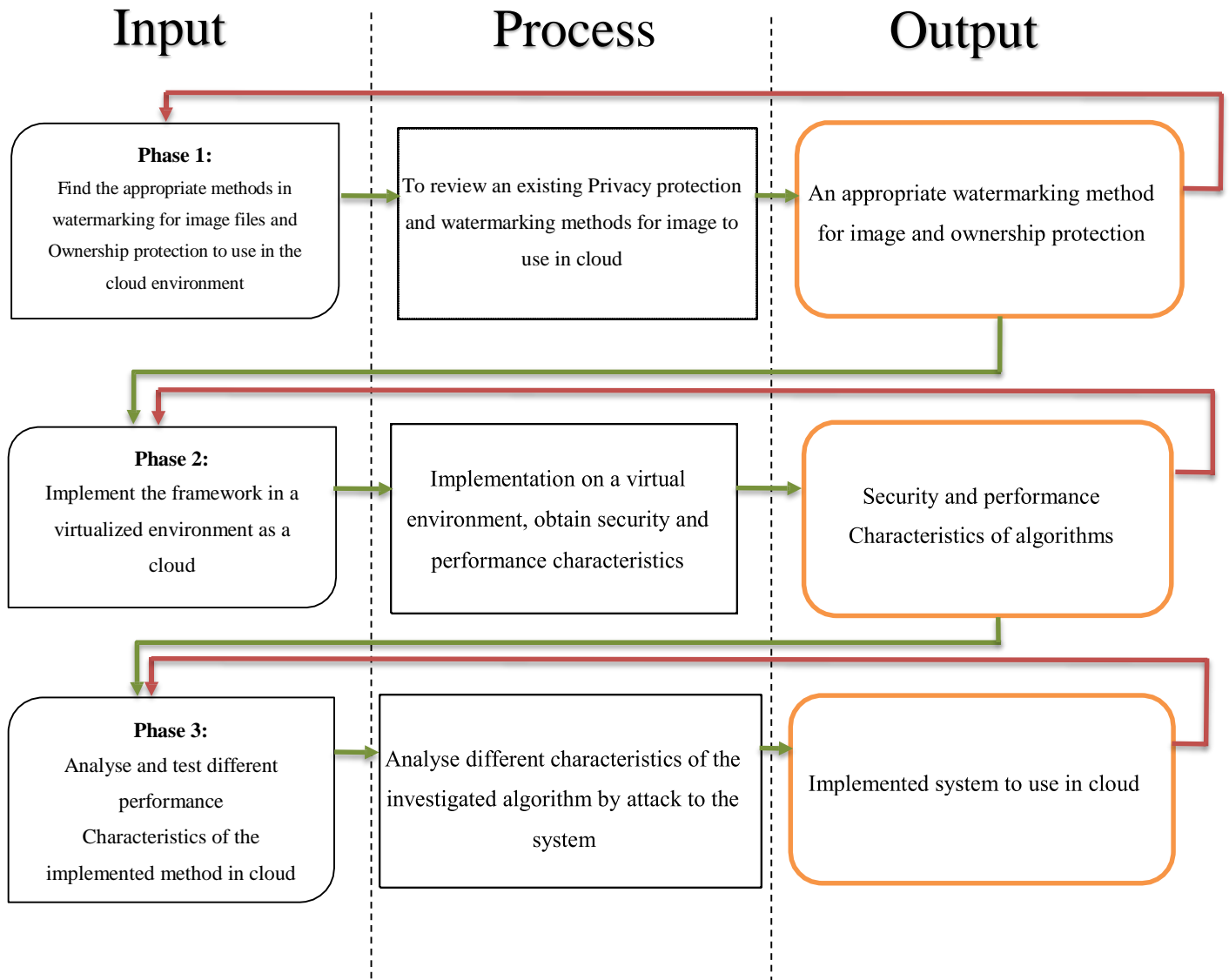


Figure 3.5: Research design

Figure 3. 5 shows the processes that each phase of this study must go through. The figure has been modified from the existing design science methodology examples to suit the purpose of this particular field study. Each phase must produce an acceptable output in order to go to the next phase. As shown in the flow of Figure 3.5 the Green arrows navigates to the next step successfully, the red arrows however show repetitive efforts to repeat the ‘Rigor Cycle’ if the output result is rejected and unacceptable (Hevner, 2007).

3.4 DESIGN EVALUATION REQUIREMENTS

The DS methodology requires data to evaluate the artifact in various aspects. It allows for a continuous improvement of the artefacts by going through sequences of revisions. It is planned to complete two evaluation cycles in the time available and to deliver recommendations for further improvement. DS does not provide a true or perfect outcome but rather it delivers utility value and quality improvement recommendations for further development and research.

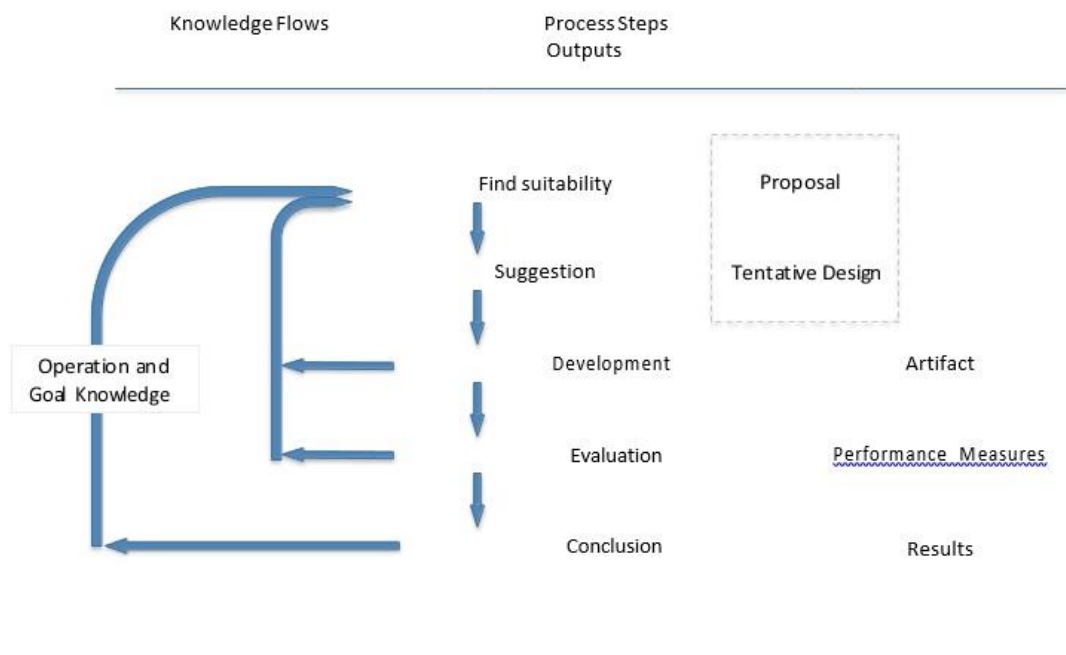


Figure 3.6: Modified design Science methodology diagram displaying process for each phase of this research (Vaishnavi & Kuechler, 2004)

It is feasible to complete two evaluation cycles in the time available for this research, and to deliver recommendations for further improvement of the artefact is future research. In this work a prototype is to be built in order to gain the evaluation feedback that is both statistical and natural (expert opinion) in nature. DS does not provide a true or perfect outcome but rather it delivers utility value and quality improvement recommendations for further development and research. The DS methodology requires data to evaluate the artifact in various aspects and relies on rigour and evaluation. The chosen evaluation methods has been elaborated in 3.4.1.

3.4.1 Data Collection Methods

Data will be collected from two different sources: Expert opinion evaluations of the produced artefacts and the statistical results from testing the artefact in the real cloud environment. Experts' feedback will be gained from participants from experts in the same field of research from the same industries. Also University experts will be consulted for feedback in compliance with section 6 of the AUT ethics criteria.

3.4.1.1 Experts Evaluation

The evaluation phase of DS based research is vital to assess the produced artefacts, as it has been outlined in sub-section 3.4.1. According to Peffers et al. (2012) experts' evaluation that utilises 'logical arguments' is part of the evaluation method classifications, where artefacts are evaluated by one or more experts. It is anticipated that the evaluation method is driven by the type and nature of artefacts (Peffers et al., 2012). Alturki et al. (2011a) point out the importance of preparation of functional specifications, metrics or criteria to evaluate the various aspects of the developed artefacts. According to March & Smith (1995) metrics should be defined before commencing the evaluation, as they play vital role in the evaluation process. Alturki et al. (2011a) indicate that attention should be paid, when selecting an environment and experts to evaluate the artefacts, to ensure quality evaluation is conducted by stakeholders who might be impacted by the future use of the design solution.

Experts' feedback evaluation is planned to take place in two stages (Internal/Artificial and External/Naturalistic) (Venable, 2006; Alturki et al., 2011a; Ostrowski & Helfert, 2012). The first stage is to be conducted by 2-3 practitioners from within the university to obtain initial assessment of the designed artefact; analyse the data gathered at that stage and make any adjustment to the design, if required. That would involve asking the Experts for opinion about the designed. The second stage will be repeated with another 2-3 Experts, to test the artefacts in the real environment, excluding the first practitioners involved in the initial evaluation. Similar data gathering and analysis procedures will be followed.

According to Mantelaers (1997) selected Experts must have many years of relevant experience in the field, in order to be acknowledged as an expert in the field. The Researcher has carefully examined the background of the nominated Experts in order to obtain creditable evaluation of the developed artefacts. Mantelaers (1997) indicates the importance of knowledge elicitation in gathering expert opinion and to

use various possible ways, so that data will be perspective driven. It can be analysed and modelled, to form practical guidelines to address the identified problem. However eliciting Expert opinion cannot be observed directly, according to Wijers (1991, as cited in Mantelaers, 1997) who points out the challenges of data gathering from Experts, and outlines some types of data gathering. For example: written and oral feedback, are the most common methods, as the methods encourages experts to outline their explanation, and make clarification. In addition, protocols such as ‘Think Aloud’ and ‘Introspection’ can be utilised to obtain Expert views on problem solving, and thinking about artificial problems. Those protocols have pros and cons, but can be utilised to gather quality data from the Experts, when the cons are mitigated.

- **Expert Evaluation Criteria**

As it has been discussed in section 3.4.1, two kinds of evaluation will be carried out (Venable, 2006; Alturki et al., 2011a; Ostrowski & Helfert, 2012). Artefacts evaluation criteria based on a system approach derived by Prat et al. (2014) as noted in Table 4.3 are to be used with the criteria and possible questions devised by the researcher.

Table 3.1: Expert Evaluation Criteria

System dimensions	Evaluation criteria	Sub-criteria	Questions
Goal	Efficacy		How effective do you think the proposed system would be in the real commercial world in case of the ownership protection?
	Validity		<p>Q1: Are the defined sections are relevant to what you observe?</p> <p>Q2: Are the provided metrics adequate and helpful to determine relevantmitigating measures?</p> <p>Q3: Is the provided strategies’ payoff guidance realistic and adequate?</p>

Environment	Consistency with people	Utility	Do you think RODS is effective and efficient in determining the rightful ownership?
		Understand-ability	Q.1 How easy it was to use the RODS, and was there any difficulty in using it? Q2.How long did it take you to go through each step from registration to watermarking?
		Ease of use	Usability and ease of operation?
	Consistency with organisation	Utility	Does the designed system has the potential to be widely adopted?
Activity (Dynamic, the operations and functionality of the artefact)	Completeness		Q1. What area of improvement - you can think of? Please list as many as possible Q2.Strengths and weaknesses of the system? Q3. How long did it take you to go through each step from registration to watermarking?

3.4.1.2 Statistical Results Evaluation

This section will rely on the outcome of the developed artefact in the real world cloud environment. The results will show the level of robustness for the created artefact and the practicality of it in the real environment. The methods, which has been used to examine the artefact has been elaborated in research progress phase 3 of the artefact development.

3.4.2 Developed Artefact

Development of the artifact has been divided into three phases, starting with finding the appropriate methods for watermarking to be used in the cloud (section 3.4.2.1), followed by implementation of the artefact. This has been introduced in section 3.4.2.2 and implemented and developed in the chapter 4. The artefact is then reported with the analysis and developmental decision-making.

3.4.2.1 Find appropriate methods for watermarking to use in cloud environment (Phase1)

According to the first objective of this research, appropriate methods for privacy protection and watermarking within a cloud environment will be investigated. For this purpose, appropriate methods in ownership detection and privacy protection will be investigated and the applicable ones chosen. Image Authentication is selected for the research as it is feasible and easy to work with. For this purpose, there are so many ways available to authenticate an image, but these matters need to be examined and tested in relation to using them in a cloud environment. Some of the methods are using a cryptographic algorithm for image authentication by using hash functions or a RSA algorithm. These methods have been used in different environments such as Neural Networks. Figure 3.7 shows relevant watermarking methods.

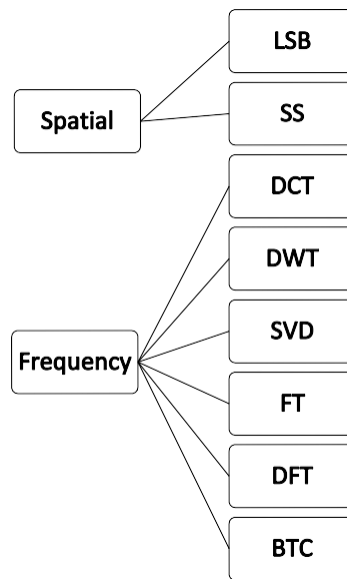


Figure 3.7: Some of the watermarking methods related to the research

In this research, according to the first objective, an investigation of the available image authentication methods will be done and the suitable ones which have the ability to be used in the cloud environment will be identified. Second, the most reliable watermarking algorithm to use in the cloud environment will be identified. The main problem of the spatial domain is that the methods are not sufficiently robust. Robustness is very important during implementation in the cloud

environment to assure the resilience of the watermark. Comparatively, frequency domain methods provide more robustness that is more suitable to be used in the cloud environment. The frequency domain methods: Singular Value Decomposition (SVD) and Distributed Wavelet Transformation (DWT) are more appropriate for robust image watermarking and also in copyright protection. The SVD technique enhances the robustness of the watermark against geometric and non-geometric attacks and can also be used for image watermarking. Another sufficient robust method for image watermarking, in digital image file formats is DWT. DWT is a method, which is used for frequency domain techniques.

The research analysed for this project in chapter 2 commonly shows these watermarking methods being performed on the client side. For example a cover image on a user file can be tampered or even destroyed. One of the causes is the noise existent through the network. This problem can be solved by transferring the file from the client to the server side securely and then conducting the watermarking procedure on the cloud server instead.

There are safe methods for transferring the watermarked image by sending it through a channel such as the SSL protocol, or select cryptography algorithms. Watermarking by using the DWT method can be done on the server side and it can be implemented by a virtualized environment provider or Cloud service providers like Amazon Web Services (AWS) or Microsoft Azure. Figure 3.8 illustrates a modified example of the potential virtual environment for implementation. This figure shows an architecture for any cloud service provider from the provider side as well as the customer side. The added components shows, where in the cloud environment, this research could fit and be implemented. The components such as the artefact developed system for watermarking check will be placed in the cloud side and the images in this scenario will be transferred through a secure channel for more reliability. Amazon Web Services (AWS) has been illustrated in figure 3.8 as a potential platform service. Each of these components will be shown, discussed and explained in detail in the following phases in this chapter.

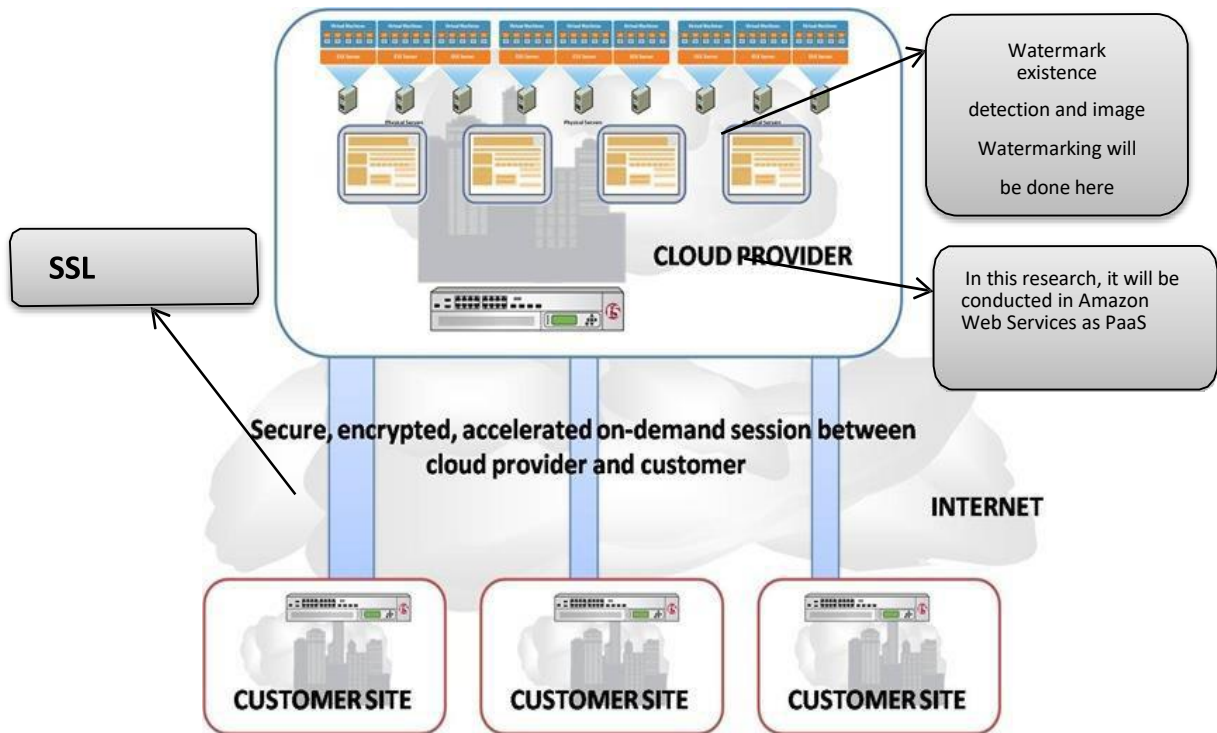


Figure 3.8: Illustration of the cloud environment focused on the research goal

3.4.2.2 Implement the artefact in a virtualized environment as a cloud (Phase2)

Implementation artefact will be divided into three sections. First, the Image and its features will be uploaded to the cloud server for further processing. Second, the uploaded image will be checked to be authorized according to the proposed artefact, which will be found the rightful ownership detection system to use in the cloud environment. This section will be divided into three steps for authenticate the uploaded image. Watermark Existence Check (WECH), Hash Existence Check (HECH) and Image Similarity Check (ISCH). These will be the three steps of authenticating an image. ISCH is a unique technique which will be used in this research regarding the image similarity check and is a significant contribution to knowledge.

The first and most important part in this section is checking whether the incoming image from the client is watermarked before or not. The cloud server database will check the received file and if the received file has been watermarked before the image file will be blocked for further process, but if it was a genuine file,

it will be sent to the next level for compression and watermarking. The second step will check the hash of each image with existing ones in the cloud server database to check whether the hash of the uploaded image is exist in the database or not. If a similar hash has been found, the image will be block to continue, otherwise the image will be directed to the next level of authentication. The third step and the most important one is ISCH system, which will check the image by a unique image authentication system. ISCH will check the image after the two other authentication steps and before the image is authorised for the watermarking step. The ISCH step is designed and elaborated in the implementation section.

For the next step the uploaded image will be redirected to the watermarking processes after passing the authentication steps and authorized to be watermarked as a new image to system. In this section, the image will be watermarked by the 3 phase method demonstrated. The DWT method will then be used to watermark the image to a cloud database.

3.4.2.3 Implementation Diagram

According to the investigated methods, Figure 3.9 shows the phase 2 implementation steps. In this diagram, the process of uploading an image to the cloud database, the feature extraction and image authentication parts; and the last step, which is watermarking the authorized image, has been shown.

The Fixed Password, Dynamic Password and Hash are the three-way unique features that will be used for the watermarks. The Fixed password is the set of users' personal information such as their name, last name and ID, which have been gathered from users during the registration process in a cloud environment. The information has been encrypted and stored in the cloud database for reference. The Dynamic Password includes a unique one time password which will be sent to users as a temporary authentication code. Users have to enter the temporary code for the first time before their images are authenticated for the first time. The final step is that a Hash code will be captured from the original image and will be used as one of the three-dimensional features for watermarking. These three-dimensional features have been simplified and called CFDH (Cloud FixPassword, DynamicPassword and Hash) for this research.

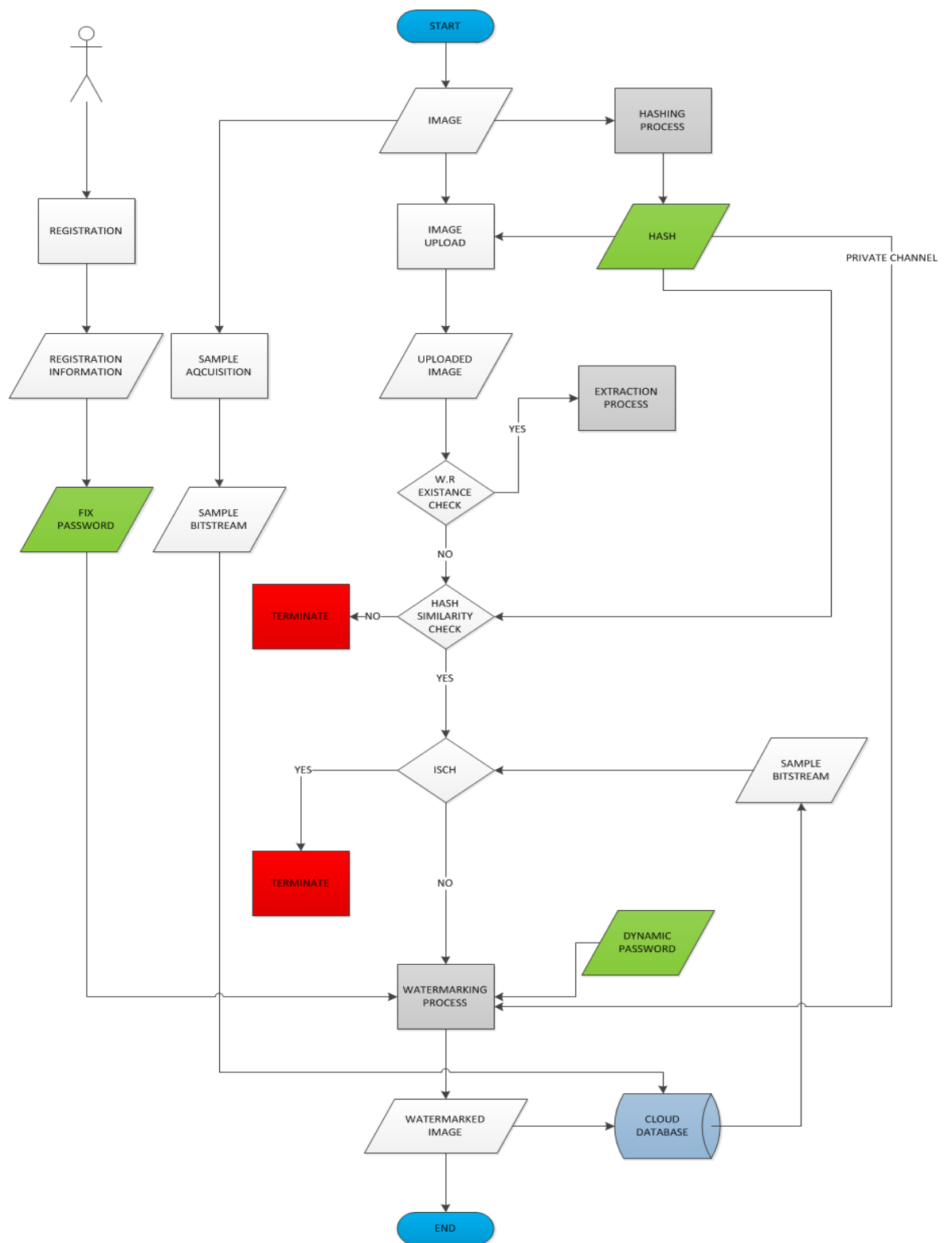


Figure 3.9: Implementation Diagram

As it has been shown in Figure 3.9, before a file is verified as a genuine image, it has to pass through the authentication process. First, it will be checked for any

watermark existence. If the picture has been watermarked before, the image information will be fetched from the database and if the image is not found and belonging to the person who claims it, system will reject the image being watermark again and store the user's information as a suspicious user. If the image passes the watermark check, it will be checked for hash similarity and if it also pass the hash check, then it will be directed to ISCH.

Every image can be easily tampered by just a simple cropping or scaling attack. If so, the hash code will be changed and also the watermark can be destroyed or damaged, but, ISCH is a unique technique for this research that will check the uploaded image and can recognise if the image already exists in the cloud database or not, and also it will be able to show the similarity percentage of the uploaded image and the existent one in the database. If the Image successfully passes the authentication steps, then it will be watermarked and stored in the cloud database and will be recognised with the ownership of the certified person who has uploaded it.

3.4.2.4 Analysing and testing different performance characteristics of the watermark method in the virtualized cloud (Phase3)

In this study, chosen appropriate method for finding the rightful ownership protection in a cloud environment has been evaluated to improve the integrity of the CIA triangle according to the use of ownership protection and increasing the protection in virtualized cloud environment.

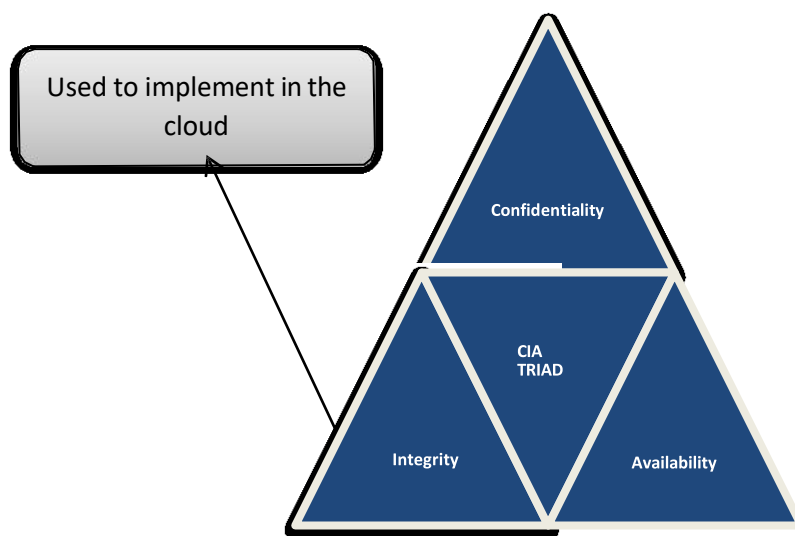


Figure 3.10: CIA Triad

To analyse and test the performance of the evaluated method in a cloud environment, the ownership detection system will be checked and benchmarked, whether it is working properly according to the integrity in the design and implement section. For this purpose, testing and evaluation will be with standard methods. For instance, the watermarking step will be evaluated with Peak Signal-to-noise Ratio (PSNR) for quality comparison.

3.4.2.5 Proposed Artefact

The proposed artefact developed in this research and in comparison with the previous proposed frameworks in the related work should give a better ownership control for cloud service providers. It is aimed to provide more reliability for cloud customers using the cloud services as an important technological service. To avoid a weak and vulnerable link in the enterprise security, rightful ownership system must be established in all the components in the infrastructure of cloud systems. This requires establishing a wide and useful system, which should be placed in every cloud service provider systems. The novelty lies in the fact that the proposed artefact has not been offered by anybody else in cloud environment yet. Combining watermarking, image authentication and cloud computing can contribute to security and privacy. The literature review shows that this artefact has not been proposed so far. The key point of difference is that the cloud service providers taking responsibility for the robust insertion of their users data by using the developed artefact. The developed artefact system is responsible to shift the process from the client side- which has been done before and still has lots of vulnerability and variation between users that prevent a secure cloud environment. The developed artefact system then, will process the factors on the server side of the cloud environment by using the techniques developed here.

Cloud Computing users can use rightful ownership detection system to upload their data without thinking about compromising of their data ownership. Since a combination of three stage image authentication and watermarking has been used in the rightful ownership detection system, this makes the system more powerful to detect the suspected image uploading. In comparison with the related works, the essential goal of the proposed artefact is to provide rightful ownership detection, which makes it:

- Authenticate cloud users, under the specific cloud provider user privacy policies.
- Ensure protection of cloud users' private data by keeping their rightful ownership.

Figure 3.11 shows the process of sending uploaded images to the cloud server by using multiple channels. Here the original image will be send through a public channel. Also, the original image, and our unique features will be sending through a private channel. While the original image is distributed freely. The original image may be tampered maliciously during the transfer, which is the purpose of the procedures to make sure that the image has not been tampered during the transfer, before it goes for the next step. Beyond these objectives, the main contribution of the work is the ownership protection and implementing it in a Cloud environment. Figure 3.11 illustrates the proposed artefact and highlights the details of transferring images from users to cloud servers, also the process of authenticating the image until the last step, which is the watermarking of the image. This table will be elaborated in more detail in a later chapter.

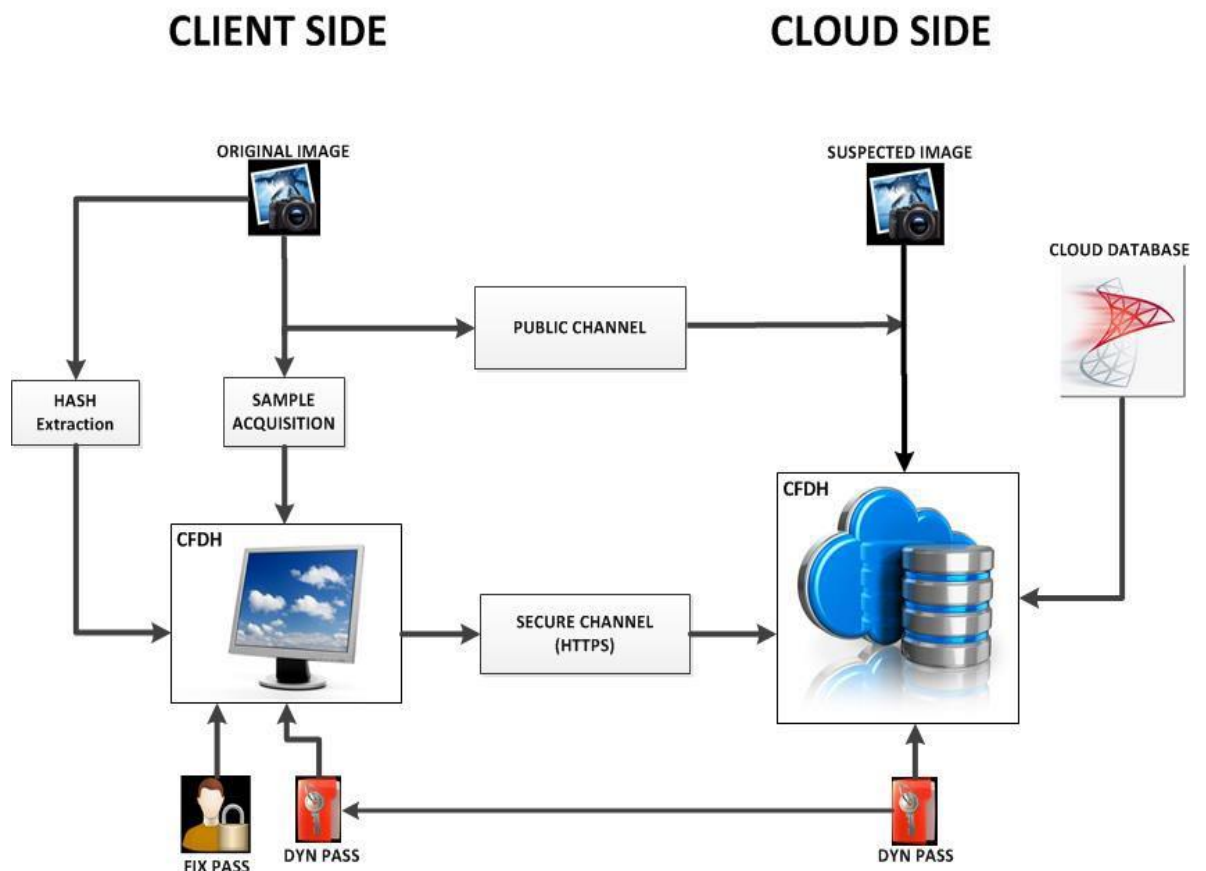


Figure 3.11: Proposed Artefact Architecture

3.5 RESEARCH METHODOLOGY LIMITATIONS

The selected method for this research has been designed to provide reliability, and a means to collect and to analyse data. The findings will lead to answering the research questions and finding a solution to the research problem. However, Berndtsson et al. (2008, p. 56) claim that “a method is only valid and reliable within a certain range of uses”. As with any research methodology, the selected DS methodology has limitations (Oates, 2006; Hevner et al., 2004; Vaishnav & Kuechler, 2008). Hevner & Chatterjee, (2008); and, Oates, (2006) indicate it is difficult to differentiate between DS research versus professional design. In addition, Oates (2006, p. 122) points out a number of disadvantages that a DS researcher could face, such as: “it could be challenging to prove it is an innovative outcome; it can be difficult to generalise the research outcomes to a wider setting; a researcher needs to have necessary technical and/or artistic skills; being enthusiastic is not enough; and, the research outcomes could be invalidated by rapidly evolving technologies that could render the artefacts inapplicable and/or obsolete”.

Trauth (1997) indicates that qualitative methods, while they have their strengths, they also have some limitations and issues that could hinder the research effort. For example, the education of IS professionals involved in the research (Trauth, 1997). In another words, the educational background and experience level of the selected Expert opinion to evaluate the research artefacts, would evidently present a level of discrepancy from one expert view to another.

This section discusses those limitations, their potential impacts on the research and viable mitigating measures to reduce the impact to a manageable level. A reasoned explanation is provided. Sub-section 3.5.1 explores Reliability, while sub-section 3.5.2 examines Validity, and lastly, sub-section 3.5.3 discusses Generalisation.

3.5.1 Reliability

Reliability is the accuracy of the selected research method in measuring or developing a proposed model. In another words, how adequate is the method in meeting the planned research objectives (Berndtsson et al., 2008). Another definition

of reliability is, according to Collis & Hussey (2009, p. 64) “refers to the absence of differences in the results if the research were repeated”. In other words, if another party attempts to conduct the same research, would they get similar results? A view shared by Trauth (1997) who emphasises the importance of being able to produce trustworthy results and institute meaningful findings and of interest to the audience. Most importantly, the results can be re-produced, should another researcher attempts to conduct and follow the same research procedure. The level of liability influences the decision of whether to trust the findings of the research or not, and/or would another use the proposed research methodology in conducting similar research.

Yin (1984) and Simones (2009) recommend documenting the research procedure so that it can be re-performed again following the same steps that have been done in the first run. The aim is to minimise the errors and biases in a study, argue both authors. In the same way Trauth, (1997) suggests that being aware of this issue would aid a researcher to put that into perspective to limit the impact. In addition, the author suggests, recording the researcher’s introspective reflection along with interviews and observational data.

Collis and Hussey (2009) claim that reliability mostly concerns positivist studies, while under the interpretive paradigm reliability is of little importance. The same authors, further add “The qualitative measures do not need to be reliable in the positivist sense”. While this research is designed to be conducted under DS paradigm, and as indicated, the collected data are qualitative data via qualitative data gathering means. Trauth (1997) indicates that qualitative methods, while they have their strengths, however, they have some limitations and issues that could hinder the research effort. For example, the education of IS professionals involved in the research (Trauth, 1997). In another words, the educational background and experience level of the selected Expert opinion to evaluate the research artefacts, would evidently present a level of discrepancy from one expert’s view to another. The DS three processes devised by (Hevner et al., 2004) see figure 3.3 along with the repetitive aspect of the processes provides self-detection and enables researchers applying necessary changes when necessary. Furthermore, the framework developed by Peffers et al. (2007) based on the Hevner et al. (2004) guidelines, would ensure an adequate documentation of the research procedures as the research progresses.

This would provide another cycle of assurance to mitigate the outlined limitations concerning validity and reliability.

Testing will be performed using quasi-judicial method, where a rational argument is used to interpret the data see section 3.5.2. Collis and Hussey (2009) indicate that for interpreting qualitative data, defined procedures and protocol would ensure authenticated results. Erikson & Kovalainen, (2008) have a similar view on the need for high reliability for quantitative data, but not so much for qualitative data. In this research the design has been argued and documented at all levels, as demonstrated in the research design section. Further details on coding and the thematic approach to be adopted to ensure all details are captured are given and can be followed, if required. The researcher believes that this measure is viable and would mitigate the risk inherent in this type of limitation.

3.5.2 Validity

According to Berndtsson et al., (2008, p. 56) validity is the relationship between what a researcher intends to measure or develop and what it is actually measured or developed. Validity is of a particular concern for qualitative researchers. Collis & Hussey (2009, p. 65) defines validity as “the extent to which the research findings accurately reflect the phenomena under study”. In other words, how accurate the findings and the drawn conclusions of what have been investigated are and what evidence have been provided to ascertain the results (Erikson & Kovalainen, 2008). Construct validation is a term used that is of importance to business research. Collis and Hussey (2008) indicate that validity is demonstrated in an interpretive paradigm analysing qualitative data, and the positivist paradigm has to have a high reliability to reproduce similar results. Kvale, (1996, p. 238) shares the same view stating that “qualitative research can, in principle, lead to valid scientific knowledge”. In line with that DS based research utilising qualitative means would utilise the strength of qualitative data gathering and analyses and manage the weaknesses to an acceptable level, without jeopardising the research objectives.

Yin (1984) refers to this limitation as construct validation and indicates that there is a high level of ‘subjectivity’ in data collection. A view shared by Berndtsson et al., (2008), who also refers to subjectivity in, conducting interviews, preparing surveys and questionnaires and analysing the data. In the same way according to Trauth (1997), one important aspect of any qualitative research project is the

‘subjectivity’ of the Expert opinions. When they evaluate the artefacts and provide their feedback subjectivity is involved. Also the researcher’s view would play a part, as the researcher would be conducting the interaction, transcribing and analysing the data. However, Simons (2009) argued that in qualitative research, subjectivity is not a negative thing. In addition, subjectivity cannot be totally eliminated. Trauth (1997) claims that in qualitative research, it can never be completely objective and judgment free, although reducing the subjectivity level would help in gaining more credibility in the research results. To reduce its impact, a form of triangulation can be used, that collects various forms of data from different resources and cross checking the outcomes (Yin, 1984). Trauth (1997) refers to triangulation of the collected data, which can be utilised to build confidence in the interpretation and understanding of any anomalies, should any discrepancy occur. The researcher’s observation of the research participants reactions, plays a part in triangulating collected data should any contradiction be witnessed and/or data be collected through others means.

In this research data collection methods have been stated, that should help in triangulation of the collected data. Trauth, (1997) suggests that being aware of the existing issue of subjectivity would aid a researcher to put that into perspective when gathering and analysing the data. However, as it is only the researcher who works on the research, there will be a level of subjectivity in analysing and justifying the outcomes. The researcher should endeavour to provide as much evidence as possible to ascertain the inferred conclusions.

3.5.3 Generalisation

Generalisation, or external validity in the Yin (1984) definition, is the ability to apply the research findings into a wider setting. While generalisation has been recognised as a limitation in any research, Oates (2006, p. 122) highlights a number of difficulties in DS based research and refers to the generalisation limitation as “it can be difficult to generalise settings from the use of an IT artefact in a single situation”. With the results of DS research conducted in a specific context, once evaluated and its applicability is approved, then another project could take place to generalise the research outcomes into a wider context (Hevner & Chatterjee, 2010). Evaluating applicability is of high importance in DS based research. In addition, key objectives of DS based research are, developing innovative artefacts, which would comprise

valuable utility, and adding new knowledge, that would help a better understanding of the complex domain.

In addition, similar critiques of other types of research are made. For example case studies are helpful. Yin (1984) refers to critics on how possible it is to generalise findings of one case study to the universe. Yin (1984) argues that the critics are inadequate as they implicitly make analogy to survey research. Survey research is based on statistical generalisation, while case study research is based on analytical generalisation. According to Kvale, (1996, p. 233) analytical generalisation “involves a reasoned judgment about the extent to which the findings from one study can be used as guide to might occur in another situation”.

Generalisation, however, does not take place automatically, argues (Yin, 1984, p. 44) and asserts that “a theory must be tested through replication of the findings in a second or even a third neighbourhood”, or another setting. That highlights the importance of communicating the research outcomes in meaningful ways (Hevner et al., 2004; Hevner & Chatterjee, 2010). The communication of research, which is the last guideline, see Figure 4.5. Hevner et al. (2004) emphasise the importance of presenting the outcomes to both technical and management audiences. The level of technical details provided would enable practitioners to re-evaluate the outcomes, extend the scope and replicate in different settings, which would facilitate generalisation of the research. As this research is following the DS guidelines (Hevner et al., 2004) evaluating the adherence to the outlined activities of DS framework, would ensure the research objectives are met and the design mitigates the impact of the limitation.

3.6 FORECASTED RESEARCH OUTCOMES

By conducting this research – the researcher aims at finding quality improvement solutions to a difficult problem. The aim of this research is to address and analyse the ever more prominent data privacy concern that each individual must now face as a cloud user. It will investigate the gap between current ownership protection tools and techniques and find a suitable rightful ownership protection method which has the ability and consistency to use in a cloud environment. At present, cloud service providers use many different security methods to protect data but they are less concerned with privacy and ownership issues. Most of the cloud service providers

ask their users to sign a privacy agreement, which tells the users that they are responsible for the data they upload in the cloud and not the service provider.

The goal of this research is to propose an artefact to find a Rightful Ownership protection system based on the problem statement and problem background. The first objective is to investigate the existing privacy protection methods and watermarking methods which have the ability to be used in cloud environments. The second objective is to propose an artefact that has a rightful ownership protection system that will increase ownership protection for information artefacts in cloud environments. The proposed artefact is to be tested in a test cloud environment by preparing and passing watermarks through the cloud and then evaluating them for performance. Finally, the last objective is to evaluate the proposed artefact for its ability to resist attacks and return the identification of ownership protection.

As there are many of such recognised settings, and they continue to increase, defining selection criteria would be paramount to ensuring a selected artefact would return the best business value. Further research is required into many aspects of this project and the DS methodology can manage the challenges. It is anticipated that new knowledge will be generated about constructing effective protection, process improvement and the challenges facing the user and cloud service provider acceptability of the proposed design solution.

3.7 CONCLUSION

This chapter 3 has specified a feasible research methodology that can be applied to solving the problems involved with Cloud privacy and specifically the ownership protection concerns that have been identified from the literature analysis. The choice of the methodology has been made so that the problem can be explored as an open-ended problem and solutions develop as the research progresses. It also allows naturalistic feedback loops that can complement the statistical analysis of the proposed water marking system for cloud environments. The research phases and process steps have been defined, and what is critical for DS research methodology is that the evaluation requirements have been clearly specified. Chapter 4 will now report the artefact design and implementation. A large part of this research is building the artefact so that it is functional and working in software. What will then follow is the testing and evaluation phases.

Chapter 4

Artefact Design and Implementation

4.0 INTRODUCTION

In Chapter 3, the research methodology based on the Design Science (DS) has been defined and justified as a suitable approach to achieve the research objectives. The research methodology has been described in detail based on the DS guidelines. In Chapter 3, it has been also argued that developing an interactive system, will enable the researcher to find an answer to the research questions. The proposed artefact will go through the design and evaluation phases of detailed testing. This chapter will focus on the design of the artefact and elaborate the design processes of the artefact and its development (all the build code can be found in Appendix B). The chapter 5 will concentrate on the evaluation of the proposed artefact from both the statistical and the naturalistic perspectives.

The first step in designing software is our requirement analysis and there are preparatory activities that need to be done before designing the algorithm. This research will be conducted using an experimental and modeling approach. It will begin with in-depth reading to understand the state of the art in the areas of cloud computing ownership protection. One of the main requirements of the study is a flow diagram of cloud ownership protection. Some of the best techniques have been analysed and discussed in the analysis of related works (Section 2.6). The advantages and disadvantages of those works were discussed. Therefore it seems that there are still open issues that are required research (section 2.7). Based on the chapter 2 literature review, a Novel ownership protection artefact in the cloud environment has been proposed. It is a combination of watermarking based on the DWT algorithm and a novel image authentication method to secure the rightful ownership. The aim is to make a seamless copyright protected mechanism for the cloud environment.

This chapter is structured as follows: in section 4.1 the artefact design process is elaborated, and the artefact implementation processes is presented in section 4.2. In section 4.3 the development of the artefact from the system requirement point of view is specified. Finally the chapter will be concluded with a

summary of value in section 4.4.

4.1 ARTEFACT DESIGN

The proposed artefact, in comparison with the previously proposed models in the related work, should give a better ownership control for cloud service providers. This will occur, to provide more reliance for cloud users in using the cloud services as an important technological service. To avoid a weak and vulnerable link in enterprise security, a rightful ownership system must be established in all the components in the infrastructure of cloud systems. This requires establishing a useful system, which should be placed in every cloud service provider system. The novelty lies in the fact that the proposed artefact has performance advantages and is yet to be tested for robust features. Combining watermarking, image authentication and cloud computing can add value to security and privacy in cloud computing. The artefact gives innovation and has potential value for cloud service suppliers.

Cloud Computing users can use a rightful ownership detection system to upload their data without concern about compromising their data ownership. Since a combination of three stages of image authentication and watermarking has been used in the rightful ownership detection system. This makes the system more capable to detect an image uploading. Moreover, using a one-time password and AES256 cryptographic algorithm as secure tools in the authentication systems reduces vulnerability of the other proposed works.

In comparison with the related works, the essential goal of the proposed artefact is to provide rightful ownership detection, which makes it:

- Authenticate cloud users, under the specific cloud provider user privacy policies.
- Ensure protection of cloud users' private data by keeping their rightful ownership.

The proposed scenario is in Figure 4.1. This figure shows the process of sending an uploaded image to the cloud server by using multiple channels. Here the original image will be send through a public channel. Also, the original image, and the unique features will be sent through a private channel. While the original image is distributed freely, it may be tampered maliciously during the transfer. The purpose

of the development is to make sure that the image has not been tampered during the transfer, or before it goes for the next step.

Beyond these objectives, the main contribution of the work is the ownership protection and transferring responsibility from the client side to the cloud service side in any cloud service. At present many clients use many different watermarking tools to protect their intellectual properties. The variability of the tools is a problem and also their performance in the different cloud environments. The proposal is to transfer the responsibility for watermarking to the service supplier and hence they have an obligation to select and prove software that is robust in their environment and service contracts. In order to achieve this objective figure 4.1 elaborates the scenario. Central to the scenario is the secure transfer of knowledge and also the embedding of a singular service side watermark that has the potential to protect the rightful ownership of the intellectual property entrusted into the cloud. Such a scenario can enhance end user client side confidence in the services provided. This can be invaluable to service suppliers because once the end user confidence increases then the patronage should be in proportion.

The artefact design is elaborated by scenarios in figure 4.1. The design portrays the shifting of responsibilities but also the requirement of security processes and mechanisms to assure the rightful owner can be identified by the watermark. The literature analysis in chapter 2 showed that there was a serious gap in knowledge around the responsibilities for secure watermarking in the cloud environment. The research analysis has shown that by shifting responsibility a major performance issue can be addressed. Consequently the systems design arose from the literature analysis and reflects the possibilities that were found in the reading. The architecture has been developed for a seamless transfer of responsibility and the audit of service suppliers for compliance against standards. In section 4. 2 the security processes and mechanisms are defined and elaborated in relation to figure 4.1 and with sufficient detail that the artefact can be constructed. Figure 3.9 illustrated the proposed artefact flowchart and highlighted the details of transferring the image for users to cloud servers, also the process of authenticating the image until the last step, which is the watermarking of the image, is explained in section 4.2.3.

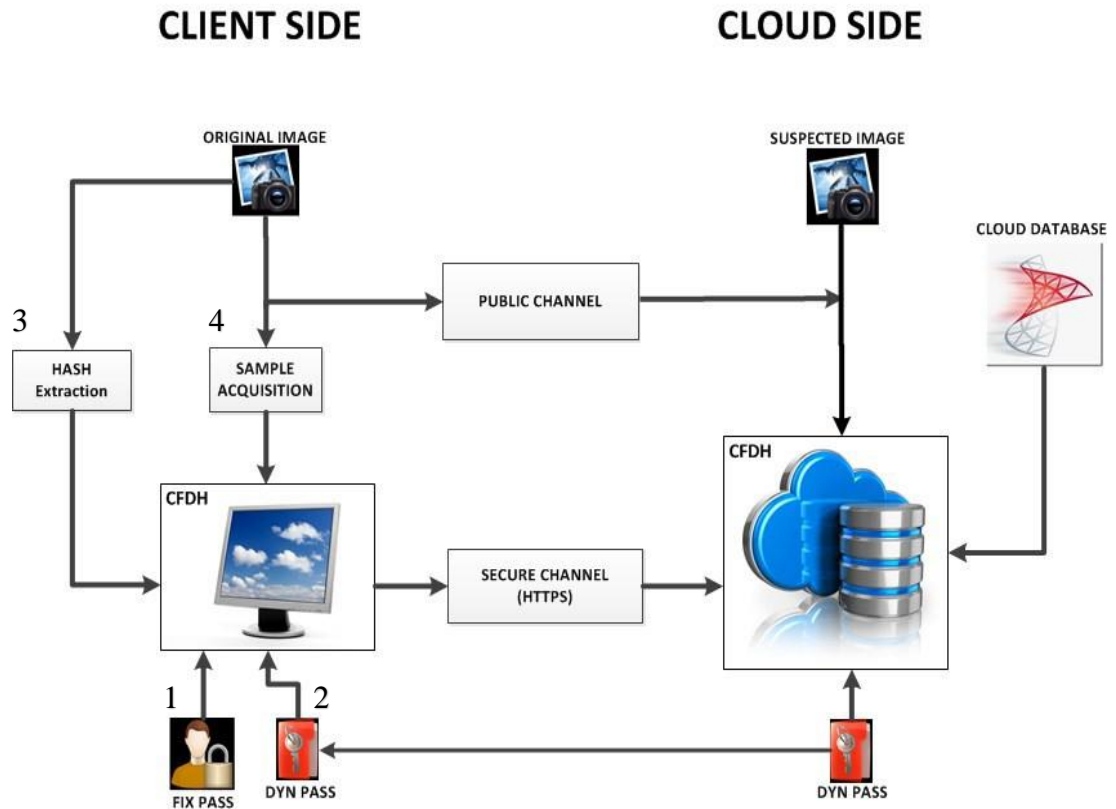


Figure 4.1: Proposed Artefact Architecture Explained

Figure 4.1, illustrates the design of the proposed artefact, repeating Figure 3.9 in Chapter 3 in more detail, which has shown the implementation flow chart of the same artefact in detail. In this design, CFDH (defined in section 3.4.2.3) as well as the sample image, will be collected from the image and the user information. The equivalent of each feature has been highlighted in figure 4.1 by a number 1-4. CFDH will be extracted and sent to the cloud side through a secured channel. The result including the original image as in hexadecimal code and its unique hash code will be stored in a cloud server database for further processing. The original image on the other hand, can be sent through a public channel. Using a hexadecimal format to store the uploaded image makes the process of fetching less time consuming and also more reliable to divide the image bits for comparing to the other images for the purpose of recognising the tampered parts (section 4.5). The Implementation processes of the designed artefact will be explained in section 4.2.

4.2 PROCESSES FOR IMPLEMENTING ARTEFACT DESIGN

The artefact architecture has been illustrated in section 4.1. This section will describe the implementation of the artefact design in detail. The watermark artefact has three principle components; the embedding algorithm (section 4.2.1), the extraction algorithm (section 4.2.2) and the three security features (section 4.2.3).

4.2.1 Embedding Algorithm

The preparation algorithm is integrated with the development of the security features and the management context so that once the security features are stable then the embedding algorithm can add these features to the image as a watermark. Together the three features formed the basis of the artefact. The preparation algorithm also provides the link between the technical and management components of the solution. In the first decision of the flow diagram (figure 4.2) a determination of the status of the incoming image is made to address the issue of user watermarks verses service provider watermarks. The embedding process must consider the three channels of red, blue and green that form the basis of image colour. By frequency blue is chosen first (a lower frequency signal) to enact the embedding process pixel by pixel (number 1). Red and green then follow to pick up the extra payload of a watermark (Number 2, 3). The byte streams then have been combined and prepared to be embedded into the image (Number 4-6).

The final embedding process will be shown in figure 4.18, with the details of the use of each channel. Section 4.2.2 will describe the feature extraction as the next step towards the final watermark identification.

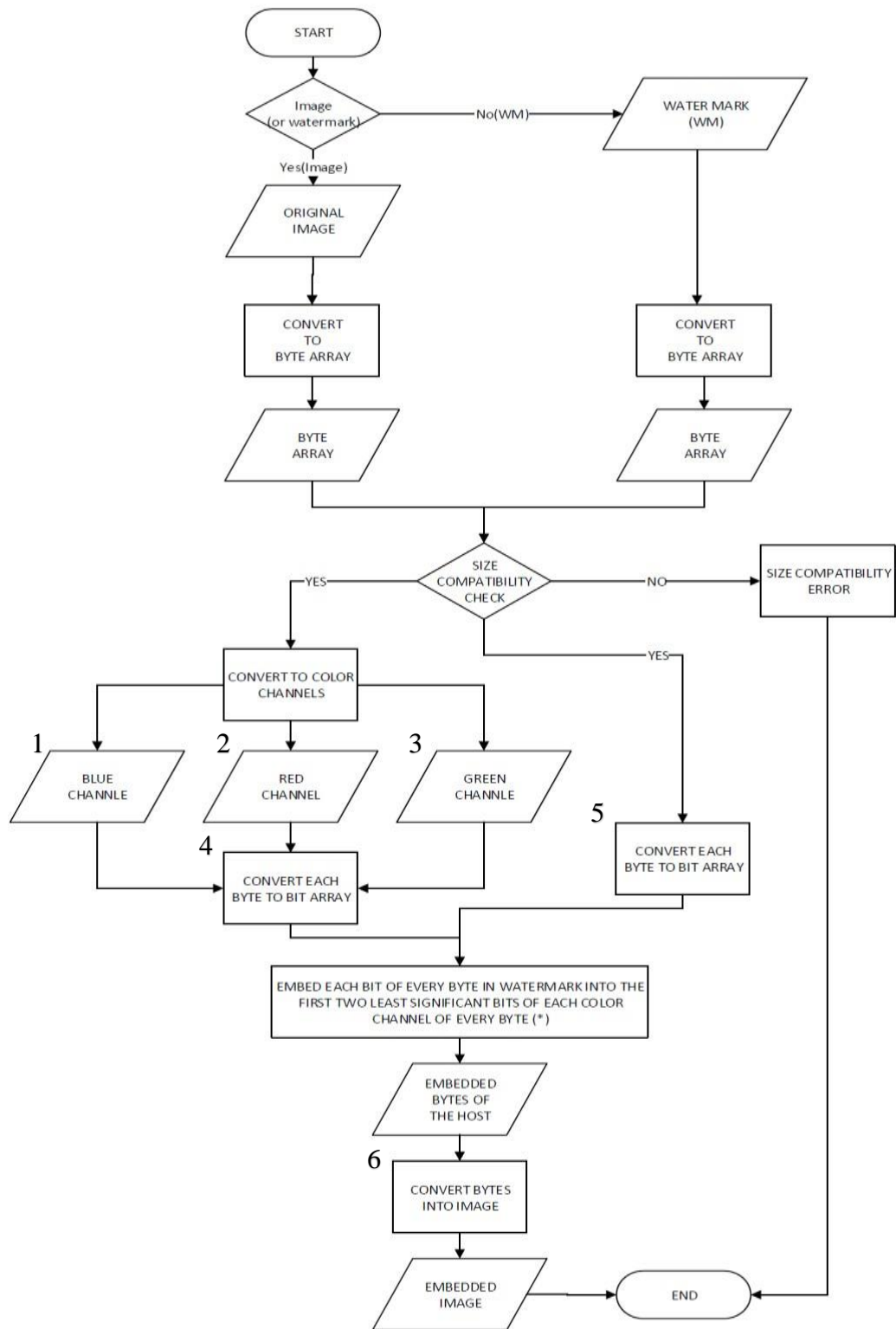


Figure 4.2: Preparation Flow Chart

4.2.2 Feature Extraction Process

Second part of the proposed scenario is feature extraction. In this stage, three important factors will be extracted as our features, which are the combination of a Fix Password, Dynamic (DYN) password and Hash function in the cloud and is called CFDH in this research. The output of the step will be send through a secure channel to the cloud for further processes in cloud servers. The following paragraphs have the specific detail of the extraction of each feature. In 4.2.2.1 a smaller sample of the image will be taken to be sent to the cloud database (Figure 4.1, number 4), then the other three features will be extracted as explained in 4.2.2 and illustrated in Figure 4.1, numbers 1 to 3.

4.2.2.1 Sample Acquisition

In this step, a copy of the original image as a sample will be taken and the following steps will be proceed for use on the sample:

- The sample image format will be changed into bitmap (. bmp) from any input format type.
- The sample image will be resized to 120 * 80 pixels.
- Every 4 bits of the sample image will be taken to send and store in the cloud database as one of the extracted features for ISCH.

Every sample image is an input to the system, with any format, it should be changed into bitmap format and the sample is to be resized to a specific dimension for the ISCH phase, ISCH is one the most important and unique step of the innovation compared with other research in the image authentication area which has been pointed in related works. It is done with the purpose of comparing all existing images with specific and unique rules, which will be applied to all images in a same way.

4.2.2.2 Fix Password Acquisition

As illustrated in figure 4.1, one of the other items of the feature extraction part, is the extraction of the fixed password belong to the authorised user who wants to upload the specific image. Every cloud user has their own fix password, which has been inserted in the registration form beside the other options like user name, cell phone number and Email address, during the sign up process. This

password will be inserted into the system in the authenticating process (Figure 4.1, Number 1) and it will be kept and saved as one the three dimensional features of CFDH in this research. Although, the latest single password techniques has been adopted and used for the design, but there are still some vulnerabilities of using a password alone. The Internet, built for resilience and information sharing, included the idea of an ID / password security, but used to not provide encryption to protect the password and allowed infinite retries to get it right. As a result, passwords are usually transmitted unprotected, and may be sent with every page that needs access to a password protected area as well as allowing the attacker all the time the site is up to try and crack it.

4.2.2.3 DYN Password Request

DYN Password is one of the other features, which will be made for each user in each transaction of image uploading. DYN Password is a 6 digit random number, which will be produced from the cloud server for three minutes in each transaction. Having a better integrity of data transaction is the purpose of using a DYN Password. In this research and the idea of using the DYN Password has been taken from the One Time Password, as defined in the literature review.

4.2.2.4 Hash Extraction

Each image has a unique hash, which is sensitive to any manipulation or modification. In this research, the extracted and stored image hash, is one of the features of CFDH. MD5 algorithm and has been used for hashing extraction format. It has more reliability, is less time consuming to produce an extraction, and also is more secure in comparison to the other available hashing functions.

4.2.3 Image Authentication Process

After sending the image and its features to the cloud server side, the uploaded image should pass through three integrity-testing steps, which are Watermarked Existence Checking, Hash Existence Checking and ISCH sequentially. Each of the listed steps will be explained in the following subsections.

4.2.3.1 Watermark Existence Check (WECH)

Here the watermark signal must be detected and then tested for damage. The extracted watermark is evaluated against the input watermark for the purpose of

testing. In the real world the evaluation would simply be against signal strength for tampering detection and against the security features for authentication. In a way the rightful ownership may be determined and with reference to a signature database. The first step of checking the incoming image from the user is to see whether the image has been watermarked with the watermarking system or not. Hence it checks the PSNR of the incoming image to check the watermark existence in the image. Firstly, if the image PSNR is not coming up with a number, it indicates that the image has been tampered or watermarked before. Secondly, the system will try to extract the image watermark with the watermarking algorithm. Number 2 in Figure 4.3 illustrates this step. Number 3, decision making indicates if the watermark has been done with RODS or not.

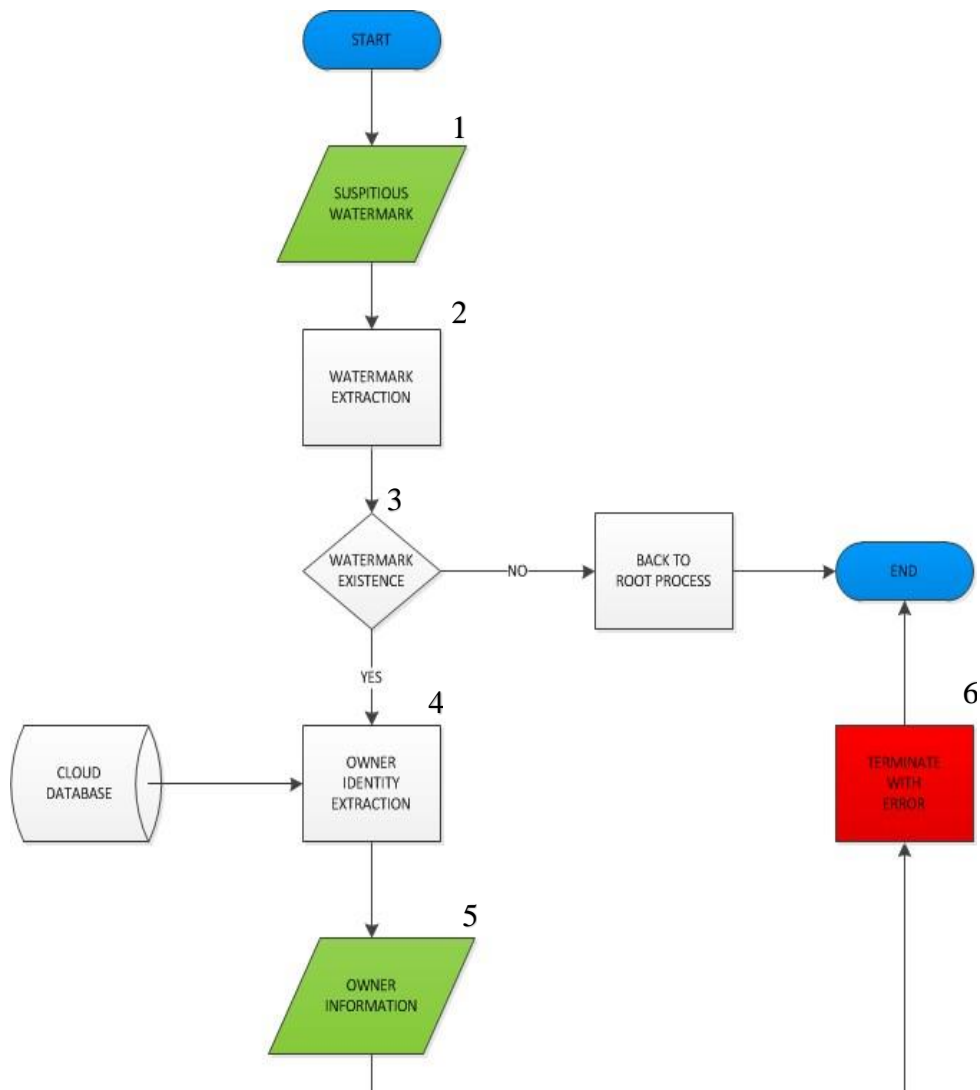


Figure 4.3: Watermark extraction process

If the system could extract the watermark from the image (figure 4.2, Number 5), then there is a binary code of the features, which has been embedded into the image before, but, if the watermark could not be found within RODS, the system will go to the end of the process and terminate with an error showing the suspected tampered watermark (figure 4.2, number 6). Finally the extracted binary code stream will be reversed to the SHA512 and also features can be extracted to find out the real owner of the uploaded image (figure 4.2, number 5). At the end, our suspicious user process will be terminated with an error and the program will be terminated. The watermark extraction process has been shown in Figure 4.3.

4.2.3.2 Image Similarity Checking

The Hashing function is not reliable enough for image authentication, because if any tiny change happens to the image during the transfer or any attack happen to the image. This makes the image pixels change a bit, the hash will be changed completely and image cannot be recognised in cloud servers as an existing one.

The ISCH step is the most important step because of its uniqueness in detecting the tampered images and reliability of the RODS to it, If the system fails to detect the manipulation in other steps. After the Hashing Check step, if the image could not be recognized by the system, the system will redirect to the secondary image authentication, which is ISCH. In this step, the uploaded image samples, which have been taken from the image during the upload, will be checked with the whole existing samples in the cloud database. If any similarity could be found between the sampled pixels in database images and the uploaded image sample pixels, the similarity percentage will be calculated and shown. The following Table 4.1 shows the logical process of calculating the similarity between an uploaded image and existing ones, if there is any.

Table 4.1: Similarity Process between uploaded image and existence image Pseudo Code

Start
For each image in the list of
images Define a
string array
Fill up the defined array with bit stream of each
image Define a counter with content of zero
For i from zero to 9600,
increase i one unit If any
similar bit in bit streams
Increase counter one digit
End if
If similarity is equal or larger than 500
Add the name of each founded image into
a cmb box
End
if End for
End for
End.

In this code, samples, which are $120 * 80$ pixels or 9600 bits, be compared with the similar samples in the database and the results will be shown in a box to choose and see the similarity results. Further information will be explained of the ISCH process in section 4.3.4 and the code is available in Appendix 2.

One of the other important steps of the image authentication and ISCH is that, after ISCH has been done, if any similarity found between data in the cloud server database and the uploaded image. Sample point is also used to take pixels

from the images as samples, and to check that they are not similar to each other. They will be graphically boxed and shown as a differentiation. More information about differentiation recognition will be explained in section 4.3.4.

4.2.3.3 Watermark Embedding Process

Watermark embedding step is the last step of image uploading process. In this stage, after the system made sure that the uploaded image has not been compromised during the transfer, and it could not be found in the database during the image authentication steps (Hash Checking and ISCH), the features will be combined together with the SHA512 cryptographic algorithm format. Then, a bit stream (binary code) of the hash function will be taken as a message, which wants to be watermarked to the uploaded images as a cover. The reason of using the bit stream of the token hash is that, the embedding of a bit stream of zero and ones is much faster and less time consuming in the watermarking process. The process of embedding the features, has been illustrated in figure 4.4.

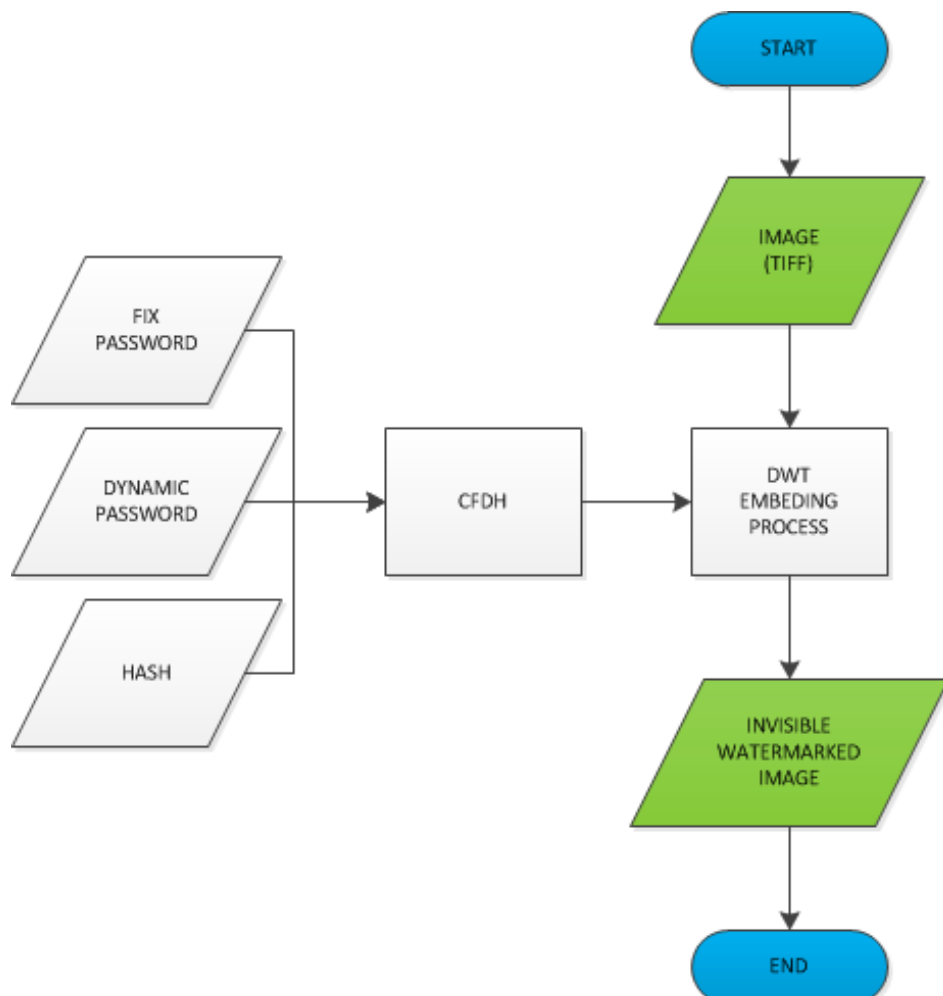


Figure 4.4: Watermark embedding process

4.3 ARTEFACT DEVELOPMENT (RIGHTFUL OWNERSHIP DETECTION SYSTEM DEVELOPMENT)

This section is a demonstration of the designed and developed artefact in the cloud environment based on an artefact build in C#. The scope of the system run in Amazon web Services (AWS) console, but the program has been also tested in other cloud provider environments such as VMware VSphere in a private hosted environment and Microsoft Azure cloud platform. Figure 4.5 has highlighted the used services such as Amazon S3 as the data storage and Amazon Relational Database Service (RDS) as the main system database. RDS with SQL server 2014 integration has been used as cloud server database to compile and store the uploaded information in the cloud side after the users' login or upload the new data.

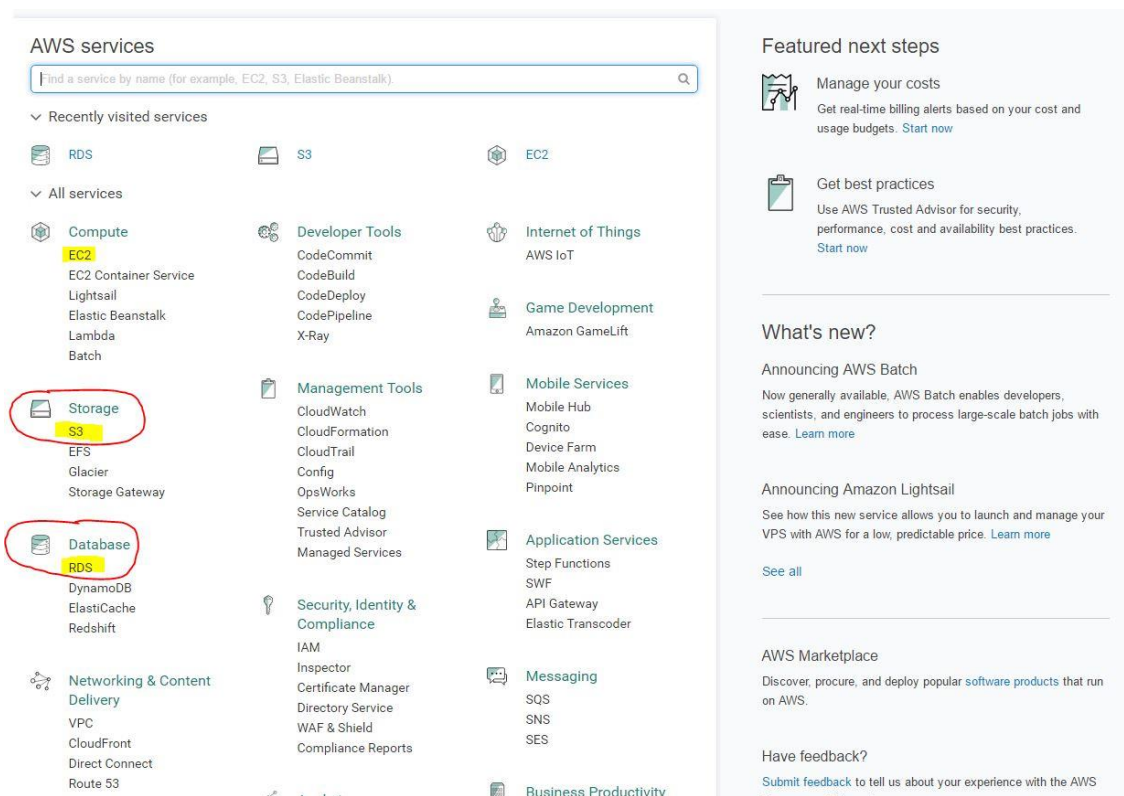


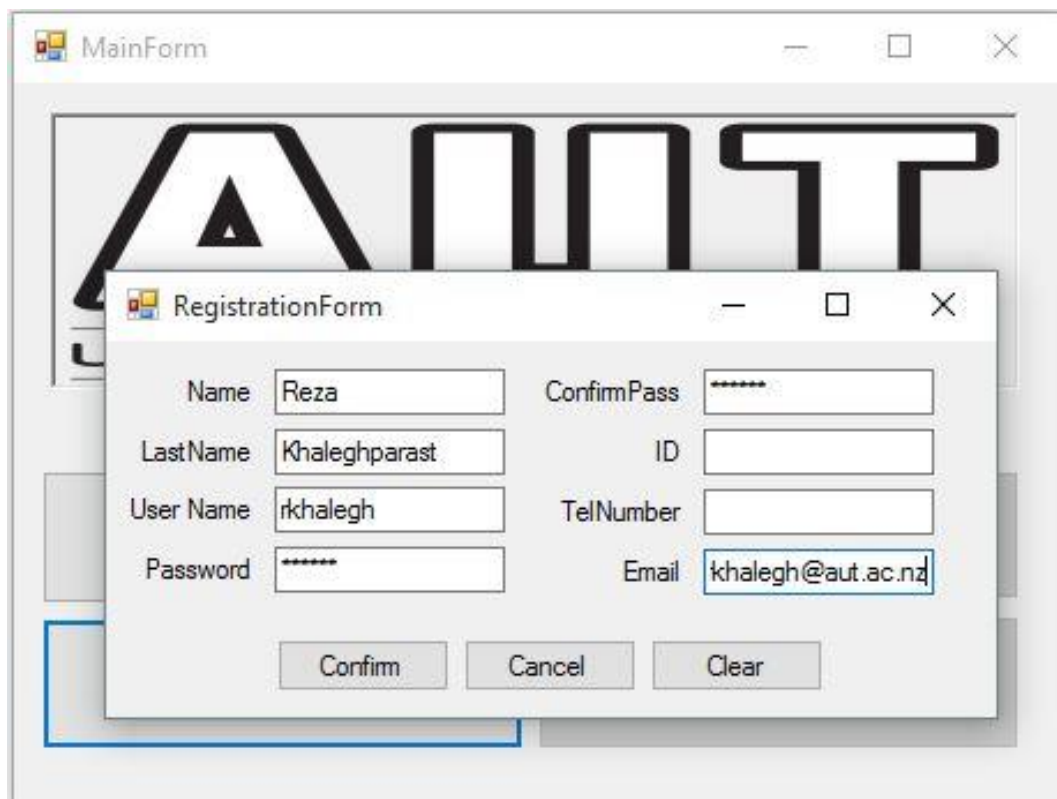
Figure 4.5: Amazon Web Services Console

The software has been implemented in windows form- based, which helps this study to simulate the proposed flow framework. It can develop applications for Windows, cloud, cell phones, Microsoft Office, and Microsoft SharePoint with the same development environment. Plus, it can automatically adapt web applications to target mobile devices with enhanced ASP.NET support for mobile browsers. The

RODS can be run under Microsoft Windows; therefore Windows 7 has been used as the selected Operating System (OS). the SQL Server is the foundation of the cloud-ready information platform. SQL Server 2014 was used for the database, and can extend data across on-premises and public cloud environments. The following sections elaborate in detail the developed environment of RODS and explains the steps taken to build the system.

4.3.1 Login

It is necessary for each user to authenticate themselves to a cloud service provider before they can use cloud. For this purpose, every user needs to sign up into Cloud Rightful Ownership Detection System (RODS). Figure 4.6 shows the user registration form, which has to be filled by the users to be able to access to the system. The RODS password rules are following the current NIST password regulation. There are some policies, which have been put in place by different cloud providers to prevent identity theft problems and prevent the use of other person's identity. This problem of identity theft is out of the scope for the research but the



The image shows a screenshot of a software application with two windows. The background window is titled 'MainForm' and displays a large, stylized logo that appears to be 'AUT'. Overlaid on top of this is a smaller window titled 'RegistrationForm'. This window contains a registration form with the following fields and values:

Field	Value
Name	Reza
LastName	Khaleghparast
User Name	rkhalegh
Password	*****
ConfirmPass	*****
ID	
TelNumber	
Email	khalegh@aut.ac.nz

At the bottom of the 'RegistrationForm' window, there are three buttons: 'Confirm', 'Cancel', and 'Clear'. A blue rectangular box highlights the bottom-left corner of the 'RegistrationForm' window.

Figure 4.6: User registration form

RODS has a mitigating effect. Some of the options, which users will enter to fill the registration form requirements, are usernames and passwords. These will be used to authenticate users to the system. Passwords will also be used as one of the options of CFDH in the embedding process. Cellphone numbers also will be used to send the users DYN Password to their personal cell phones as a secondary authentication method and accordingly increase the system integrity.

Users need to login to Cloud Rightful Ownership Detection System each time they want to use the system as it has been shown in Figure 4.7. After login to the system, they will be able to access to the cloud to upload their data. This authentication can be improved by using the secondary authentication methods or OpenID systems can be used to authenticate users to the system as future research.

The image shows a login window with a light gray background. It contains two input fields: 'UserName' with the text 'Reza' and 'Password' with three asterisks. Below these fields are two buttons: 'Login' and 'Clear'. At the bottom, there is a blue underlined link that says 'Forgot Password'.

Figure 4.7: Login window

4.3.2 Upload Image

Users will be able to upload their images to cloud servers in this step. This step has included three parts. In the first step the users browse their images and upload it to the cloud by clicking on Upload button. The original image, and its Hash also will be sent to the cloud through a public channel for further processing. Figure 4.8 shows the successful transaction of the uploaded image to the cloud server.



Figure 4.8: Successful transaction of uploading the image

The second step after uploading the image, users need to request a DYN code from the cloud. This will be done with the purpose of better integrity, because the DYN code will be sent to the cellphone of the registered user. If any other person has the Username and Password of the real user, they will not be able to continue uploading an image with another identity. The request of the DYN code, by the user to cloud, has been shown in Figure 4.9.



Figure 4.9: DYN sample code

Third step and the last one, is sending the extracted features (CFDH) to the cloud servers to start the three-dimensional authentication parts. The following figure (Figure 4.10) will show that the image and its features have been sent to the cloud server (Database) successfully.



Figure 4.10: Notification of successful features sending

4.3.3 WECH Process

WECH process is the first step of three-dimensional image authentication part, which will check the watermark existence, coming from the users with the purpose of recognizing the image that whether it has been watermarked with the Cloud Rightful Ownership Detection system or not. For this to be done, the image will be checked with the watermark algorithm to find out if there is any watermark embedded in the image before or not. The following table (Table 4.2) is the pseudo code for extracting the embedded message, which has 512 bits of the features.

Table 4.2: Extracting the embedded message Pseudo Code

<p>START</p> <ul style="list-style-type: none"> - Read the suspected image - Convert the suspected image to double
--

- Do the DWT2 algorithm on suspected image
- Build an empty matrix with 512 rows and one column
 - FOR 1 to 65535 in every 128 bits
 - Read the HH bit and put it into the built matrix
 - Save the output in a text file format
 - Increase the counter
 - END FOR
- END

Immediately after checking the watermark existence, the MD5 hash code of the uploaded image will be checked with the exist images in cloud database. If the hash code could not be found in cloud database and also system could not find any embedded watermark in the uploaded image, the user will allow continuing to the next step of checking (Figure 4.11).

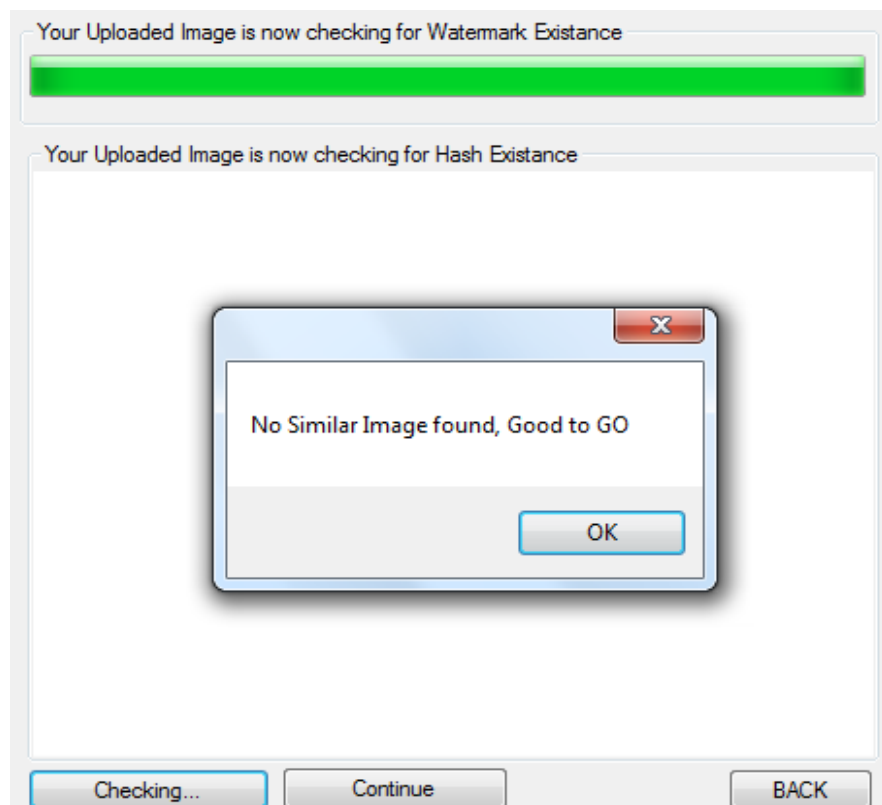


Figure 4.11: Notification of user clearance to continue to next step

If any similar hash code could be found in the cloud database, the system will stop the user continuing by showing the existent image in a picture box (Figure 4.12); and also an error to the user.

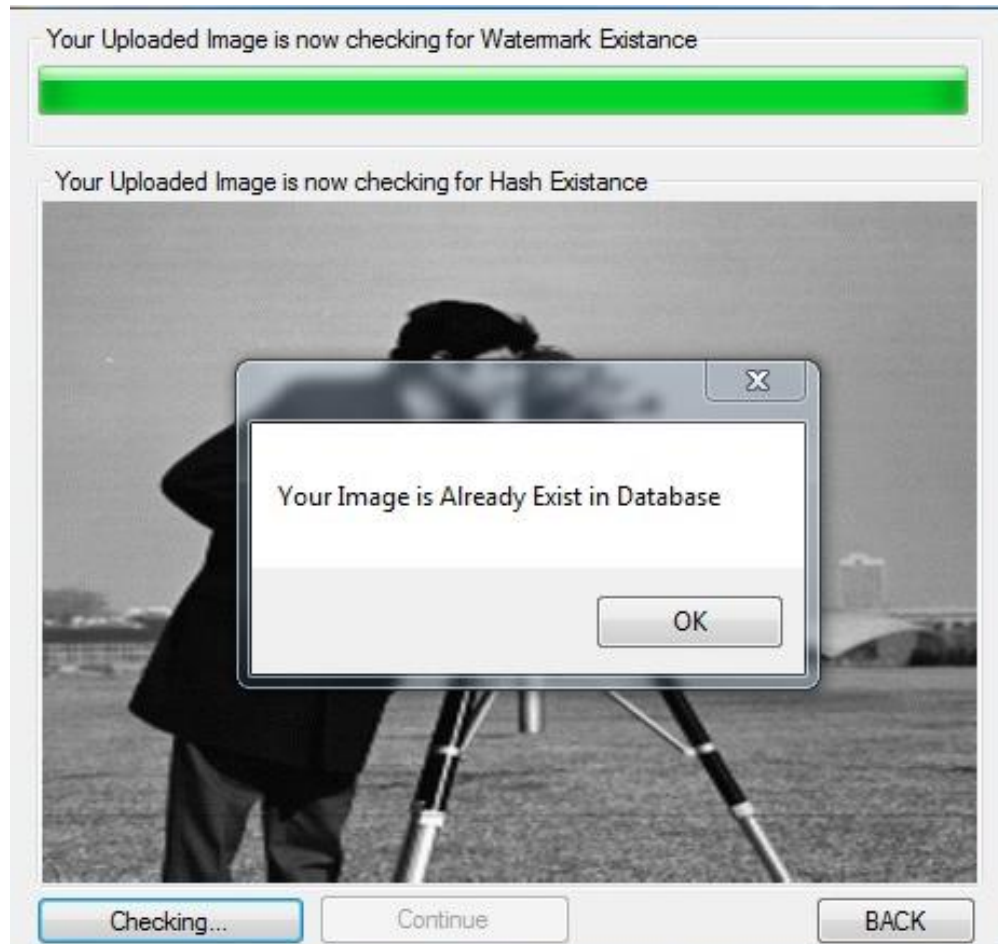


Figure 4.12: Image existence notification in hash existence check system

4.3.4 ISCH Process

After the uploaded image could pass the first and second image authentication steps, it will be checked by the ISCH system as the last step of authentication. In this step, first, a sample of the uploaded image will be acquired and is examined for similarity as explained in section 4.2. If the similarity in each image during the ISCH step reaches the limit, it will be marked as similar image with the uploaded one and it will be shown in the field of "Number of similar images". Second, the image name will also be placed in a combo box in similarity form. By choosing the image name, similarity percentage and similarity factors will be showing the form of the selected image. Third, selected similar image will be fetched from the database and

will be shown in a picture box on founded image. Finally, differentiation between the uploaded image and the selected similar one from the cloud database will be graphically shown. A box of red color will be colored on the similar pixel with opacity of 70% that makes the differentiation more visible to see. The advantage of using this graphical tamper detection system is because of the better recognition of the different pixels, even with a tiny change. It also can recognize the differentiation happened because of the formatting change. For instance, if the format of the uploaded image has been changed to another format, ISCH still can recognize the changed format image. Figure 4.13 shows the four mentioned steps.



Figure 4.13: Image Similarity Check (ISCH)

4.3.5 Watermarking Process

Watermarking process is the last step of the Cloud Rightful Ownership Detection System, which is embedded part as watermark. This step can be divided into three sections. First, gathered features will be combined into one line code, which uses an SHA512 algorithm shown in figure 4.14. In this section, an SHA512 hash code will be created from the combination of extracting features, and it will be saved as hexadecimal code.

Features

Fix Password

123

Dynamic Password

827190


Hash

dba1ea0270d6359c

SHA512

56ba4836b61a600f96c1479e304
8bf9c0de2e3fd054281596d6e04d
b1ccce66ab4605440d02c278c03
a9007028314f0fab8da7538ab0f4
9b556f7c7455bbca80

Cover Image



RETRIEVE

SAVE

EXIT

BACK

Figure 4.14: Watermarking with extracted features

In the second section, the hexadecimal output hash is altered into an array of bits for faster and less time-consuming purposes. Figure 4.15 shows the bit stream output, which has been built from the SHA256 hexadecimal code. This code is embedded into the cover image as a message for the watermarking section. This code also can be extracted from the suspected image, which has been uploaded to the system for authentication. The code will be converted into hexadecimal and is checked with the available code of each image to find the similarity.

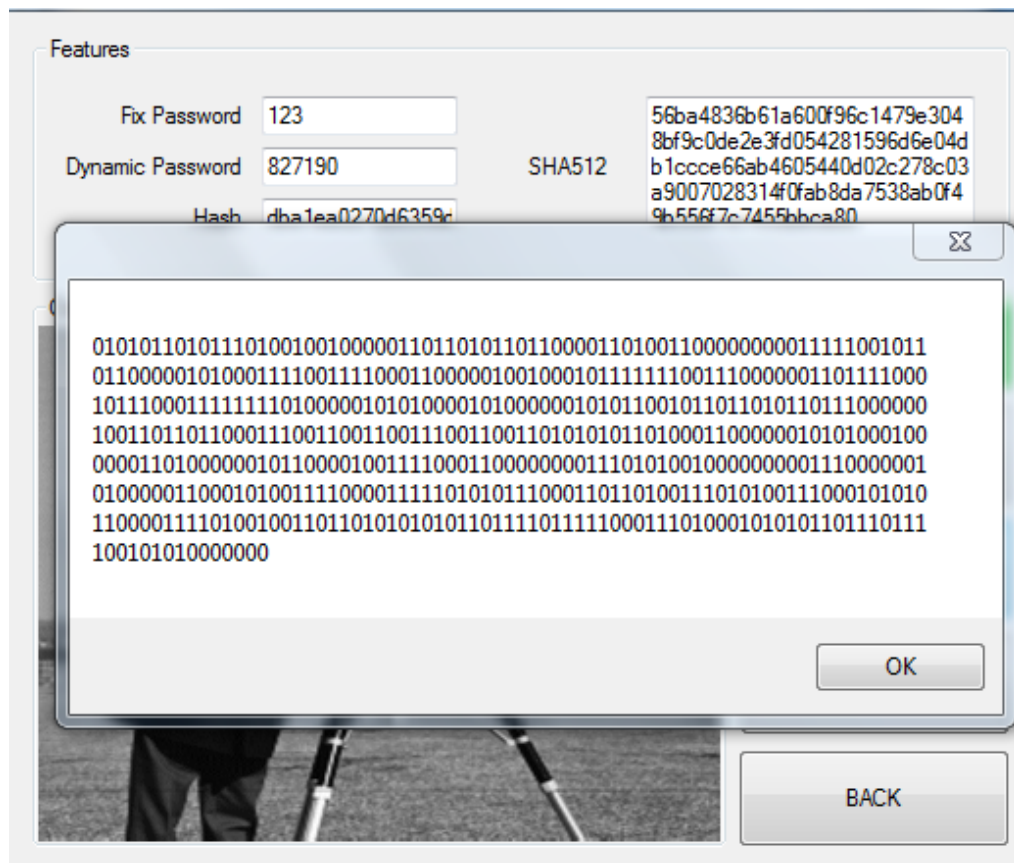


Figure 4.15: Bit stream code built for watermarking purpose

Finally the message is ready to be embedded into the uploaded image, which has passed the entire authentication checking steps, and is ready to be used as a cover image. By pushing the watermarking button, the message is embedded into the cover image and is saved in cloud database as a new identified image belonging to the registered user.

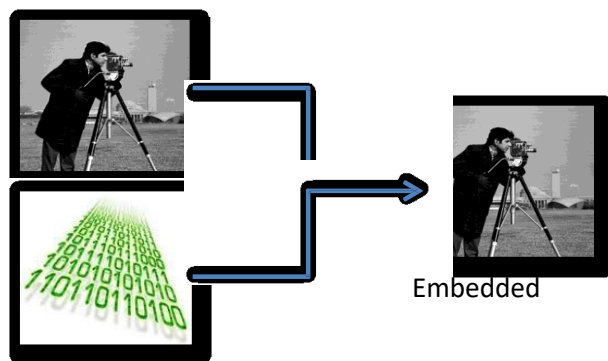


Figure 4-16: Embedding process

Figure 4.16 is an illustration of the watermarking step. This figure shows that the watermark has been embedded into the host image without any visible changes in the final image. Figure 4.17 is also showing the last step in RODS before the final image is stored in the database after passing all the required authentication steps successfully. In figure 4.17 the image has been successfully watermarked without any problem.

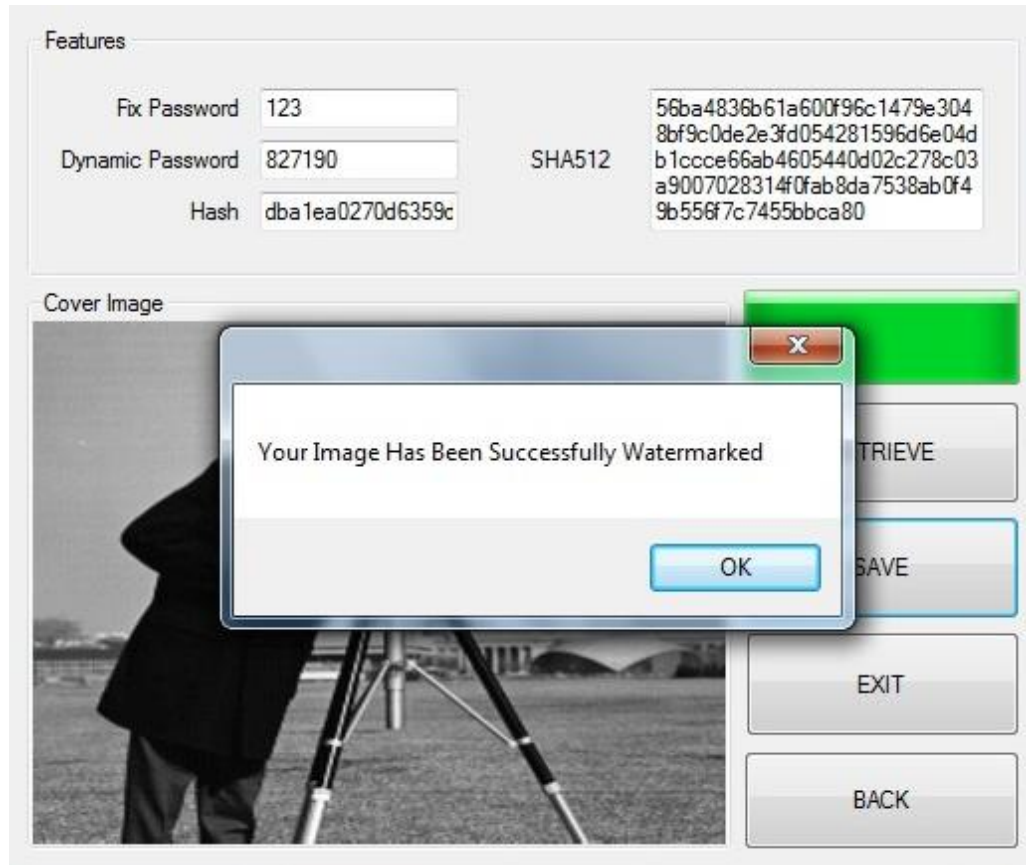


Figure 4.17: Notification of successful watermarking

The three security features that form the core to the artefact were constructed from data available in the cloud environment to uniquely identify the user. The first feature termed ISCH allows an image a user uploads to be stored with original hex and hash tags. The second feature termed CFDH comprises of a fixed password, a dynamic password and a hash (section 4.2.2). The CFDH consequently provides unique identification that is carried in the watermark. The third feature is the watermark existence check that is outlined in section 4.3.3.

Together these security features provide unique identification for the user in the uploading action, in the Cloud processing and in the Cloud database. After passing from all RODS authentication steps, image is ready to be embedded and saved. Figure 4.18 illustrates the embedding final embedding process. This process starts with the watermark size to be embedded into highest rate array of the host, following by the other channels. This process will continue and the results can be varies depends on the size of the watermark and the host.

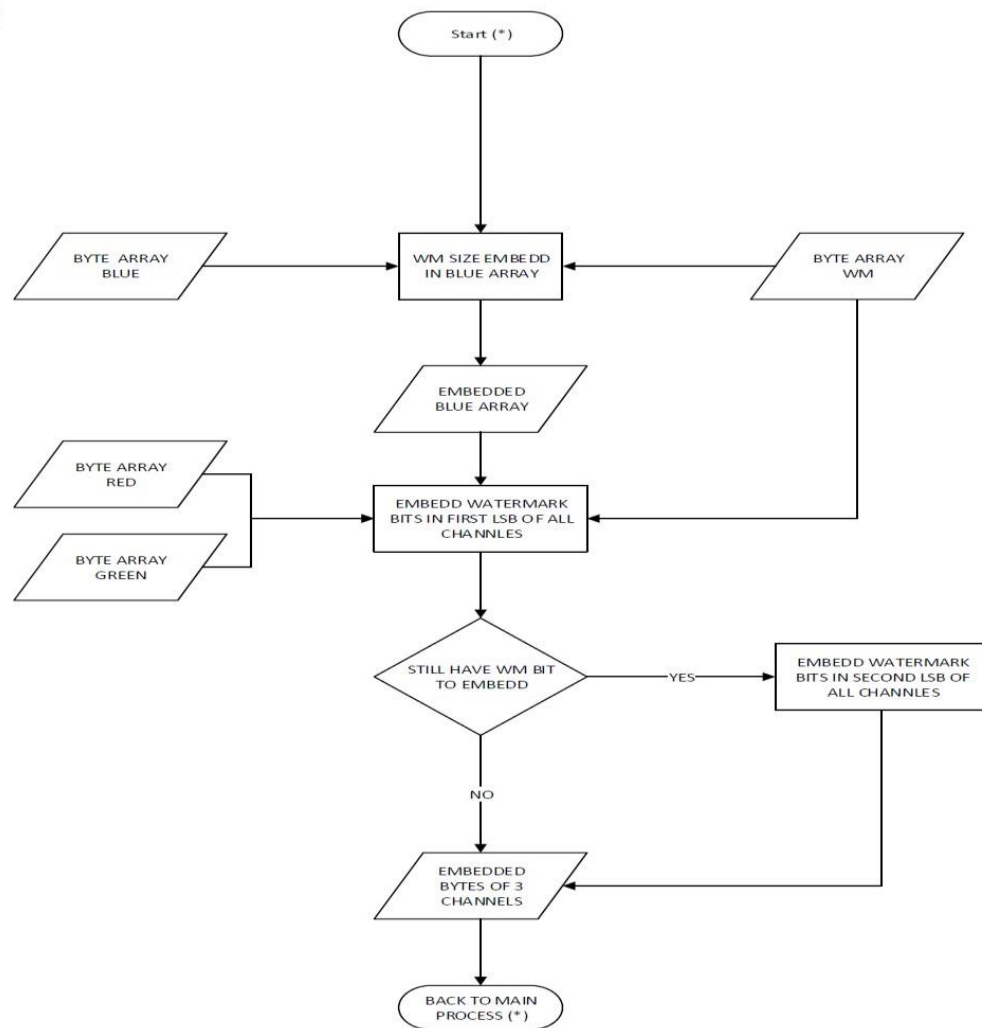


Figure 4.18: Embedding algorithm

In Summary a number of important aspects have been discussed and implemented. The results of RODS implementation in section 4.4 will be sent and added into the AWS RDS to be stored and to be used for the future image uploads. The bigger the database gets, the better results will be obtained from the use of RODS.

4.4 SUMMARY

Chapter 4 has provided and demonstrated the artefact design, architecture and security mechanisms for implementation. The artefact was designed and developed by the researcher in software and in this chapter it has been demonstrated step-by-step. The flow diagrams and design tools have also been outlined and carefully explained so that another researcher may follow these processes. These research processes are compliant with the design science framework that is being used to guide the research. In chapter 5 the deliverable from chapter 4 is to be evaluated from two different perspectives. The first will be the statistical analysis and the second from expert feedback. In this way not only is a technicality of the development exposed but also the usability and functionality are fully evaluated. Hence the scope of the design for both software and hardware has been justified.

Chapter 5

Artefact Evaluation and Analysis

5.0 INTRODUCTION

In chapter 4, the design, development and implementation of the research artefact comprising of an interactive system design based on DS, were reported, illustrated and described. The Rightful Ownership Detection System (RODS) has been demonstrated and made ready for the evaluation in chapter 5. In Chapter 3, subsection 3.4.1, a great emphasis has been made of the evaluation aspects of DS research, and the necessity of validating the artefact solution empirically. In a similar fashion to what is presented in section 3.4.1, artefacts will be subject to the two types of evaluation: Naturalistic evaluation from experts' feedback and statistical evaluation by putting the artefact under the evaluation techniques discussed in Chapter 3, section 3.4.2. Gathering experts' evaluation and collecting resulting data must follow AUT Ethics Committee procedures and the requirements. For details please see Appendix A.

In Chapter 5, based on the outcome of chapter 4, the Evaluation of the proposed solution will be presented in detail. Input, process and output are the three parameters of each system. The detail of the requirements are discussed and then the process explained. Also description about the pre-requirements for conducting experiments are provided and finally the output found by running several sample tests. The output part for results has been divided into three parts according to the design section in chapter 4, which are: testing results of the Watermark Existence Check, Hash Existence Check, ISCH system and watermark embedding. The result of the proposed design must fulfill the objectives of the project, which is finding rightful ownership in cloud environment.

In Chapter 5, section 5.2, the two types of evaluations are adopted in the DSR roadmap devised by Peffers et al. (2007) and Alturki et al. (2011) and shown in Figure 3.3. The 2-teir evaluations were noted as Internal and External evaluation, with the aim of ensuring the quality of the artefact. A number of artefact evaluation criteria and corresponding questions were formed based on the output of the phases discussed in section 3.4.

This chapter is structured as follows: sections: 5.1 outlines the Naturalistic Expert evaluation, including the requirements such as fieldwork activities in subsection 5.2.1 and evaluation preparation activities in section 5.2.2; followed by the expert evaluation results and finished by a critical evaluation reflection. Section 5.2 then, focuses on statistical evaluation of the developed artefact, including the evaluation of each designed image evaluation steps in RODS; starting with subsection 5.2.2, following by a full evaluation of the designed ISCH in subsection 5.2.6. The evaluation continues by the watermarking evaluation process in section 5.3 and then the chapter will be concluded with a summary in section 5.4.

5.1 NATURALISTIC EXPERT EVALUATION

For the artificial evaluation, three experts (Exp1 and Exp2 and Exp3) have been approached and agreed to evaluate the artefacts, based on DS method that is explained in Chapter 3, section 3.4.1.1. While all experts have experience in cloud computing, watermarking and cryptography and they have been working in the same field. However, Exp1 has more years (> 20 years) of mixed work experience in IT and has considerable knowledge of the cloud computing. While Exp2 has (= < 10 years) and also has some experience in software development and has worked in IT security field and cloud computing field as an advisor. The third expert also has more than 20 years of experience in Digital Right Management (DRM) field. He has been working in this field and his oral comment on the development of the artefact were also very useful for later considering a commercialized version of the artefact. The aim is not only to get their feedback on the applicability of the artefact, but also on the usability, functionality, effectiveness and efficiency of the developed artefacts.

This section comprises the following sub-sections: 5.1.1 outlines the evaluation fieldwork activities, followed by section 5.2.2 discussing the evaluation preparation activities and continues with the expert evaluation in 5.1.3 and 5.1.4 concludes the section with a critical reflection of the experts' evaluation.

5.1.1 Fieldwork Activities

Initially some emails were exchanged with the two experts explaining the objectives of the research and the proposed model. Then, an initial meeting was arranged with each expert when the link and other materials (hard copies of the files) were

provided. During those meetings the researcher demonstrated the system for the expert explaining briefly the background of the artefact, and how to install and use RODS. Following that, the researcher went through the RODS steps, as demonstrated in Chapter 4, section 4.3 to ensure the experts understanding of the implementation and evaluation procedures. Furthermore, the researcher explained the instructions on how to use the developed system and what the expert was expected to do, and the set of evaluation questions they needed to answer at the end of the evaluation exercise.

The experts were given 1-2 weeks to try the developed system. During that time; Exp2 raised some questions for discussion and reflected the Exp2's interest in using the system. It also gave the researcher an opportunity to enhance the applicability of the system in the real world. As an answer to the main question from the experts about the usability environment of the system, it was emphasised that the more use and trust gained from the cloud provider would allow the system to be used in broader areas and databases.

When the experts managed to use RODS, other meetings were arranged to meet up with them individually to collect the answers and the updated spreadsheet. The files were checked by the researcher to ensure the instructions were followed according to the provided document. On a few occasions some rework needed to be carried out by Exp1 as some of the instructions were not clear. In addition to the written feedback, which comprises the answers the experts have provided, also oral feedback was provided. The researcher made notes from the oral feedback for analysis and triangulation with the written notes to validate the captured feedback.

5.1.2 Evaluation Preparation Activities

The list of the files described in this sub-section, in addition to the installation files, have been prepared as listed in Table 5.1, to provide more detail for the user on the prepared files.

Table 5.1: Artefact list provided for experts evaluation

No.	Name of the File	Description
1	RODS Cloud instance access link	Installation file for the RODS has been provided for experts to install the system

2	Manual Documentation of the system	The instruction manual has been provided for a better user friendliness and a better understanding of how the system works.
3	Link to the whole package	All the files are packaged in a provided link

5.1.3 Experts' Evaluation

Experts' artefacts evaluation is an essential stage in a DS based research as theory and developed artefacts applicability are put to the test. Evaluation outcomes could be reflected upon at the various research stages of artefact development as deemed necessary. More knowledge could be obtained as the evaluation unravels new findings and/or clarifies any ambiguity that might have been presented.

As noted in 5.1.1.1 a set of questions have been prepared to obtain experts' feedback after using RODS. Table 6.1 lists the set of questions and both experts' replies. Salient points of their answers have been shaded indicating the experts' key points. Written and oral feedback were obtained from the experts during the mentioned meetings.

With regards to the experts' feedback, data were extracted from the spreadsheet and tabulated in respective tables, checked to ensure experts' identities remain anonymous and as it was found necessary, the feedback text was edited and typos were rectified. In the experts' feedback tables, salient points are highlighted in gray to attract a reader's attention.

5.1.3.1 Expert1

For Expert1, has considerable knowledge in Cloud Computing, watermarking and Steganography area as well as security systems and currently works for a University. Expert1 has raised questions about the commercial usability of the System, but he has also mentioned that this could have strong potential for industry level use. Expert1 responded to the questions in the fashion as outlined in Table 5.1.

Table 5.3: Expert 1 respond to the questions asked

No.	Description	Expert's Answer
	The RODS overall evaluation:	
1	Overall, how effective do you think the proposed system would be in the real commercial world in case of the ownership protection?	I think that this system that I see in a prototype version is very thoughtful and has a real-world application. It will need to be integrated within a robust commercial software package in order to see its real advantages. However as a prototype I think that it clearly demonstrates the theoretical understanding is and does offer businesses a new opportunity.
2	Are the defined sections relevant to what you observe?	Yes.
3	Are the provided metrics adequate and helpful to determine relevant mitigating measures?	Yes. Further refinement can occur after more attacks are tested. However at present it is sufficient.
4	Is the provided strategies' payoff guidance realistic and adequate?	Yes.
5	How easy it was to use the RODS, and was there any difficulty in using it?	It was very easy to use. I thought that the interface and ideas been communicated were intuitively strong.
6	How long did it take you to go through each step from registration to watermarking?	It took about 2 to 3 minutes once I worked out what to do.
7	What area of improvement - you can think of? Please list as many as possible	As a prototype this is fine. However the interface and the input requires refinement for commercial use.
8	Do you think RODS is effective and efficient in determining the rightful ownership?	Yes. It is a very good idea and I think that many service suppliers will want to use it.
9	Usability and ease of operation?	I found it easy and intuitive to use but as I said above for a commercial application the interface will need to be redeveloped and the coding secured.

10	Strengths and weaknesses of the system?	It is easy to use. It does what it says. It solves a problem. As mentioned above it requires redevelopment for commercial implementation.
11	How complete do you think the system is?	It is a proof of concept at this point of time in a prototype. Before release to the commercial world it will need further testing, a new interface, and secure coding.
12	Does the designed system has the potential to be widely adopted?	Yes, once the above improvements are implemented and the cloud service providers see the advantage of using it.
13	How effective do you think the system will be If more Cloud Service Provider start using RODS?	Effectiveness improves in quality cycles so that learning would have to be built into the adoption framework to be effective. If it was universally adopted then it is a good idea.

5.1.3.2 Expert2

Next in the list shown in Table 5.2 is Expert2, who is a Cloud Computing advisor and has worked and has extensive knowledge and work experience in the field of cloud computing and IT security. He has been working in industry level positions while doing academic positions in higher education. Expert2 answers to the set of questions shown in Table 5.2:

Table 5.4: Expert 2 respond to the questions asked

No.	Description	Expert's Answer
	The RODS overall evaluation:	
1	Overall, how effective do you think the proposed system would be in the real commercial world in case of the ownership protection?	The idea is of this app is precious and has a lot of commercial potential. This app could be very useful If this can be used in a vast area
2	Are the defined sections relevant to what you observe?	Yes. I think there is enough info provided
3	Are the provided metrics adequate and helpful to determine relevant mitigating measures?	Yes.

4	Is the provided strategies' payoff guidance realistic and adequate?	Yes.
5	How easy it was to use the RODS, and was there any difficulty in using it?	It was user friendly and easy to use after the demo given to me
6	How long did it take you to go through each step from registration to watermarking?	It took about half an hour to get use to it, but after that it take about couple of minutes
7	What area of improvement - you can think of? Please list as many as possible	This needs more detailed work to be commercialised, but in overall it works perfect for me. It can also get expanded to cover more area
8	Do you think RODS is effective and efficient in determining the rightful ownership?	Yes.
9	Usability and ease of operation?	It was fairly easy to operate. I think I have answered that before.
10	Strengths and weaknesses of the system?	It solved the problem, especially with the commercial demand to the end line product
11	How complete do you think the system is?	This is a prototype as I have informed, and It works just fine, but I think the final version could be better
12	Does the designed system has the potential to be widely adopted?	Yes, this has a lot of commercial potential
13	How effective do you think the system will be If more Cloud Service Provider start using RODS?	If it gets adopted globally the product will be known for its features

5.1.3.3 Expert 3

With regards to Expert3, table 5.4 shows Exp 3's review of the RODS. Exp 3 has been working in the Digital Right Management (DRM) and has a lot of experience

in the same area of research. An assumption note is made by Expert3 that controls are operating effectively, to ensure the assumed system rating.

Table 5.4: Expert 3 respond to the questions asked

No.	Description	Expert's Answer
	The RODS overall evaluation:	
1	Overall, how effective do you think the proposed system would be in the real commercial world in case of the ownership protection?	Overall the given prototype works just fine and I personally think this can be used in a bigger scale, If the software can attract more service providers to use this.
2	Are the defined sections relevant to what you observe?	Yes.
3	Are the provided metrics adequate and helpful to determine relevant mitigating measures?	Yes.
4	Is the provided strategies' payoff guidance realistic and adequate?	Yes.
5	How easy it was to use the RODS, and was there any difficulty in using it?	Very easy to use
6	How long did it take you to go through each step from registration to watermarking?	about 10 minutes
7	What area of improvement - you can think of? Please list as many as possible	It looks fine to me. But It can have more features like informing the true owner of the image, also these sort of notification can be added
8	Do you think RODS is effective and efficient in determining the rightful ownership?	It looks pretty useful and user friendly. I think It can be tested in real environment to get more feedbacks
9	Usability and ease of operation?	Very easy, but needs more work to get commecialised

10	Strengths and weaknesses of the system?	It is user friendly and functional, but it would not work well enough, If there is no one using it. This system needs to be tested in real environment
11	How complete do you think the system is?	The app works fine, but It can add up some more features as I mentioned, to more widely used.
12	Does the designed system has the potential to be widely adopted?	Yes, I mentioned above
13	How effective do you think the system will be If more Cloud Service Provider start using RODS?	As I mentioned, this system has a lot of potential to be commercialized, but this require the app to be used in a bigger area. And yes if more service provider start using it. This can get better in practice.

5.1.4 Critical Reflection on Experts' Evaluation Results

Based on the artefacts evaluation criteria and the corresponding question as outlined in Chapter 3, Table 3.1, and similarly to what has been done in Chapter 5, the experts' evaluations are analysed and critiqued against the criteria as shown in Table 5.5. Furthermore, in this section the suggested changes resulting from the expert evaluation are outlined in sub-section 5.1.4.1.

Table 5.5: Critical Reflection on Expert Evaluation Results

No	Questions	Exp1 Answers	Exp2 Answers	Exp3 Answers	Researcher's Comment
	The DSS overall				
1	Overall, how effective do you think the proposed system would be in the real commercial world in case of the ownership protection?	I think that this system that I see in a prototype version is very thoughtful and has a real-world application. It will need to be integrated within a robust commercial software package in order to see its real advantages. However as a prototype I think that it clearly demonstrates the theoretical understanding is and does offer businesses a new opportunity.	The idea is of this app is precious and has a lot of fine and I personally think this can be commercial potential. This app could be very useful If this can be used in a vast area	Overall the given prototype works just as expected and I personally think this can be used in a bigger scale, If the software can attract more service providers to use this.	Agreed to the comment from all three experts about commercializing the system for a better understanding in the real world environment
2	Are the defined sections are relevant to what you observe?	Yes.	Yes. I think there is enough info provided	Yes.	
3	Are the provided metrics adequate and helpful to determine relevant	Yes. Further refinement can occur after more attacks are tested. However at present it is sufficient.	Yes.	Yes.	
4	Is the provided strategies' payoff guidance realistic and adequate?	Yes.	Yes.	Yes.	

5	How easy it was to use the RODS, and was there any difficulty in using it?	It was very easy to use. I thought that the interface and ideas been communicated were intuitively strong.	It was user friendly and easy to use after the demo given to me	Very easy to use	All three agreed to a certain point that the system is fairly easy to use
6	How long did it take you to go through each step from registration to watermarking?	It took about 2 to 3 minutes once I worked out what to do.	It took about half an hour to get used to it, but after that it take about couple of minutes	about 10 minutes	
7	What area of improvement - you can think of? Please list as many as possible	As a prototype this is fine. However the interface and the input requires refinement for commercial use.	This needs more detailed work to be commercialised, but in overall it works perfect for me. It can also get expanded to cover more area	It looks fine to me. But It can have more features like informing the true owner of the image, also these sort of notification can be added	All three experts have mentioned different comments to improve the usability of the system
8	Do you think RODS is effective and efficient in determining the rightful ownership?	Yes. It is a very good idea and I think that many service suppliers will want to use it.	Yes.	It looks pretty useful and user friendly. I think It can be tested in real environment to get more feedbacks	Overall the feedback on effectiveness is positive and expert one has mentioned again that this could have commercial potential
9	Usability and ease of operation?	I found it easy and intuitive to use but as I said above for a commercial application the interface will need to be redeveloped on the coding secured.	It was fairly easy to operate. I think I have answered that before.	Very easy, but needs more work to get commecialised	
10	Strengths and weaknesses of the system?	It is easy to use. It does what it says. It solves a problem. As mentioned above it requires redevelopment for commercial implementation.	It solved the problem, especially with the commercial demand to the end line product	It is user friendly and functional, but it would not work well enough, If there is no one using it. This system needs to be tested in real environment	Expert 3 commented on the need of this product being used in a bigger scale for a better testing scale.

11	How complete do you think the system is?	It is a proof of concept at this point of time in a prototype. Before release to the commercial world it will need further testing, a new interface, and secure coding.	This is a prototype as I have informed, and It works just fine, but I think the final version could be better	The app works fine, but It can add up some more features as I mentioned, to more widely used.	
12	Does the designed system has the potential to be widely adopted?	Yes, once the above improvements are implemented and the cloud service providers see the advantage of using it.	Yes, this has a lot of commercial potential	Yes, I mentioned above	
13	How effective do you think the system will be If more Cloud Service Provider start using RODS?	Effectiveness improves in quality cycles so that learning would have to be built into the adoption framework to be effective. If it was universally adopted then it is a good idea.	If it gets adopted globally the product will be known for its features	As I mentioned, this system has a lot of potential to be commercialized, but this require the app to be used in a bigger area. And yes if more service provider start using it. This can get better in practice.	

5.1.4.1 Suggested Changes

Based on the artefact evaluation from experts, this could be concluded that the there is a need to the system to be tested in a bigger scale. The use of the artefact in a larger scale could lead to results of a better understanding of the requirements from the cloud service provider point of view. Changes raised and discussed in section 5.1.4 has been noted and has been reflected on the second version of the system. Since this is an academic work, the results has been tested in a lab environment with fixed terms and scales. Section 5.2 has focused on the statistical evaluation of the results of the developed artefact.

5.2 ARTEFACT STATISTICAL EVALUATION

Statistical evaluation is described often as the ‘real’ test where the designed solution or artefact is tested in an actual environment to check how effective and efficient the designed solution is. Statistical evaluation, evaluates the artefacts, solution in real setting, this approach is always empirical. Following the DSR roadmap outlined by Alturki et al. (2011b), statistical and naturalistic evaluation to be carried out. Prior to any testing a full build of the information system was made. The code for this can be found in Appendix B.

Before conducting the experiments and demonstrating their results, it is necessary to state that the experiments are conducted in specific images, and in what format and type. Also, the kind of manipulation that is performed on the watermarked images and the metrics for calculating the quality of each section should be clear. The following sections will discuss the statistical evaluation results of each step of the artefact discussed in Chapter 4.2.3. First, the results of each image authentication process has been shown in visual form (section 5.2.2), and then the results of the watermarking with the illustration of the evaluation metrics is shown (Section 5.3).

5.2.1 Cover Images

The experiments are conducted on 512×512 grayscale images as the cover. Also, the format of the images is TIFF. The ten selected grayscale images are the most famous ones, which are used in image processing experiments, such as Lena, House, Mandrill, Cameraman and Peppers. These images are shown in Figure 5.1 and are to be used in the testing. Each of the following images has been taken from publically available websites and there is no copyright protection rights on them. These images have been used as reliable samples for this research, in size and format, but RODS is also able to use any other kind of images as well.



(a)



(b)



(c)



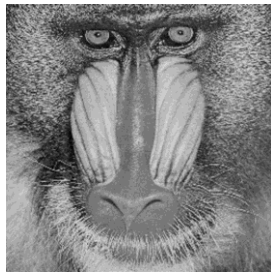
(d)



(e)



(f)



(g)



(h)



(i)



(j)

Figure 5.1: Standard-watermarking images. (a) Camera man, (b) House, (c) Jet Plane, (d) Lake, (e) Lena, (f) Living Room, (g) Mandrill, (h) Peppers, (i) Pirate, (j) Walking Bridge

5.2.2 Experimental Results for Watermark Existence Check

In this part of the artefact demonstration, the uploaded image will be checked for the watermark existence. If any watermark has been done on the uploaded image with the watermarking algorithm, the system will find and extract the embedded bit stream code. The bit stream code can be changed into hexadecimal and can be checked with a SHA512 hash code in the test cloud database. Finally the original image owner and related image can be found. The result is that the user is able to continuing through to the next step.

The following code is the extracted 512-bit stream code (Figure 5.2), which could be extracted from the Camera Man test image, which has been watermarked in the test system before.

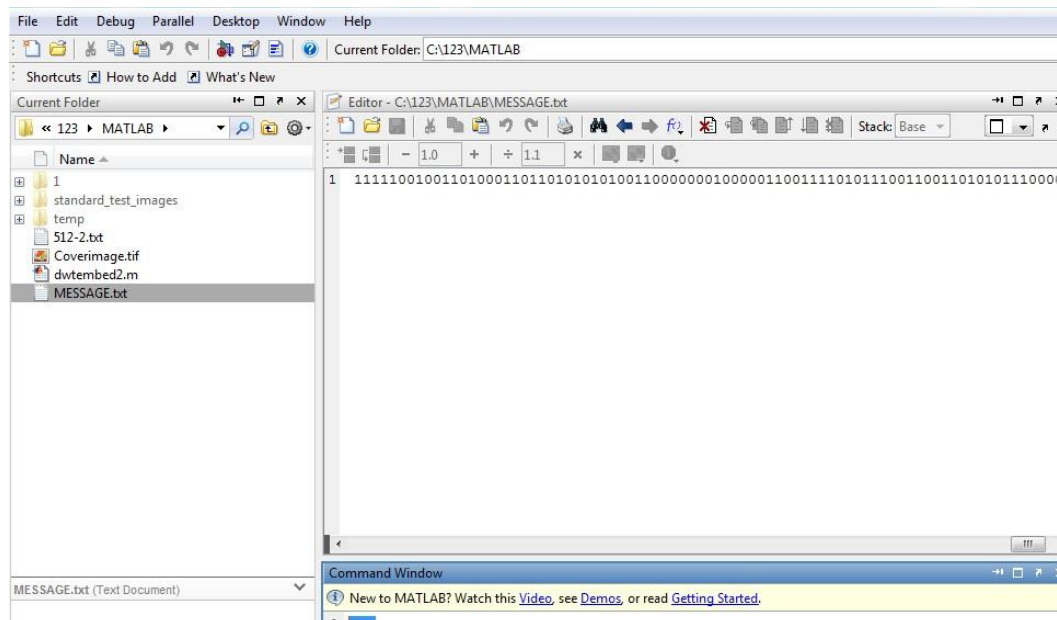


Figure 5.2: Message extraction

Figure 5.3 is the captured image from the cloud database, which shows the MixPassword as SHA512 hash code. This code has been saved in cloud database along with any authorised image, stored in there. The extracted bitstream code from the uploaded suspect image in Matlab will be changing the format into hexadecimal code. It then compares with the existing images hash in the test cloud database. Then the researcher can extract the original image and identify its real owner for further processing.

SQLQuery1.sql - WLMALQ.cloud (sa (54))

```

/***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP 1000 [FullID]
,[RegID]
,[FxPass]
,[DynamicPass]
,[Hash]
,[MixPass]
,[Image]
,[Calc]
,[ImageName]
FROM [cloud].[dbo].[Full]

```

	FullID	RegID	FxPass	DynamicPass	Hash	MixPass	Image
1	48	11	1	954434	dba1ea0270d6359dcf3a8929fd9fbbad	c2b7ffd7ad7ffd3c223a2fee748537339f777fb5b676e958a405...	0x49492A00!
2	49	11	1	954434	2d3cea98cd2923091b547666cbfdd8d5	d0565b9642a21c9aa19c0819e76d37e156dfee68e9e5c5795...	0x49492A00!
3	50	11	1	954434	f8b1b57d3c59e064867179c09dae921a	c97a49339647b03d330efd0e9d4611a2b695ff6c9c0eaff1fefa...	0xFFD8FFEO
4	51	10	123	619897	c583aebabffd9bfa938d3b6b9f5a8087	5ef861d49fb12b302d1716d684c475a4d901446aae76fd2c1a...	0x49492A00!
5	52	10	123	745978	2f3814ee340ce2be301d6851fc78cdc0	28d220432834e9b20064ed22450b53ecde29456b4ca50107...	0x49492A00!
6	53	10	123	745978	5a665d09aeebe65c61351ba4edeaaa03	801bc30ea10a9ee9a027ecbe52897a254039455ff6f394e251...	0x49492A00!
7	54	10	123	745978	ea35200af49ba0be8a8c6139a3579043	ebf4773d723ca701380c82111e8db16b71c9a9f67bfa9785d...	0x49492A00!
8	55	10	123	929283	68089b80745564a91670e9957d0df5ce	4111f4c3e441969be821268a35450f910644cac8151a2b56f3...	0x49492A00!
9	56	10	123	243161	7b7e6cdead514faefbe02070b061ff7a	5aba94f1c893d3b76bff0930b16629c068cdf83e9e16eed84...	0x49492A00!
10	57	11	1	472193	3e7e9d67c42846ca70332eada1213c70	5d3070b4edcd4f6888743bd0afa0882e13b17e71fd8449d48...	0x49492A00!
11	58	11	1	472193	69bf0988ffd77e31bf251e44de96255	983f21d72c65d0433fe4c234751d64f1051a47785a9c70012...	0x49492A00!

Figure 5.3: Cloud database capture of table "Full" which shows the stored output of SHA256

5.2.3 Experimental Results for Hash Existence Checking

This part is the second step of image authenticating after the watermark existence check. In this step, the uploaded image, which needs to be authenticated in the system, will be checked under the Hash Existence Check system.

In this step of the artefact demonstration, an MD5 hash code is extracted from the uploaded image and checked with an existing MD5 Hash code, which has been taken from the authorized and watermarked images in cloud database. If any similar image could be found in cloud database images with the uploaded one, the system will block the user from continuing through the system and flag an error with the system. The identified image will also be shown in a picture box.

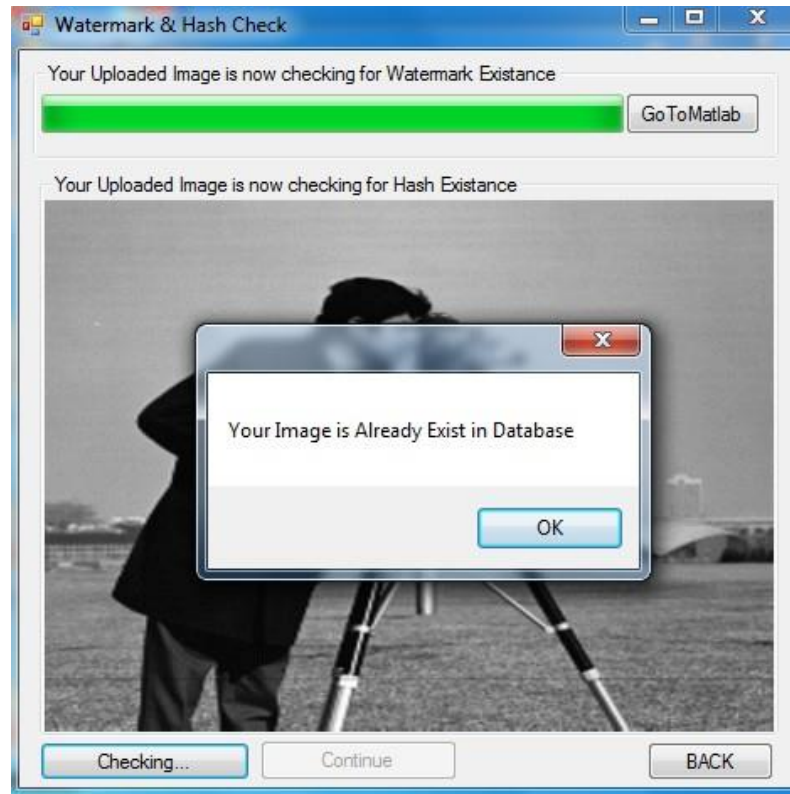


Figure 5.4: Result of Hash Check if the hash exists

Figure 5.4 shows the result of testing the Camera Man under the Hash Existence Checking system. In this result, the Camera Man has been uploaded successfully before it appears in the test cloud database. After testing the uploaded image, the system will find the existing image of Camera Man, show it in a picture box and block the user with an error.

In the following Figure 5.5, a Pirate Image has been uploaded to the cloud which doesn't exist in the test cloud database. The results show that the uploaded image could not be matched with any existing image hash in the database, so the user will be allowed to continue to the next step.

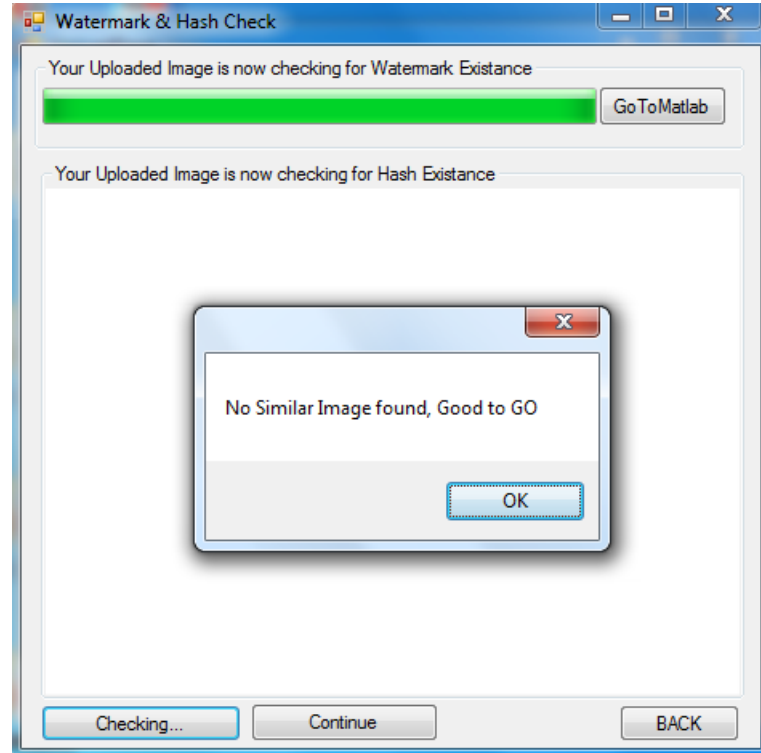


Figure 5.5: Result of Hash Check if the hash could not be found

The Hash Existence Checking system is a great option to detect the uploaded images from their hash code whether they have been uploaded to cloud database before or not, but it is not reliable enough to make it a primary system for image authentication, because with any tiny change to the original image, hash code of the uploaded image will be completely changed from the original one. So the system could be able to detect the manipulated image from the other existing ones in the test cloud database. As a solution to this problem, the Image Similarity Check (ISCH) system is used for a secondary image authentication and hence for reliability. The result of the ISCH functionality will be shown in section 5.5.

5.2.4 Experimental Results for Image Authentication

In this part, a quality test of ISCH system is done with ten of the popular standard images, which have been used in image authentication and watermarking tests. Testing the Resizing, Cropping, Format Changing, Text Manipulation and Flipping are all attacks that are tested. ISCH, which has been taken from the test simulation

system, will also be shown. The results include the similarity factors and similarity percentages that are found in similar images in the simulation tests. The original image has been shown on top of each figure and left side images and the right side images are the ones that has been tampered. The system has highlighted the tampered with red boxes, if the tamper could be detected in the image, otherwise the right side box would be empty. That means the image has not been detected with RODS.

5.2.4.1 Quality Test on ISCH

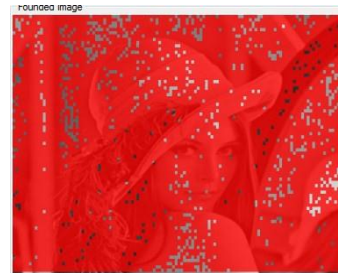
Resizing, Cropping, Brush Manipulation, Flipping, Manipulation with a text message and format changing to JPEG format has been extracted from ISCH system. These features are illustrated in the following figures. Other attributes will be explained separately in each tested image scenario.



(a)



(b)



(c)

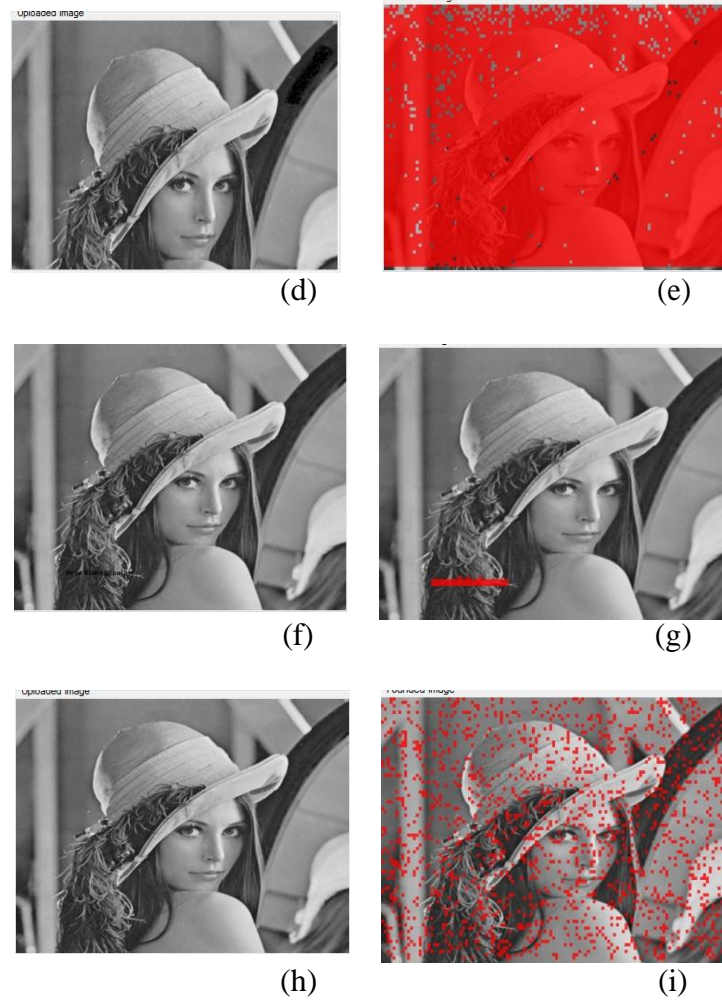


Figure 5.6: Lena ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

Figure 5.7 has resized the Cameraman to 10%. The results show that the system could recognize the image as a similar image in the database, but as it has been shown in this figure pixels of the uploaded image has been completely changed. The same thing has been done on a cropping test. In text manipulation, there are some extra pixels turned on, and it may be the cause of the mistakes during the manipulating attacks.



(a)



(b)



(c)



(d)



(e)



(f)



(g)

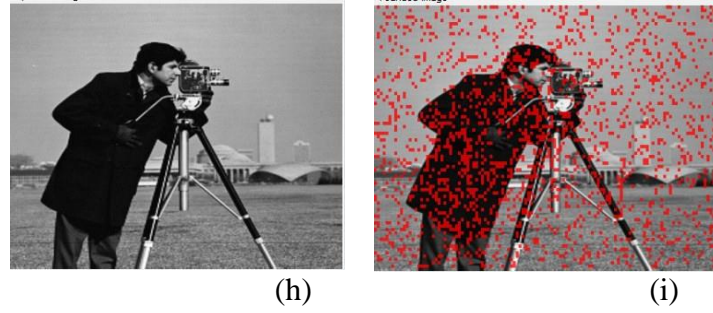


Figure 5.7: Cameraman ISCH results, (a) original image, (b) resize, (c) resizeresult,crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

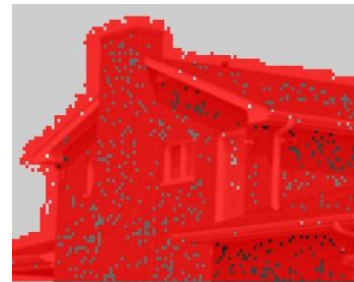
The House image was one of the interesting test images among the others, because, it also has been detected under the Flipping test. This image was the only image, which has been detected by ISCH system during the test of flipping. The other tests images could not be detected under flipping test. The other interesting finding is that, as it has been shown in Figure 5.8, the house object in the image has been recognized as a differentiate part in the demonstration, but the others do not differentiate.



(a)



(b)



(d)

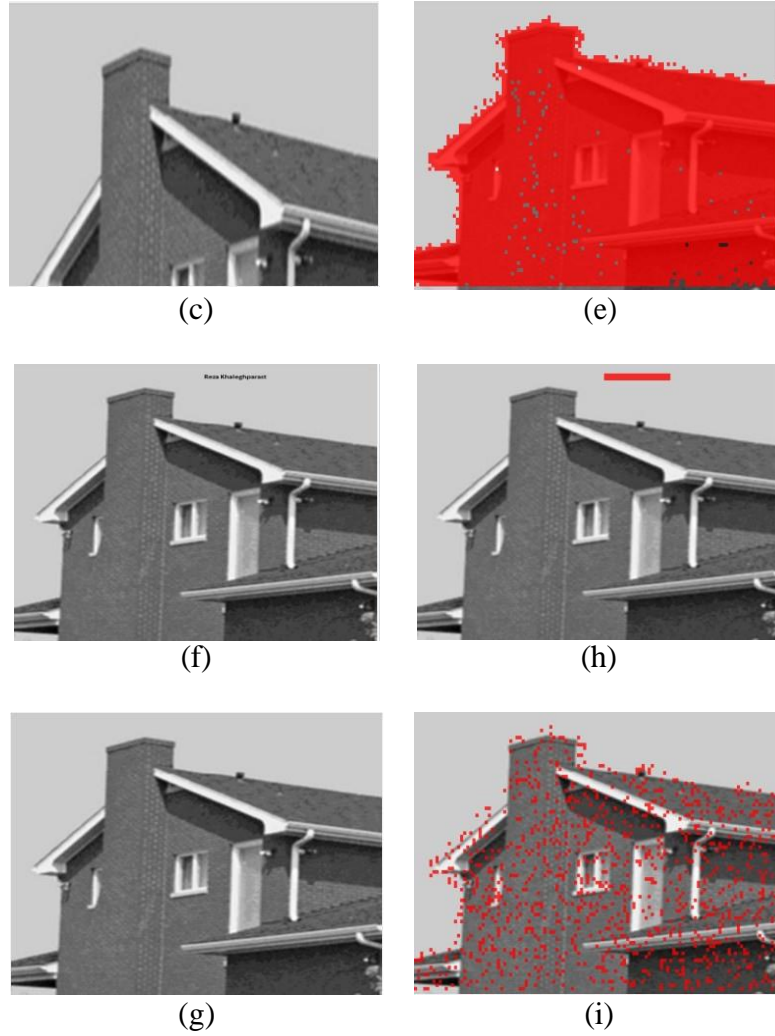


Figure 5.8: House ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

Resize, Crop, Text Manipulation and Format changing have been done in Figure 5.9. ISCH has failed to recognize the cropping test, but in the other tests shows the same results as the other images. Text manipulation is tried on a smaller area to show the fact that the system is able to detect any tiny manipulation of the uploaded image.



(a)



(b)



(d)



(c)

(e)



(f)



(h)

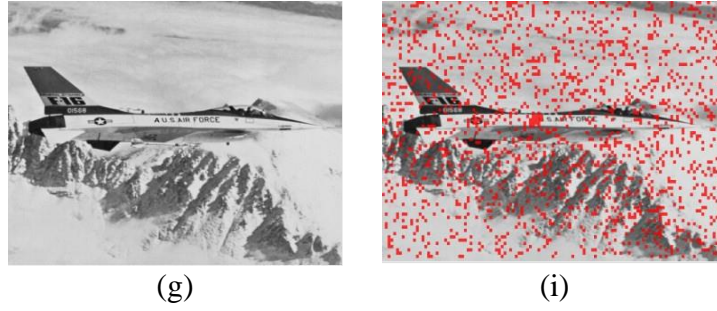


Figure 5.9: Jet Plane ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

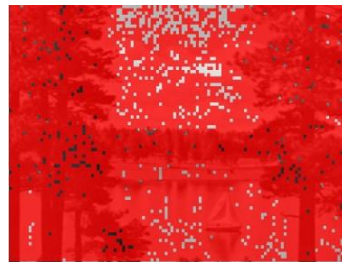
Crop test and flipping test have failed to be recognized by ISCH, but the other tests had the same results as the other images. This image was one of the test images, which has been recognized by ISCH under the Double Flipping test.



(a)



(b)



(d)

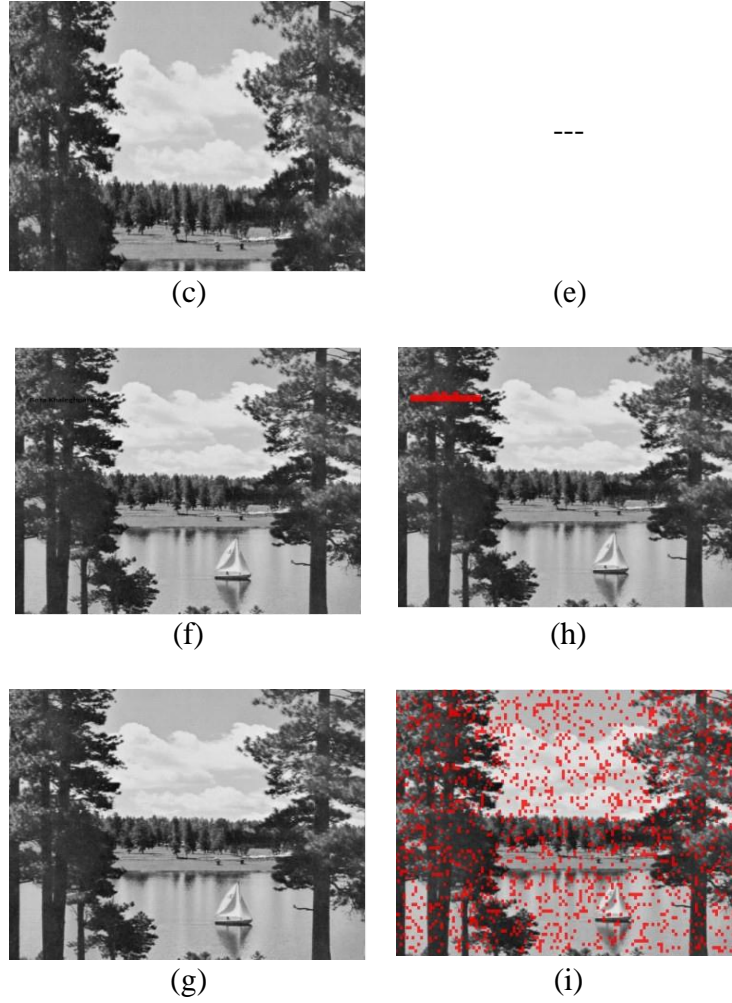


Figure 5.10: Lake ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

The following image shows the Living Room test image under the ISCH system, which can be seen in the following figures. The result of the testing on the Living Room image was the same as Lake test image.



(a)



(b)



(d)



(c)

(e)



(f)



(h)

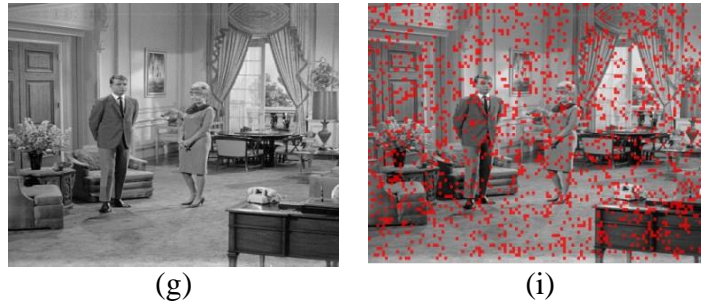
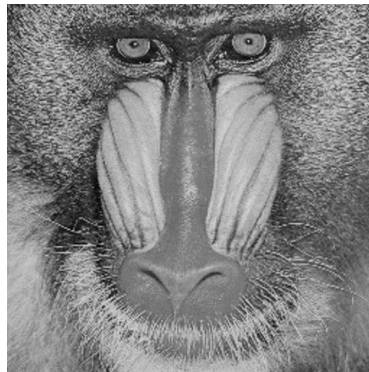


Figure 5.11: Living Room ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result



(a)



(b)



(d)



(c)

(e)

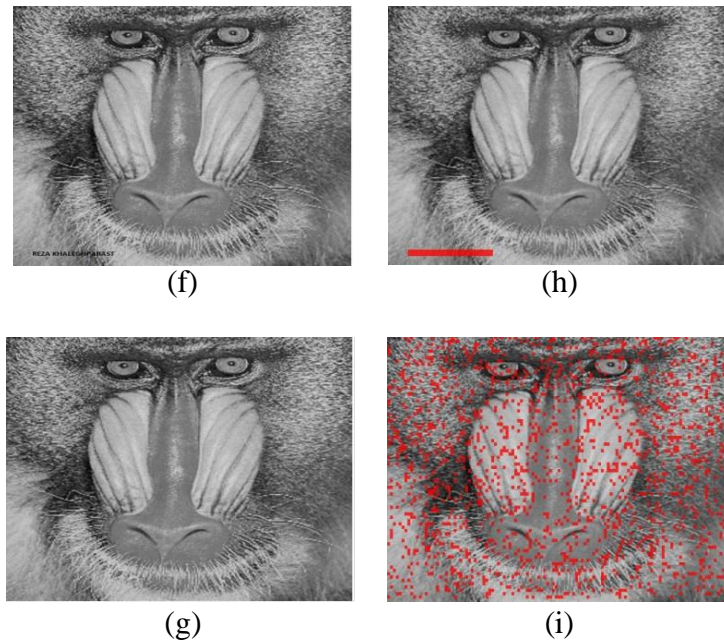


Figure 5.12: Mandrill ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

The following Figure (Figure 5.13) shows the result of ISCH system, which has illustrated the four testing actions: Resize 10%, Format Changing, Text Manipulation and Cropping. This image is one of the other tested images which has been under the flipping test and the results shows that it also could not be recognized by ISCH.



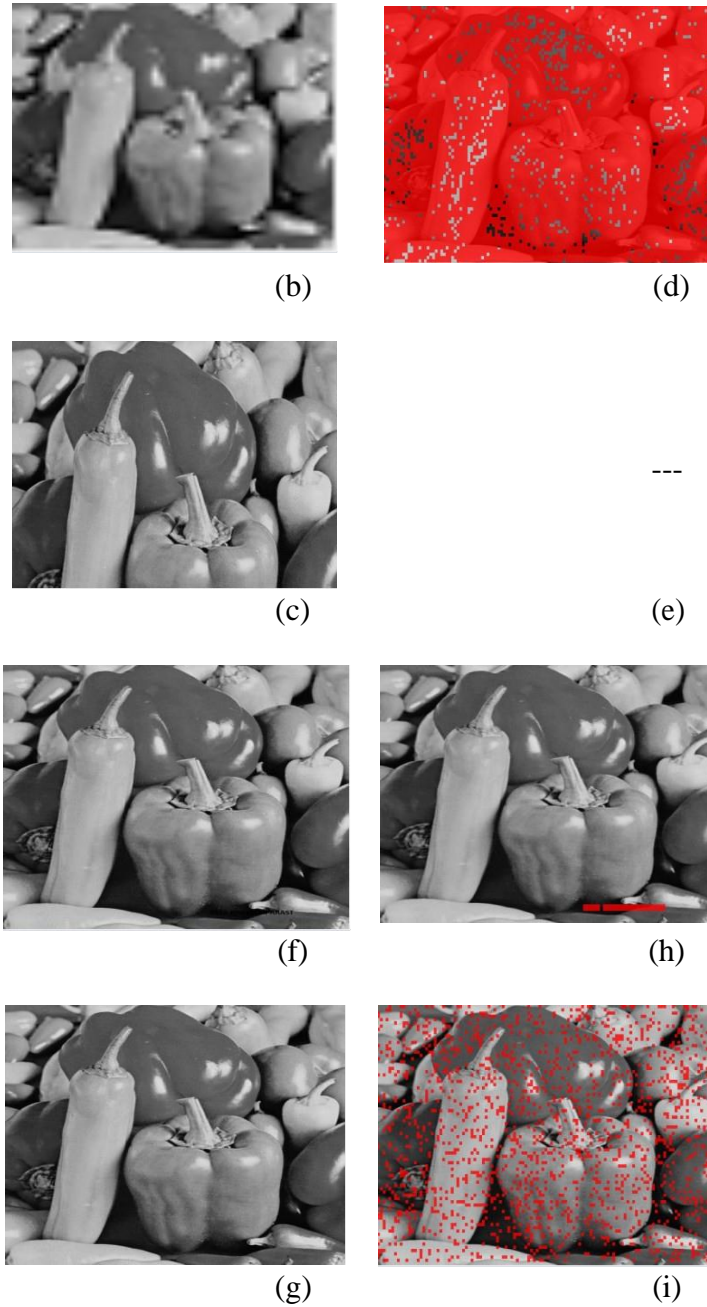
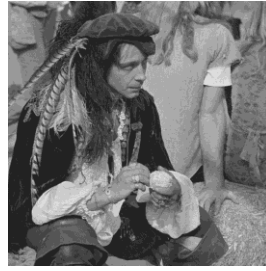


Figure 5.13: Pepper ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

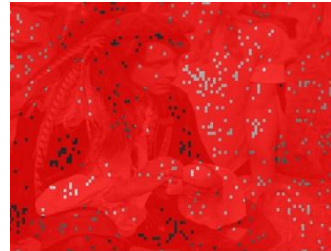
The Pirate image has been tested under Flipping and Double Flipping and the other results shown in Figure 5.14. Flipping could not be recognized, but Double Flip could be detected by ISCH.



(a)



(b)



(d)



(c)

(e)



(f)



(h)



(g)



(i)

Figure 5.14: Pirate ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

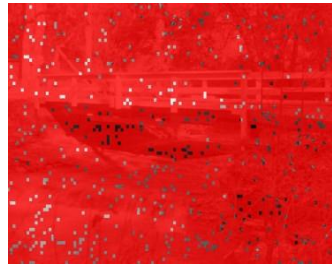
Walking Bridge is the last tested images, which have been under the four mentioned demonstration tests. The output results show the same results as Pirate Image.



(a)



(b)



(d)



(c)

(e)



(f)



(h)

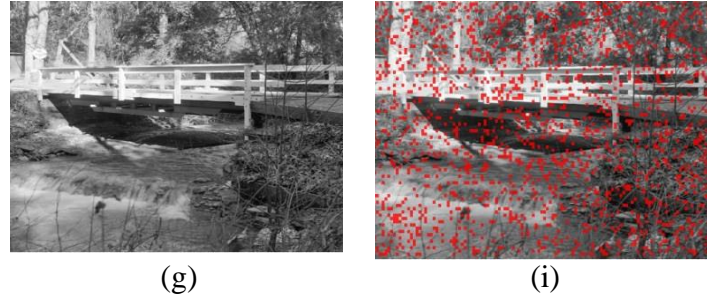


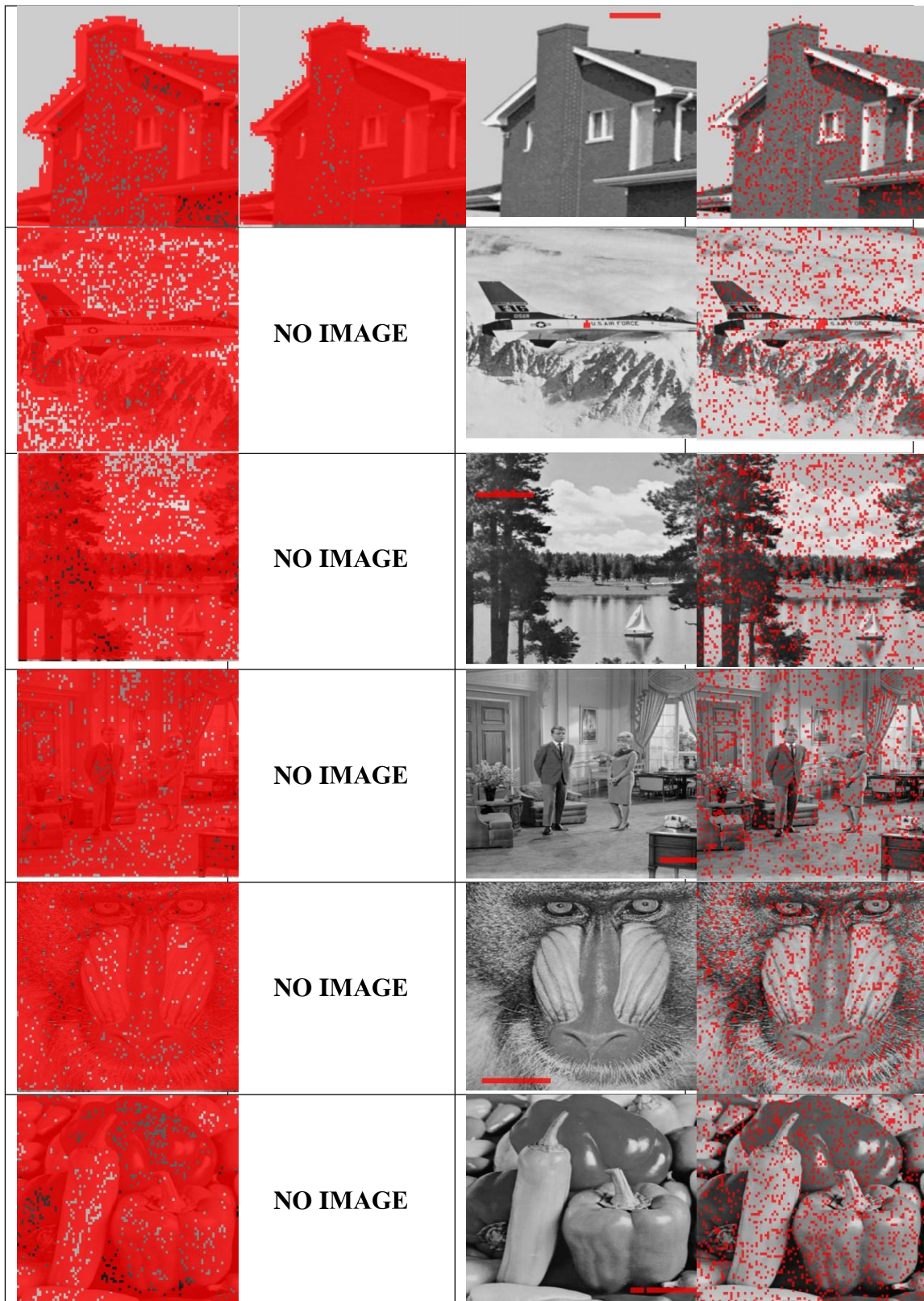
Figure 5.15: Walking bridge ISCH results, (a) original image, (b) resize, (c) resize result, (d) crop, (e) crop result, (f) text manipulation, (g) text manipulation results, (h) format change, (i) format change result

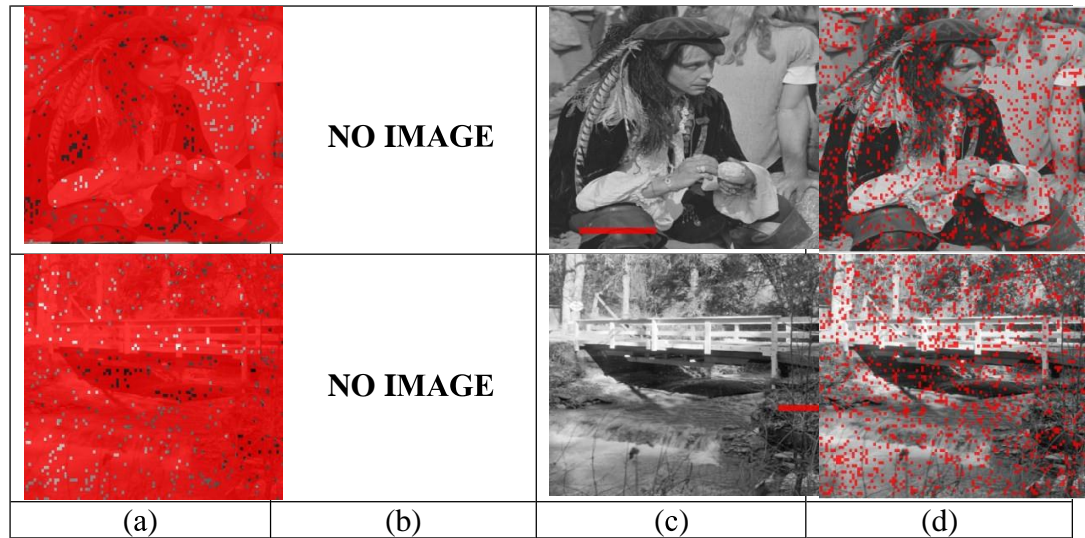
5.2.5 All Tested images Differentiation Recognition

Figure 5.16 illustrated the Differentiation Recognition of all tested images, and shows the similarity between the output results of the ISCH system. The output results show Resizing, Text Manipulation, Format Changing to JPEG have been detected by ISCH, but in Cropping, results show that in Figure 5.11 to Figure 5.22 ISCH could not find the similar image in the test cloud database. Hence, the proposed system is not fully robust on the cropping manipulation.

Table 5.6: ISCH test results for each manipulation, (a) Resizing, (b) Cropping, (c) Text manipulation, (d) Format changing

Resize	Crop	Text Manipulation	Format Change





According to the results which came from Figures 5.16 it can be conclude that the ISCH system is robust under Resizing and Text or any tiny brushing manipulation. Cropping manipulation results show that among ten tested images, only three of them could be recognized by ISCH system as a similar image in the cloud database. Hence, the ISCH system is not reliable on the Cropping test. The Flipping test results also show that the image, which could be recognized by ISCH, was the House. So ISCH cannot be used in this type of manipulation.

Format changing has been tested on the testing images. Changing the format to JPEG has been done on all test images. For JPEG format testing, all images could be detected by ISCH, but for better results other format changing was tested. The test results and their transformed format can be seen in Figure 5.11. Figure 5.11 shows the result of testing Format Changing Manipulation for the Camera Man test image. PNG, GIFF, BMP, JPEG are the tested formats in these test images which have been shown in (a), (b), (c), (d). The output results show that ISCH could recognize all manipulation with the above formats on the mentioned test image. The results would be the same in the rest of test images, which shows that the ISCH system is also robust enough under Format Manipulation testing.

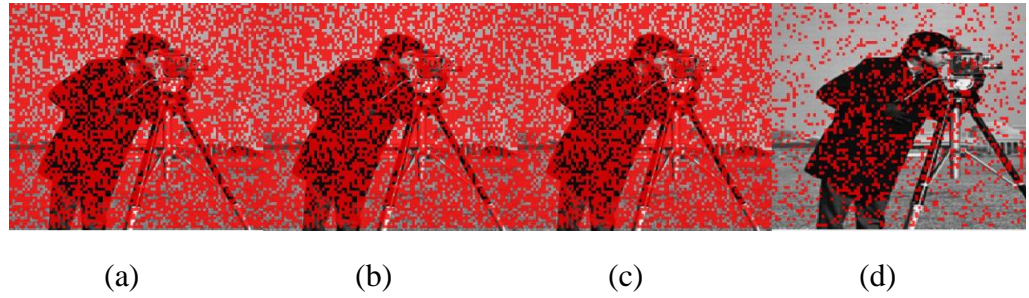


Figure 5.17: Camera Man under format changing manipulation, (a) PNG format, (b) GIFF format, (c) BMP format, (d) JPEG format

5.2.6 ISCH output results

The following table is the result of testing the examined standard images of the ISCH system. By testing each uploaded image in ISCH system, three items will be shown by choosing each image, which has been found as a similar image. First, the number of similar images and second similarity factors (SF), which has been calculated from 9600 bits that came from the sample acquisition in section 4.2.2.1. The third factor is the similarity percentage (SP), which has been calculated from the similar bits of each image. The result of the second and third part of the ISCH system has been shown in Table 5.6. Resizing to 50%, 30%, 10%, Cropping 20%, 40%, Text manipulation and Format Changing manipulation (To JPEG) has been tested and calculated for each of the demonstration tests. The same results from changing the format (Format Manipulation) on the formats in addition to the JPEG format, has been shown in Figure 5.17.

Table 5.6: Result of comparison between tested images in ISCH system

	Resize to 50%		Resize to 30%		Resize to10%		Crop 20 %		Crop 40%		Text Manipulate		Format Manipulate	
Camera Man	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	1339	13%	2047	21%	1684	17%	937	9%	706	7%	9547	99%	7821	81%
House	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	3308	34%	3623	37%	3088	32%	2874	29%	2971	30%	9556	99%	8553	89%
Jetplane	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	1399	14%	1779	18%	1493	15%	0	0%	0	0%	9558	99%	8012	83%
Lake	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	956	9%	1433	14%	861	8%	0	0%	0	0%	9544	99%	7996	83%
Lena	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	969	10%	1776	18%	923	9%	2854	29%	516	5%	9545	99%	8030	83%
Living Room	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	946	9%	1423	14%	720	7%	0	0%	-	-	9544	99%	8006	83%

Mandrill	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	0	0%	0	0%	0	0%	-	-	0	0%	9552	99%	8025	83%
Peppers	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	-	-	-	-	890	9%	-	-	0	0%	9554	99%	8010	83%
Pirate	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	-	-	-	-	660	6%	-	-	0	0%	9562	99%	7921	81%
Bridge	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP	SF	SP
	-	-	640	6%	0	0%	-	-	0	0%	9557	99%	8116	84%

Table 5.6 illustrates the output results of the ISCH system. According to the results in Table 5.6 detecting the manipulation in changing format, the system is robust and reliable enough to this kind of manipulation. Text manipulation has also almost the same results, which has been 81% to 89%, although, the text position was not in the same direction in each image. According to the results, resizing to 10% also could be detected by ISCH in all images, except in the Walking Bridge, which could be detected in 30% resizing. So it can be conclude that the ISCH system is also reliable on resizing and any kind of brushing manipulation like texting, and it also shows that any tiny brushing manipulation can be recognized in ISCH. During the examination, results show that the Cropping test was detected in three of the tested images (Lena, Camera Man and House).It can be concluded that ISCH is not reliable enough through the cropping manipulation.

Figure 5.18 illustrates the results of the resize manipulation of ISCH, which has been tested on ten standard uploaded images. This figure shows that the similarity factors of the ISCH mostly divided between 500 and 1500 pixels. The results of testing the House image were drastically different, because of the similarity of the pixels of the House.

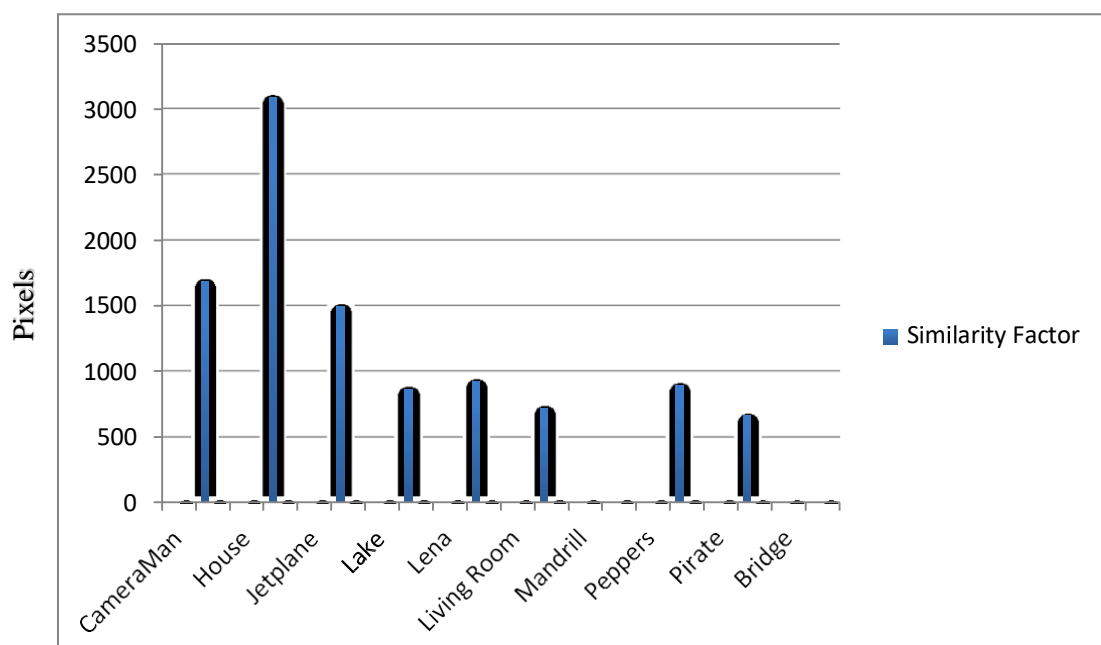


Figure 5.18: Resize manipulation results of ISCH

Text manipulation results of ISCH step are illustrated in Figure 5.19, The Figure shows that the ISCH is reliable in any brush or text manipulation. The differences between the lowest results to the highest one are slightly different.

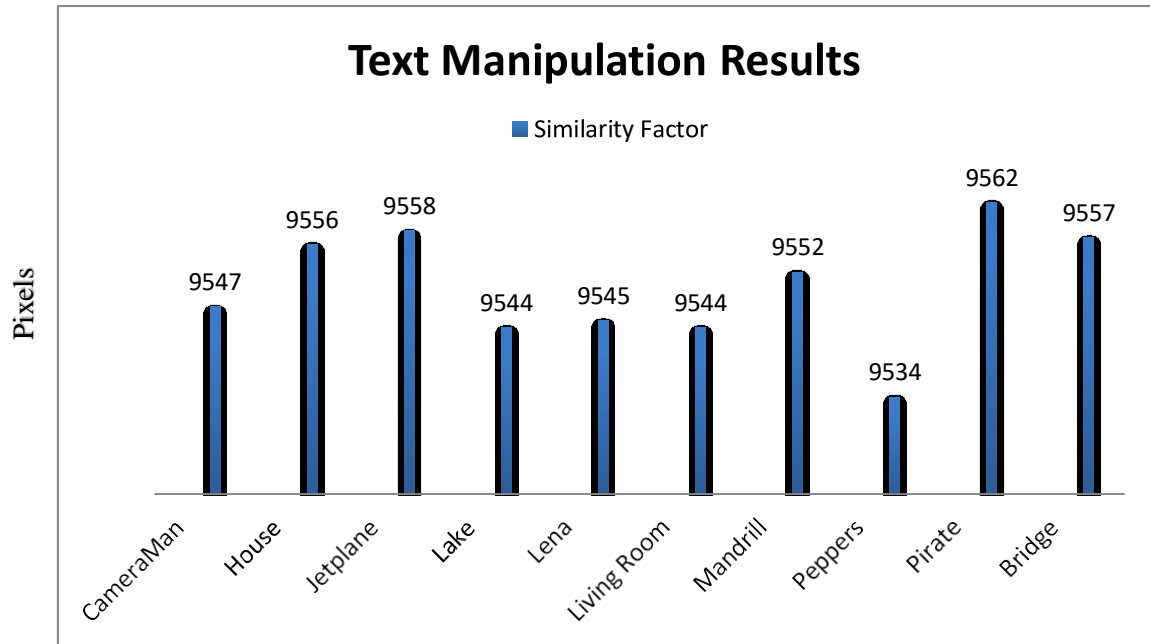


Figure 5.19: Text manipulation results of ISCH

Figure 5.20 shows the results of ten standard tested images in changing format manipulation. In this analysis the standard image format has been changed to JPEG format, which is a compressed format that could change or lose a lot of pixels from the original image. The results show that ISCH is reliable and powerful enough under format changing. The House image has gained the highest similarity factor because of the simplicity of its pixels in comparison of the other images.

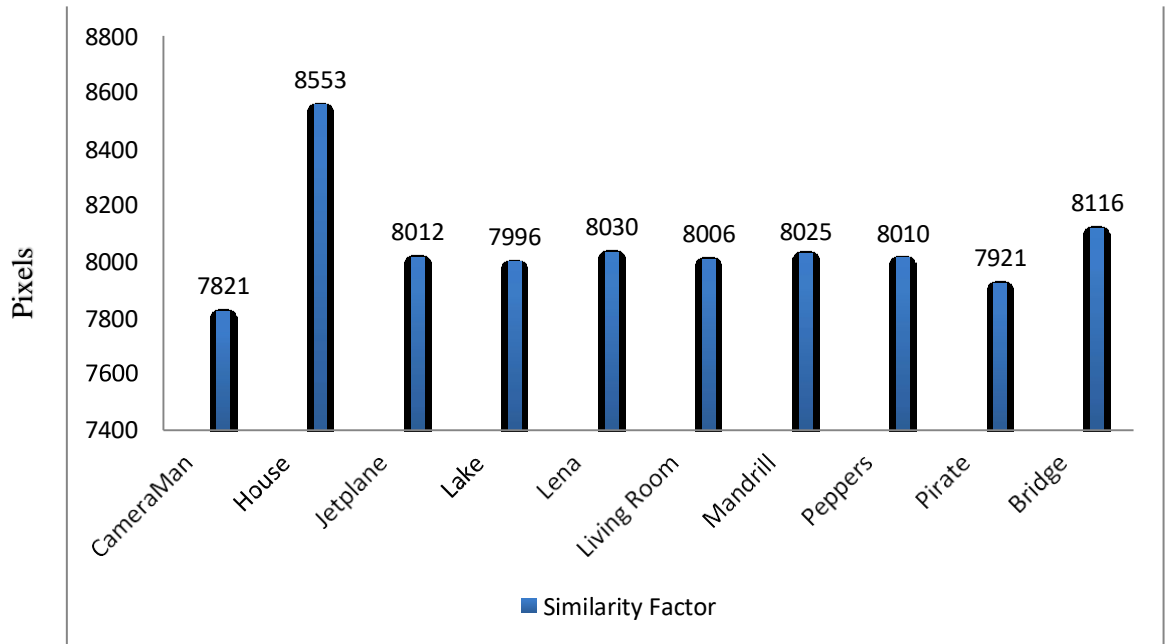


Figure 5.20: Format changing manipulation results of ISCH

5.3 EXPERIMENTAL RESULTS FOR THE WATERMARKING PHASE

In the watermarking functionality, the DWT algorithm has been used to embed the bit stream code, which has been taken from SHA512 hexadecimal code that is a combination of the three dimensional features (CFDH). The watermarking has been done in the frequency domain with the DWT algorithm because of having a better robustness form factor. The DWT method divides the cover image (Authorized Image) into four layers, which are LL, LH, HL and HH. The test message (CFDH) is embedded into the HH layer of the cover image. The image sizes are $512 * 512$ pixels; the embedding will be done on HH, which is $256 * 256$ pixels, that will be 65535 bits. The test message is also 512 bits. The image size of the HH layer is x, which is 65536 in bits will be divided into y, which is 128, and the result will be z, which is 128. The HH layer size is put in parameter x which is 65536. Parameter y will be filled up by the message size, which is 512 bits. The Results will be 128 bits, which will be replaced by z. The test message will be embedded into the cover image every 128 bits to have the best PSNR result.

To evaluate the result of the watermarked image, PSNR has been used to mark the watermarked image with features. The PSNR is one the best evaluation

methods in watermarking systems to estimate the quality of the watermarked images. A reliable watermark is that the one which has the PSNR more than 30 decibels. The following table illustrates the PSNR of the examined standard images, which have been used in this research.

Table 5.7: PSNR result of embedded images with CFDH

NO.	IMAGE NAME	PSNR OF W.IMAGE (dB)
1	Cameraman	71.3943
2	House	74.4646
3	Jet plane	64.4702
4	Lake	57.4402
5	Lena	64.3343
6	Living Room	59.2661
7	Mandrill	65.0687
8	Peppers	59.5659
9	Pirate	60.0222
10	Bridge	52.9055

Figure 5.21 shows the output results, which have been coming out of PSNR quality test. Results show that all tested images have PSNR more than 50 dB, which is more 30 dB. The least rate has belonged to the Walking Bridge image in comparison to the highest rate which belongs to the House with the rate of 74 dB. The reason could be because, the House image has less difference between its pixels in comparison with the Walking Bridge and it is more unevenly distributed.

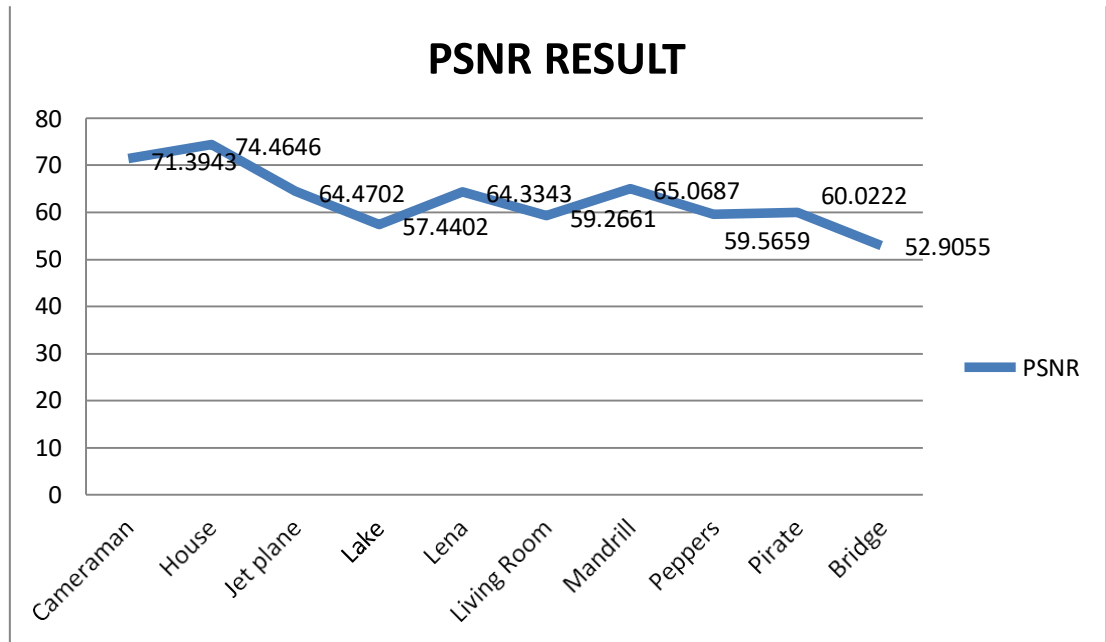


Figure 5.21: output result of the PSNR quality test of embedding the CFDH in tested images

By comparing the results from Table 5-1 and Figure 5.21, it can be concluded that the PSNR values are generally reliable due to the standard results, which should be more than 30 dB. It can be found that conducting DWT decomposition is reliable enough to embed CFDH features into the uploaded images. The pseudo code in table 5.21, which has been used to calculate PSNR is given below.

Table 5.8: PSNR Calculation Pseudo code

START	
-	Read first image
-	Read second image
-	Convert first image to double
-	Convert second image to double
-	IF (size of first image \neq size of second image)

```

-      Display error

-      Return zero as PSNR value

-      END IF

-      Calculate number of rows and columns of first image

-      Set sum to zero

-      FOR number of rows

-      FOR number of columns

- Calculate, sum = sum + (first image (number of rows, number of
columns) – second image (number of rows, number of columns)) ^2

-      END FOR

-      END FOR

-      Calculate, PSNR value = -10 × log10 (sum / (255 × 255 ×
number of rows × number of columns))

-      Return PSNR value END

```

5.3 SUMMARY

In chapter 5 the artefact evaluation and analysis has been completed. According to the proposed framework each step has been defined and explained. First, the HECH results of testing the uploaded image have been analyzed. Second, ISCH results has been fully tested and analyzed. Finally, the watermarked image PSNR has been measured to identify the robustness under each test. Hence, the Watermark Existence Check, Hash Existence Check, ISCH system and watermark embedding has been demonstrated and tested. In addition feedback from three experts has also been received and will be used for design improvement. The proposed design must fulfill the objectives of the project, which is finding the rightful ownership of objects and images in the cloud environment. In chapter 6 the hypotheses are to be tested and the research question answered based on the results delivered in this chapter. The importance of chapter 6 is the reconciliation of these results with the more general literature assertions found in chapter 2. Such a positioning will put these results into context and also moderate the research contribution.

Chapter 6

Research Contribution

6.0 INTRODUCTION

Chapter 5 has provided the statistical and the naturalistic evaluation of the artefact that was presented by design and implementation in chapter 4. Chapter 6 is structured to take the evidence presented in chapter 5 and use it for qualitative hypothesis testing. In addition the research question is answered by considering the outcomes of the hypotheses tests and other evidences accrued during the research process. The answer to the research questions are delivered in terms of the expectations of chapter 2 and chapter 3; and hypotheses of chapter 6. These discussions then lead to a statement regarding the contribution of the research that is for theory and for practice. The chapter concludes by a critical review and evaluation of the design science methodology.

6.1 HYPOTHESIS EVALUATION

In Chapter 3 a set of hypotheses were formulated to assert the researcher's proposed theory developed from the literature review in Chapters 2. In this section relevant evidence is evaluated from within the collected and analysed data of the obtained experts' written and oral feedback, as well as the statistical results from the practical tests of the artefact and the researcher's observations as they were articulated in Chapter 5.2. The relevant points will be referenced and cross-examined to determine a verdict for the hypotheses. The relevant points are presented in text, as shown in Table 6.1. The text will be analysed with a qualitative approach quasi-judicial method, where a rational argument is used to interpret the data in searching for 'for' and 'against' statements that prove or refute the hypothesis in question. The qualitative approach relies on a weighted judgment regarding the force of arguments for and arguments against the hypothesis.

Table 6.1: Hypothesis Evaluation

H1: DWT method in the transform domain is the most resilient and robust for the cloud environment.	
For	Against
<p>In the literature review, it was discussed and argued, that Digital watermarking is a technology for copyright protection, which embeds the copyright information into digital production to avoid being tampered, peculated, and illegally copied. All aspects and techniques in watermarking has been elaborated.</p> <p>To ensure quality outcomes and goals are achieved; Research Method process should be executed as part of an assurance program. The potential watermarking techniques to be used has been considered and illustrated in Chapter 2, Figure 2.5. they have been then explained and elaborated in Chapter 2, Section 2.7.1. As a result the potential one to be used in cloud environment has been chosen and elaborated as the first phase of the artefact development in the research methodology, chapter 3, section 3.4.2.</p> <p>The experimental results in Chapter 5, section 5.3 with the researcher's observations, were critiqued and articulated showing the robustness and resilience of the adopted watermarking techniques with the research contribution. Corresponding mitigating measures are reviewed accordingly and ensuring their effectiveness and efficiency in the same section. However, implementing an effective program comes at cost and has a number of implementation and maintenance challenges</p>	<p>No reference found that refute the stated hypothesis.</p>
<p>Verdict: ACCEPTED</p> <p>The weight of evidences in favour of the RODS watermarking technique which provides a better resilience and robustness for the cloud environment.</p>	

H2: The proposed novel artefact provides strong ownership protection.	
For	Against
<p>Experts' written and oral feedback, were critiqued and articulated in Chapter 5, Table 5.2 to Table 5.4 and the researcher's observations, were also shown and articulated in Chapter 5, Table 5.5, in the list of artefacts evaluations criteria and their corresponding questions:</p> <ul style="list-style-type: none"> - Goal> Efficacy : Q1 - Goal> Validity: Q2 - Environment> Consistency with Organisation > Fit with Organisation: Q1 - Environment> Consistency with Organisation > utility: Q1 <p>The experts with their years of relevant work experience indicated the importance of having a integrated system to ensure the user's copyright protection will be assured. Furthermore, when some of the internal or external environment attributes change, it results in the changing of corresponding underpinning assets' value and other vital aspects.</p>	<p>No clear and direct statement found that contradicts this hypothesis.</p>
<p>Verdict: ACCPTED</p> <p>Given the noted positive evidence and the lack of negative evidence then the H2 hypothesis is supported, and accepted.</p>	

H3: The proposed Authentication method improves rightful ownership protection in a cloud environment.	
For	Against
<p>The experimental results in Chapter 5, section 5.2.4 were critiqued and articulated showing the reliability of the Rightful Ownership Detection System (RODS) under different tests and attacks. The unique Image Similarity Check (ISCH) also has been tested and challenged in the same section.</p> <p>Experts' written and oral feedback in the other hand, and the researcher's observations, were critiqued and articulated in Chapter 5, Table 5.4, in the list of artefacts evaluations criteria and their corresponding questions:</p> <ul style="list-style-type: none"> - Goal> Consistency with people> Utility: Q1 - Goal> Consistency with people >Understandability: Q1 - Goal> Consistency with people >Understandability: Q2 <p>All experts, were agreed that the RODS has a very good potential to be used in a larger scale and it can be commercialised and be used by more cloud service providers and it provides a systematic way of creating required functions and processes, assessing associated tasks and placing necessary mitigating measures to ensure desirable outcomes.</p>	<p>No reference found that refutes the stated hypothesis.</p>
<p>Verdict: ACCPTED</p> <p>The presented evidence supporting this hypothesis carries more weight than the disapproving evidence, leading to the conclusion that H3 is supported and accepted.</p>	

6.2 ANSWER TO THE RESEARCH QUESTION

In Chapter 3.1.1 the research questions were stated to be:

1. What preparation methods improve ownership protection in cloud environments?
2. What could be a suitable management framework to increase ownership protection in a cloud environment?
3. What tests show the reliability of the proposed method in a cloud environment?

In this section the evidence compiled from the hypotheses tests, relevant figures, and chapter 5 analysis will be used to find answers.

6.2.1 Question 1

The preparation methods to improve ownership protection in the cloud environment have been set out in chapter 3. In the figure 3.9 the implementation diagram specifies the actions that must be undertaken in order to achieve the watermarking of an image. In hypothesis 1 it was found that effective performance was established by adopting the watermarking technique concerned which provided better resilience and robustness in the cloud environment. To achieve these levels of performance figure 4.2 outlined the preparation flowchart. Here the uploaded object to the cloud had to go through a logical sequence of decisions and actions in order to be prepared and ready for resilience. In figure 4.4 the watermarking embedding processes is specified. This process had three security features that were required to prepare prior to the CFDH consolidation. The preparation methods then lead to the selection of DWT in bathing and the secure watermark being available for the cloud services.

Hence question one is answered by consideration of all of these aspects. In simple terms a lot of preparation goes into the algorithm before a watermark is ready and available for cloud usage. This includes architecture, design, and computational algorithms. Also the potential watermarking techniques to be used in cloud environment has been identified and then justified in Chapter 3.4.2.1. To answer to the research question 1, hypothesis 1 specifies that the DWT method in the transform domain is the most resilient and robust for the cloud environment.

6.2.2 Question 2

To answer to the second question a suitable management framework requires identification. After identifying the suitable watermarking method, the research then focuses on designing a unique artefact to be implemented based on focusing in improving the ownership protection in the cloud. The design of the artefact has gone through different phases (shown in Figure 3.5) based on the adapted DS methodology. The implementation diagram illustrated in Figure 3.9 has been produced with the main purpose of implementing the artefact to enhance the copyright protection (shown in Chapter 3, Section 3.4.2.3). An artefact and management framework has been proposed in Chapter 3.4.2.5 to answer question 2. The proposed artefact has different security and Authentication features as elaborated in Chapter 4.1. These have been used to enhance the reliability of the implemented system (RODS). The RODS defined is specifically designed and implemented for the research main aim and it has included features such as the Image Similarity Check (ISCH).

In figure 3.2 the traditional architecture of Cloud services is specified. In contrast figure 3.8 has a redesigned architecture which shows how the cloud provider and the end user can interact in secure sessions. In addition figure 3.11 outlines a suitable management framework that can increase ownership protection in a cloud environment. Furthermore hypothesis 2 shows that the proposed novel artefact provides strong ownership protection. These two elements of evidence indicate that a suitable management framework can be established but all of these are new works. The innovation from this research suggests that current security techniques and mechanisms have to be redesigned and put into new architectures if they are to be effective in cloud environments. A suitable management framework is found in figure 3.11.

6.2.3 Question 3

Two types of tests have been completed. The first was statistical and the second naturalistic by getting industry experts to give feedback. In chapter 5 table 5.4, the critical reflection on expert value results are summarised. This feedback leads to the shaping of the artefact and also suggestions for further testing. The internal reliability of the artefact is presented in chapter 5.2 is a series of reports on the consistency of

deliverables from the embedding of a watermark in different cover objects. These tests show that the RODS consistently delivers security features across the spectrum that has been tested. For example, the image similarity check was shown to be consistent. This is where the similarity percentage was calculated from similar bits of each image and compared with the other managerial action effects. The house image performed the best.

Furthermore the reliability was established in the experimental results at the watermarking phase. The PSNR values all came out above 50 dB which is more than the 30 dB cut-off. This indicates that the CFDH is reliable as an embedding algorithm and that it is not only consistent, but also performs at a very high level. The only variations were found in the distribution of pixels within an image. Those that were more widely distributed performed slightly less well than those of the more concentrated pixels.

6.3 DISCUSSION OF FINDINGS

Cloud computing introduces a range of risks a user has to reconcile with their appetite. The user also has expectations for privacy and ownership protection that may not be met in many Cloud computing environments. The present purchasing arrangements for services obscure the potential loss of control the user may experience. Sales agents are employed to sell the service and may not be informed of complex service arrangements. Service level agreements within and between service suppliers are service centric and have many interpretations across jurisdictional boundaries. As a consequence users have generally taken responsibility to provide security mechanisms such as encryption for their data. The approach has left a legacy of issues around the effectiveness of such measures and the viability of variation in a controlled environment. The research completed suggests that if service suppliers take responsibility for information security then the variation in security mechanism performance can be reduced and suitable mechanism may be tested by the service provider prior to use to assure user data control.

The research specifically focused on five management attacks that can be expected in a Cloud service environment. The artefact designed in Chapter 3, Section 3.4.2, shown in Chapter 3, Figure 3.11 and elaborated in Chapter 4, Section

4.1, was resulted from the selected watermark that had been prepared with these attacks in mind. It had three layers and embedded security features explained in Chapter 4, Section 4.2, to promote the longevity. The performance showed the torrid nature of policy driven attacks. No watermark escaped degradation and the best lost 30% of the intensity. This suggests that the problem identified is a serious issue and further work is required to assure robust preparation algorithms for future artefacts. The worst case lost almost 50% of the intensity suggesting that the nature of an image has an influence on performance (Chapter 5, Section 5.2.6). Further questions arise regarding the extent to which an artefact may be exposed to and in such an environment before the intensity drops below detection. Metrics such as duration, respective occurrences, pixel intensity and so on can be valuable indicators for forecasting an artefact robustness. In this research cloud technical attacks were out of scope and these can be investigated in future iterations of the research. The management attack results suggest that some images may lose further intensity when exposed to further attacks and reduce the positive impact of these findings. It can be anticipated that all of the managerial attacks will be present and some technical. In such an environment information regarding the artefact performance is required before a complete solution to the research problem is reported. However, the results give a strong indication that managerial attacks can be overcome and that the artefact has potential for further development (Chapter 5, Table 5.4). The suggested redistribution of responsibility for security to the service provider also places on them the responsibility to develop a robust solution that users may choose to use or used by default.

The research methodology has achieved the aim of answering the research question in a series of partial solutions and a forecasted further round of testing for technical attacks. As such the methodology has delivered against the six phases of activity. The applicability to IS security research has been demonstrated. The concept of Cloud security and relevant mechanism performance are still maturing in the literature. There are many gaps and big assumptions that have come from using security mechanisms from other environments in the Cloud. The Cloud represents a new context in which to design security solutions. One mechanism have been taken and a selected range of attacks to show how the DS framework can be applied for achieving IS security research. The DS framework has given the flexibility to

try and to test assumptions and then when complete the ability to loop back and to seek improvement, answers to questions raised, and to address incomplete parts in this research. As such DS as a framework and a methodology is an effective approach for managing security mechanism research in new environments and contexts.

The issue of rightful ownership and inter jurisdictional issues surrounding the cloud will not go away. These are material concerns that have eroded trust in cloud services but may be negotiated by better understandings and mitigated by better application of security technologies to the new environment. A different system architecture has been proposed in this research to better fit the watermark security technology into the cloud environment and also built an artefact that has potential to fit the new environment. Such innovation may become common practice as cloud services move out of their infancy and greater trust is gained by more users. The users who unwittingly use cloud services by default also require assurance that their privacy and ownership is protected. Further research and development are required to grow the effective application of security technologies to the cloud environment.

6.4 RESEARCH CONTRIBUTION

In Chapter 3, sub-section 3.2, it was argued that in DSR the produced artefacts are meant to serve an objective and must produce value for the specified problem. The value will be verified when the artefacts are evaluated. Artefacts must be novel and a new knowledge must be added to the domain. The research outcomes must be communicated to an adequate audience of technical people experienced in the same field as well as being statistically evaluated by going under the specific mitigation measurements. The DS guidelines listed in Chapter 3.2, regarding communicating research outcomes to technology and management oriented audiences, where the foundations for theory leading to either new or enhanced existing knowledge, is added to the knowledge base. Section 3.2 then shows the DSR process stages, in which ‘Communication’ is noted as the last stage of the process, where the outcome of the research is communicated through scholarly and professional publications. Furthermore, the DSR roadmap depicted about communicating findings, which requires preparation and outcomes to be articulated before communicating them through the possible means.

In this section (Sub-section 6.4.1 and 6.4.2), the DSR findings are to be articulated to targeted audiences in theory and business. Sub-section 6.4.1 outlines the research contribution to theory, while sub-section 6.4.2 explores the research contribution to business from practitioners and organisations' perspectives.

6.4.1 Contribution to Theory

In this research the DS methodology was adopted following the DS guidelines shown in Figure 3.3. The research progress has been benchmarked against the tasks adopted from the DSR roadmap developed as illustrated in Figure 3.5 and Figure 3.6. The theory for DS is well developed and articulated in the literature cited. Consequently the developed artefacts of the design solution were evaluated against criteria articulated from the adopted DS and shown in Figure 3.11, for a theory that is already well developed. This research confirms that DS theory is applicable for guiding the development of security artefacts. It also shows that DS is a trustworthy guide for research and for achieving the transfer of ideas from thought and into practice.

The adoption of a methodology to select the literature in chapter 2 is also proved valuable in focusing the research onto key themes and problems, and then identifying gaps in the missing parts in the current literature (see figure 2.1). Literature Research Questions have been used for determining the content and structure of the systematic review (SR), for designing strategies, for locating and selecting primary studies, for critically evaluating the studies, and for analysing their results. The research literature review is concept-centric as it classifies and presents the publications according to the privacy area they address. The DS methodology grounds the production of artefact in its theoretical context before the pragmatic implementation.

The DS methodology is both theoretical and practical in application. In the first instance there is a lot of literature to be read and analysed before a researcher can start to effectively implement a DS research project. There are also many choices that have to be made with regard to the particular problem and subsequent project. In this research, the researcher have reported each phase, each step, and each process that he went through in order to implement the DS theory. The researcher have also reported the transfer of theoretical knowledge into practice.

Much of DS theory is found in the underlying pragmatic philosophy that is embraced. For example the concept of continuous improvement and the ability to receive from feedback loops, and to step back in the development process to prior steps is all part of a pragmatic approach. In this research the researcher has followed the theoretical advice of some of the top academic scholars with regard to the theory of DS. As a consequence the report in this thesis contributes further evidence that DS theory can be put into practice and it provides a use case.

Throughout the study the DS theory tended to be confirm rather than refute the intentions of the research. It was a facilitator and not an obstacle to progress or attainment of the research objectives. The theory provided the basis for guidance and direction that facilitated critical reflection and theorising of the problems and the solutions as the research project progressed. In this way DS tended to be a fluid continuum of theory and practice reticulated and reflecting upon one another for the enhancement of the development of the artefact. The consequence was that the researcher was constantly thinking and reflecting upon the theory and the context, and try not only to maintain the direction but also a successful solution. The DS methodology hence was particularly helpful in this situation where the problem solutions were tentative and the investigation exploratory. The consequence was that the theoretical planning and guidance can be passed to another researcher who can either replicate or vary this application and to build their own solutions.

6.4.2 Contribution to Practice

As noted in the introductory paragraph that DS research outcomes are to be communicated to management through professional publication. For that purpose, this sub-section summarises this research's contributions to practice from the organisations' and practitioner's perspectives when using the methodology. The DS methodology acts as a guideline toward improving practice. The options and choices that are provided for the practitioner (see figure 3.3 for example) require training and previous experience so that the best decisions are made. For example, a practitioner has to decide where they will enter the process iterations. Such a decision requires an understanding not only of the problem but also the processes through which solutions may be discovered.

When an artefact is presented to the practitioner they must first decide where it fits. Artefacts such as the RODS has already gone through to developmental cycles of the DS methodology and hence could be adopted from the “design and development initiation” or the “client context initiation”, for further development. Both of these entry points are theory driven and require the practitioners to develop critical reflection and critical appraisal skills that can adequately address the problem and issues that may arise at the current stage of development of the artefact. This creative process is theoretical and may be undertaken in teams, group work, or through independent critical reflection; but each process will lead to better theorising of the artefact and its integration with in the context of use. To a practitioner the opportunity for improving the performance and the suitability of an IT artefact, presents an opportunity for better value realisation and work system productivity.

From a practitioners’ points of view, this may be an end user or a technical person in the cloud service supplier organisation. For the end user sufficient trust must be gained from the cloud service provider before the RODS can be successfully implemented. In practice trust as a key element in facilitating cooperation and actions between participants. At present end users are often doubtful about the security and the secure practices that may be encountered in a cloud service. The RODS is an opportunity for the cloud service providers to enhance the trust factor and to relieve the end user of the burden of doing their own watermarking prior to uploading. From the cloud service provider perspective the RODS can not only enhance the trust factor with the end user but also increase business. Successful security mechanisms allow end users to do their business seamlessly and to achieve the objective of their interaction.

6.5 CONCLUSION

In chapter 6 the reported findings from Chapters 4 and 5 were examined in relation to the research hypotheses and questions presented in Chapter 4. The evidence gave grounds for evaluating the hypotheses proposed in Chapter 4 as well as answering the research question. Qualitative testing of the hypotheses resulted in validating the proposed hypotheses with enough supporting evidence that conclusions could be drawn. Subsequently, the answers to the research questions were gained and these were used to inform the discussion from these findings. The discussion led to the critical evaluation of both the findings and the application of DS research methodology. It was concluded that both in theory and practice DS has a contribution that is invaluable for researchers and practitioners.

The following chapter 7 will tie together all these points and conclude the thesis by presenting recommendations for future research.

Chapter 7

Conclusion

7.0 INTRODUCTION

In Chapter 6, the research contribution has been discussed by the evaluation of the hypothesis and a justification of the findings. Research questions have been answered and the research contribution from both the theory perspective and practitioner (natural) perspective have been presented.

Chapter 7 is structured as follows: Section 7.1 summarises the research journey by explaining the challenges, the Methodology, the Discovery and Innovation contributed, and the personal impact of the study. Section 7.2, then revisits the limitations of the research to assure moderation and reasoned expectations for its use. Section 7.3, closes the thesis by elaborating what future research works can evolve from this completed project.

7.1 THE RESEARCH JOURNEY

This journey of the researcher from the beginning of the research to the end is an important learning contribution that needs to be stated. The journey was a challenge to the researcher who initially suspected that the cloud environment had many vulnerabilities, and that these vulnerabilities would impact negatively on both the end user and the cloud service supplier, unless better managed. The fact that a singular contribution has been made is the result of the focus and the narrowing to a target that a PhD research project delivers. I'm confident that the artefact at this stage demonstrates both the theory and potential practice that can increase security around rightful ownership of objects in the cloud environment, and also as a contribution to the discussion of digital rights. To communicate the journey the researcher will break it into the phases of initiation, methodological selection, challenges faced, innovation and contribution, and where the journey will go from here. These points are covered in subsections 7.1.1 to 7.1.5.

7.1.1 Initiation

The researcher began his journey by coming to New Zealand to start a fresh topic in security sciences. Prior to this, he had completed a Master's thesis in Malaysia with first class honours in security sciences. It seemed to the researcher that the cloud environment was presenting difficult challenges for traditional security theory. Hence, he needed to find a supervisor who understood the issues being presented by cloud technology challenges and also the latest theory development modes in security sciences. The journey began by developing a PGR2 proposal in an area where there did not seem to be a lot of coverage from the literature the researcher had read previously.

The serious concerns the researcher read regarded privacy issues. In the cloud environment there seemed to be little concern about protecting the ownership of intellectual property when the major thrust in cloud computing was to provide a ubiquitous system that was distributed without consideration of jurisdictions or security, law and controls. This to the researcher, was a big problem. For example with copyright protection there seem to be little concern beyond what the end user could contribute to their artefacts before everything gets uploaded into the different cloud environments. For businesses such as photographic studios, this is a major problem. Their business is images and yet these images could be taken without permission and reused in different jurisdictions because of the reach of the cloud. Hence, it seemed sensible to the researcher, to develop tools and techniques that will begin to address these problems.

7.1.2 Challenges

The biggest challenges the researcher faced were the lack of similar works in the e-library, because there seemed to be an emphasis in the literature largely on the Cloud service provider and very little on the end user. In addition the researcher faced practical problems of establishing the testbed in which to develop his prototype and then to get feedback from experts in industry in order to understand, how he could better improve this tool. The biggest issue here was a trust issue. It was difficult to get people outside of the laboratory to trust what he was doing. The researcher had to work through professional networks, the supervisor, and international networks in

order to get the right levels of expertise and experience from people that would give me the right feedback.

In addition, the researcher had to have a commercial testbed in which to demonstrate the different phases of development through the DS methodology for the RODS. However, as he persisted and he gain sufficient support from the different technical services and financial services at AUT, and the project was moved into a position where he could test the theoretical ideas in practice. The whole project demonstrates the taking of a theoretical problem, resolving potential solutions, building an IT artefact, testing the artefact, and then checking the capability of the artefact against a potential solution for the original problem.

7.1.3 Methodology

The design science methodology was selected because the researcher wanted to build and test an artefact that he knew would not be perfect from the start. The researcher had to start from the literature, the ideas and guidance from literature and then interpret this into a software artefact. The best approached for this kind of problem is definitely design science that allows for continuous improvement cycles. It increases the intensity of scrutiny and evaluation of the artefact so that it is slowly moved towards a useful working product. Design science also contributes to the understanding of theory and the solution of problems. Given that there was not a lot of literature and many examples of other people addressing the particular problem that he had selected then he thought this was an excellent incremental approach toward providing better solutions and innovation in this critical area for cloud computing security.

Many people think that design science is too general or insufficiently robust to be applied to abstract problems. The researcher disagrees with this point of view because design science is a powerful guiding methodology for building progressively improved solutions to abstract and practical problems. The way design science works is that it relies on continuous feedback loops that feed statistical and natural data sources to the researcher who then has to process them through an abstract and continuously evolving process of research.

As discussed in Chapter 3.2, the purpose of the DS research methodology is not limited to developing an artefact but also capable to answer research questions.

Depending on the characteristics and the goals of the research, the processes can be shaped to deliver innovative or confirmatory outcomes. DS is solution oriented whereas the other research methodology such Natural Science or Social Science, are problem oriented and the researcher chose DS, because it is solution oriented and not problem oriented. It did help me to review the artefact and be able to loop back and fix the required changes. The current state of the artefact is at a stage that it will always be at. The artefact can always be improved but it any point demonstrates an acceptable level of utility and a tentative solution to the theoretical problem.

7.1.4 Discovery and Innovation

During the research process the researcher had flashes of imagination and visualisation that showed me the solutions he was working on were indeed valuable. The researcher could see that by developing an artefact of the type that has been presented in this thesis, that end users could have protection of their property rights. In addition the cloud service providers could have the confidence that their services would provide rightful ownership protection to a degree that would be acceptable not only to the end user but also for quality control and legal purposes. The researcher's innovation allows a cloud service provider to add an extra attribute of protection for the end user. An end user often has to accept policies that do not cover privacy and rightful ownership protection. The researcher's innovation as it has been demonstrated in this thesis is capable of providing an extra layer of security for the end user and protection of the cloud service provider for yet another area of service.

7.1.5 Where to from Here

The artefact presented in chapter 4 requires further development and adaptation for implementation into different environments. It has potential for commercial use but requires greater trust on the part of the cloud service providers and also implementation into their current software suites. The people who are concerned with digital rights management can also gain considerable value from a prototype such as this. Although the thesis has been completed at this point in time, and the artefact presented as a proof of concept through testing, the artefact in its current state can be taken through further iterations of design science improvement and development for adaptation and generalisation into a multiplicity of situations.

7.2 LIMITATIONS

The fundamental limitations of this research are based upon the methodology that was adopted. In chapter 3, Section 3.5.1 and 3.5.2, the issues of reliability and validity were specified and discussed in relationship to the potential outcomes for this research. The major concerns were the absence of differences in results if the research was to be repeated. In chapter 4, the researcher have carefully elaborated each of the steps and decisions that have been made and the content elements which contribute to the building of the artefact. In many respects the limitations raised in chapter 3.5 regarding reliability have been considered in the presentation this research. However there will always be errors and biases in a study such as this. These errors and biases can be the starting point for further research and further quality improvement of the artefact. Although they are limitations they are also contributors and drivers to further innovation. The variation and opinions expressed by the experts was helpful and has been processed to better improve the reliability of the artefact. On the issue of validity there will always be a gap between the idea and the software produced. This again has been commented on in chapter 3.5.2. The result of a design science development such as this is not perfection but it is utility.

The artefact that has gone through the iterations in this research is a prototype that will deliver the results according to the constraints and the declarations made. There is always a limitation regarding constructed validation because there is a high level of subjectivity in the data being used. However the level of subjectivity in the situation has been reduced by putting the artefact through continuous improvement performance cycles and as much evidence as practical has been provided to justify the decisions that have been made. It is not intended that the artefact can be generalised to every situation. In this instance the artefact cannot be generalised beyond the specific cloud environments described in the tests but the theory and the methodological processes allow for the adaptation into different environments. It is possible though that the artefact can be taken from its current environment and put into new environments, such as commercial environments, in its current state and be readily assimilated for value generation. In this way through continuous improvement innovation and development it can be generalised into a multiplicity of contexts. In many respects the adoption of the design science methodology allows the research objectives to be met and the design to mitigate the limitations of different

contexts by adaptation. The advancement of knowledge from this point in the research can go in a multiplicity of directions. The following section will discuss some of these potential possibilities.

7.3 FUTURE WORK

A number of possibilities for future work arise from the scope reduction in for this current research. Also the implications of what has been achieved can be extended beyond what was achieved to address some of the many other outstanding issues in the area of right for ownership and digital rights. The key points are now listed paragraph by paragraph:

The future development of this research can also focus on different file types and these can be scoped out and tested for the capability in applying the techniques and watermarking communicated in this research.

The evaluation of literature for this thesis suggested that little attention had been paid to the problems created by cloud computing when it came to the protection of intellectual properties and privacy. There needs to be a lot more research into this area and the impact of cloud computing as an information technology in relation to these issues.

The prototype that has been designed can now be migrated into different environments to test for its usefulness. The utility value is that the system developed here can be put into many different areas where people are now using cloud services for their information management. For example in the health sector, the law sector, the education sector and so on.

One of the bigger issues that remains un-addressed is the updating of cloud policies, particularly from the cloud service suppliers end, that include the protection of privacy and other ownership issues. On this matter further research is required at the policy level so that lawmakers and other interests that are involved with computer services can reasonably articulate controls that will benefit both the end user and the cloud service supplier.

The biggest concern in this area is for having practical applications available online for users, and for cloud service providers to have at their fingertips. There needs to be further software development and awareness of the problem in order to

address the biggest issues that still remain untouched. This thesis has made a strong contribution to filling a gap not only in the literature but in the practical implementation of services that will protect rightful ownership and digital rights.

REFERENCES

- Abbadi, I. M., & Martin, A. (2011). Trust in the Cloud. *Information security technical report*, 16(3), 108-114.
- Bruce, A. M. (2001). A Review of Digital Watermarking. *Department of Engineering, University of Aberdeen*.
- Al-Turki, U. (2011). A framework for strategic planning in maintenance. *Journal of Quality in Maintenance Engineering*, 17(2), 150-162.
- Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.
- Asghar, M. R., Ion, M., Russello, G., and Crispo, B. (2012). Securing data provenance in the cloud. *IFIP WG 11.4 International Workshop on Open Problems in Network Security, iNetSec 2011, June 9, 2011 - June 9, 2011*. Lucerne, Switzerland: 145-160.
- Bangaleea, R., and Rughooputh, H. (2002). Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterisation 293-298 vol. 291.
- Cayre, F., Fontaine, C., and Furon, T. (2005). Watermarking security: theory and practice. *Signal Processing, IEEE Transactions on*. 53(10), 3976-3987.
- Chandra, D. V. S. (2002). Digital image watermarking using singular value decomposition. *Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on*. 4-7 Aug. 2002 III-264-III-267 vol.263.
- Chang, C.-C., Hu, Y.-S., and Lin, C.-C. (2007). *A Digital Watermarking Scheme Based on Singular Value Decomposition*. *Combinatorics, Algorithms, Probabilistic and Experimental Methodologies*. In B. Chen, M. Paterson and G. Zhang (Eds.), (Vol. 4614, pp. 82-93): Springer Berlin / Heidelberg.
- Collis, J., & Hussey, R. (2009). *Business Research*: Palgrave Macmillan.
- Chang, C. Y., Wang, H. J., and Su, S. J. (2010). Copyright authentication for images with a full counter-propagation neural network. *Expert*

Systems with applications. 37(12), 7639-7647.

Chuhong, F., Kundur, D., and Kwong, R. H. (2006). Analysis and design of secure watermark-based authentication systems. *Information Forensics and Security, IEEE Transactions on.* 1(1), 43-55.

Computing, S. C. (2007). Definition of cloud computing. from <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>

Dillon, T., Wu, C., and Chang, E. (2010). Cloud computing: Issues and challenges. *24th IEEE International Conference on Advanced Information Networking and Applications, AINA2010, April 20, 2010 - April 23, 2010.* Perth, WA, Australia: 27-33.

Eriksson, P. K., Johansson, E., Kettaneh-Wold, N., Wikström, C., & Wold, S. (1999). A.(2008). *Management of Natura 2000 habitats: 6280 Nordic alvar and precambrian calcareous flatrocks.*

Gao, T., Gu, Q., and Emmanuel, S. (2009). A novel image authentication scheme based on hyper-chaotic cell neural network. *Chaos, Solitons & Fractals.* 42(1), 548-553.

Gien, M. (1978). A File Transfer Protocol (FTP). *Computer Networks (1976).* 2(4– 5), 312-319.

Gruschka, N., and Jensen, M. (2010). Attack surfaces: A taxonomy for attacks on cloud services 276-279.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 37(2), 337-355.

Goes, P. B. (2014). Editor's comments: big data and IS research. *Mis Quarterly*, 38(3), iii-viii.

Gu, L., and Cheung, S. C. (2009). Constructing and testing privacy-aware services in a cloud computing environment: challenges and opportunities 2.

Hernandez Martin, J. R., and Kutter, M. (2001). Information retrieval in digital watermarking. *Communications Magazine, IEEE.* 39(8), 110-116.

Hevner, R. F., Daza, R. A. M., Englund, C., Kohtz, J., & Fink, A. (2004). Postnatal shifts of interneuron position in the neocortex of normal and

- reeler mice: evidence for inward radial migration. *Neuroscience*, 124(3), 605-618.
- Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2), 4.
- Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22). Springer Science & Business Media.
- Huang, C. H., and Wu, J. L. (2004). Attacking visible watermarking schemes. *Multimedia, IEEE Transactions on*. 6(1), 16-30.
- Hwang, K., and Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *Internet Computing, IEEE*. 14(5), 14-22.
- Jing, Z., Anthony, T. S. H., Gang, Q., and Pina, M. (2007). Robust Video Watermarking of H.264/AVC. *Circuits and Systems II: Express Briefs, IEEE Transactions on*. 54(2), 205-209.
- Johnson, N. F., Duric, Z., Jajodia, S., and Memon, N. (2001). Information Hiding: Steganography and Watermarking—Attacks and Countermeasures. *Journal of Electronic Imaging*. 10, 825.
- Johannesson, P., & Perjons, E. (2014). *An introduction to design science*. Springer.
- Jong Won, S., and Jin Woo, H. (2001). Audio watermarking for copyright protection of digital audio data. *Electronics Letters*. 37(1), 60-61.
- Kirovski, D., and Malvar, H. S. (2003). Spread-spectrum watermarking of audio signals. *Signal Processing, IEEE Transactions on*. 51(4), 1020-1033.
- Kuttera, M., Voloshynovskiya, S., and Herrigela, A. (2000). The watermark copy attack. *Security and watermarking of multimedia contents II: 24-26 January, 2000, San Jose, California*. 3971, 371.
- Li, D. (2004). Artificial intelligence with uncertainty 2-2.
- Lickert, H., Takeuchi, J. K., von Both, I., Walls, J. R., McAuliffe, F., Adamson, S. L., ... & Bruneau, B. G. (2004). Baf60c is essential for function of BAF chromatin remodelling complexes in heart development. *Nature*, 432(7013), 107-112.
- Liu, Y.-C., Ma, Y.-T., Zhang, H.-S., Li, D.-Y., and Chen, G.-S. (2011). A method for trust management in cloud computing: Data coloring by cloud watermarking. *International Journal of Automation and Computing*. 8(3), 280-285.

- Lombardi, F., and Di Pietro, R. (2011). Secure virtualization for cloud computing.
Journal of Network and Computer Applications. 34(4), 1113-1122.
- Mantelaers, P. (1997). Acquiring expert knowledge on IS function design.
In *Information systems and qualitative research* (pp. 324-340).
Springer US.
- O'Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M. (1996).
Watermarking digital images for copyright protection. *Vision, Image
and Signal Processing, IEE Proceedings* -. 143(4), 250-256.
- Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009, May). Outline
of a design science research process. In *Proceedings of the 4th
International Conference on Design Science Research in Information
Systems and Technology* (p. 7). ACM.
- Oligeri, G., Chessa, S., Pietro, R. D., & Giunta, G. (2011). Robust and
efficient authentication of video stream broadcasting. *ACM
Transactions on Information and System Security (TISSEC)*, 14(1), 5.
- Ostrowski, L., & Helfert, M. (2012). Design science evaluation—example of
experimental design. *Journal of Emerging Trends in Computing and
Information Sciences*, 3(9), 253-262.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A
design science research methodology for information systems
research. *Journal of management information systems*, 24(3), 45-77.
- Peffer, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012, May).
Design science research evaluation. In *International Conference on
Design Science Research in Information Systems* (pp. 398-410).
Springer Berlin Heidelberg.
- Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014, June). Artifact Evaluation in
Information Systems Design-Science Research-a Holistic View.
In *PACIS* (p. 23).
- Pretorius, D. L., Goede, R., & Terblanche, J. T. (2016, January). Action
Research or Design Science Research as Methodology for the
Development of a Historical Digital Graphical Novel? A Critical
Systems Perspective. In *Proceedings of the 59th Annual Meeting of
the ISSS-2015 Berlin, Germany* (Vol. 1, No. 1).

- Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: implementation, management, and security*. CRC press.
- Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., and Desprez, F. (2012). Building safe PaaS clouds: A survey on security in multitenant software platforms. Langford Lane, Kidlington, Oxford, OX5 1GB, United Kingdom: 96-108.
- Sherekar, S., Thakare, V., and Jain, S. (2008). Role of Digital Watermark in e- governance and e-commerce. *International Journal of Computer Science and Network Security*. 8(1), 257-261.
- Sherekar, S., Thakare, V., Jain, S., Miss Ashwini, D. B., Tijare, P., Deshpande, M. S. A., et al. (2011). Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks. *International Journal Of Computer Science And Applications*. 4(2).
- Simonsohn, U., Nelson, L., & Simmons, J. (2017). Research Methodology, Design, and Analysis. *Annual Review of Psychology*, 69(1).
- Sreenivas, V., ArunaKumari, B., and VenkataRao, J. (2012). Enhancing the security for information with virtual data centers in cloud. *2011 International Conference on Future Wireless Networks and Information Systems, ICFWI 2011, November 30, 2011 - December 1, 2011*. Macao, China: 277-282.
- Tan, X., and Ai, B. (2011). The issues of cloud computing security in high-speed railway 4358-4363.
- Tek, F. B., Dempster, A. G., & Kale, I. (2010). Parasite detection and identification for automated thin blood film malaria diagnosis. *Computer vision and image understanding*, 114(1), 21-32.
- Trauth, E. M. (1997). Achieving the research goal with qualitative methods: lessons learned along the way. In *Information systems and qualitative research* (pp. 225-245). Springer US.
- Thakurta, R., Müller, B., Ahlemann, F., & Hoffmann, D. (2017, January). The State of Design—A Comprehensive Literature Review to Chart the Design Science Research Discourse. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.
- Venable, J. (2006, February). The role of theory and theorising in design science research. In *Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST*

2006) (pp. 1-18).

Wang, K., and Shao, Q. (2012). Analysis of cloud computing and information security. *2nd International Conference on Frontiers of Manufacturing and Design Science, ICFMD 2011, December 11, 2011 - December 13, 2011.*

Taichung, Taiwan: 3810-3813.

Wieringa, R. (2010, June). Relevance and problem choice in design science. In *International Conference on Design Science Research in Information Systems* (pp. 61-76). Springer Berlin Heidelberg.

Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., & Ren, K. (2016). A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, 11(11), 2594-2608.

Xia, Z., Xiong, N. N., Vasilakos, A. V., & Sun, X. (2017). EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, 387, 195-204.

Yang, C.-T., Lin, C.-H., and Chang, G.-L. (2011a). Implementation of image watermarking processes on cloud computing environments. *2nd International Conference on the Emerging Areas of Security-Enriched Urban Computing and Smart Grids, SUComS 2011, September 21, 2011 - September 23, 2011.*

Hualien, Taiwan: 131-140.

Yang, C. T., Lin, C. H., and Chang, G. L. (2011b). Implementation of Image Watermarking Processes on Cloud Computing Environments. *Security- Enriched Urban Computing and Smart Grid*, 131-140.

Yin, R. K. (1984). Case study research: Design and methods. Beverley Hills.

Yu, Z., Wang, C., Thomborson, C., Wang, J., Lian, S., and Vasilakos, A. V. (2011).

A novel watermarking method for software protection in the cloud.

Yuhan, Z., and En-hui, Y. (2009). Joint robust watermarking and compression using variable-rate scalar quantization. *Information Theory, 2009. CWIT 2009. 11th Canadian Workshop on.* 13-15 May 2009 183-186.

Zander, S., Armitage, G., and Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. *Communications Surveys & Tutorials, IEEE*. 9(3), 44-57.

- Zhao, X., and Ho, A. (2010). *An Introduction to Robust Transform Based Image Watermarking Techniques*
- Intelligent Multimedia Analysis for Security Applications*. In H. Sencar, S. Velastin, N. Nikolaidis and S. Lian (Eds.), (Vol. 282, pp. 337-364): Springer Berlin / Heidelberg.
- Zheng, D., Liu, Y., Zhao, J., and Saddik, A. E. (2007). A survey of RST invariant image watermarking algorithms. *ACM Comput. Surv.* 39(2), 5.
- Zhou, F., Goel, M., Desnoyers, P., and Sundaram, R. (2011). Scheduler vulnerabilities and attacks in cloud computing. *Arxiv preprint arXiv:1103.0759*.
- Zhu, C., and Hu, Y. (2008). A multipurpose watermarking scheme for image authentication and copyright protection. *Electronic Commerce and Security, 2008 International Symposium on*. 930-933.
- Zhu, J., Wei, Q., Xiao, J., and Wang, Y. (2009). A fragile software watermarking algorithm for content authentication. *2009 IEEE Youth Conference on Information, Computing and Telecommunication, YC-ICT2009, September 20, 2009 - September 21, 2009*. Beijing, China: 391-394.

Appendix A

ETHICS EXCEPTION

EXCEPTIONS TO ACTIVITIES REQUIRING ATEC APPROVAL

The following activities do not require ATEC approval:

6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise.

-

See more detail at:

<http://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-activities-requiring-atec-approval-6>

Appendix B

RODS SOURCE CODE

```
Frmlogin
using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Drawing;
using System.Linq; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
public partial class frmlogin : Form
{
public static string username;
//public static string username;
//public static string passcode; public static string userID;
public frmlogin()
{
InitializeComponent();
}
private void button1_Click(object sender, EventArgs e)
{
//username = txtname.Text;
//class Program
//{
//Static void Main(string[] args)
//{
//SqlConnection con = new SqlConnection("Removed Due to Security Reasons");
```

```

//insert the information to the database
//SqlCommand cmd = new SqlCommand("Insert into
registerinfo(Name,lastname)values(@Name,@lastname)", con);
//Console.WriteLine("Enter the Id:");
//cmd.Parameters.Add("@name", SqlDbType.NVarChar, 50).Value = txtname.Text;
//cmd.Parameters.Add("@lastName", SqlDbType.NVarChar, 50).Value =
txtPass.Text;
//if (con.State == ConnectionState.Closed)
//{
//    con.Open();
//}
//int i = cmd.ExecuteNonQuery();
//if (i > 0)
//{
//    MessageBox.Show("Success"); SqlDataReader Reader = null;
SqlConnection con = new SqlConnection("Data Source=192.168.91.130;Initial
Catalog=cloud;Persist Security Info=True;User ID=sa;pwd=reza123456");
con.Open();

SqlCommand cmd = new SqlCommand("SELECT dbo.RegInfo.RegID FROM
dbo.RegInfo where Username = @Username AND Password = @Password", con);
cmd.Parameters.Add(new SqlParameter("Username", txtname.Text));
cmd.Parameters.Add(new SqlParameter("Password", txtPass.Text)); Reader =
cmd.ExecuteReader();
if (Reader.HasRows)
{
Reader.Read();
frmlogin.userID = Reader[0].ToString(); this.Close();
username = txtname.Text;
frmmain frmmain = new frmmain(); frmmain.Show();

```

```

    }
else
{
    MessageBox.Show("Login Failed");
}
}

private void label1_Click(object sender, EventArgs e)
{
}

private void btnclear_Click(object sender, EventArgs e)
{
    txtname.Clear(); txtPass.Clear(); txtname.Focus();
}
}
}

Frmmainform
using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Drawing; using System.Linq; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
    public partial class frmmain : Form
    {
        public frmmain()
        {
            InitializeComponent();
        }

        private void btnlogin_Click(object sender, EventArgs e)
        {
            frmlogin login = new frmlogin(); this.Hide();
            login.ShowDialog();

```

```

    }
    private void btnregistration_Click(object sender, EventArgs e)
    {
        frmregistration reg = new frmregistration(); reg.Show();
    }
    private void btnupload_Click(object sender, EventArgs e)
    {
        frmupload upload = new frmupload(); upload.Show();
    }
    private void button1_Click(object sender, EventArgs e)
    {
        frmManipulation manipulate = new frmManipulation(); manipulate.Show();
    }
    private void frmmain_Load(object sender, EventArgs e)
    {
        btnmaniulate.Enabled = false; btnupload.Enabled = false;
    }
    private void frmmain_Shown(object sender, EventArgs e)
    {
        if (frmlogin.username != null)
        {
            label1.Show();
            lbluser.Text = frmlogin.username; btnmaniulate.Enabled = true; btnupload.Enabled
            = true;
        }
        else
        {
            label1.Hide(); lbluser.Hide();
        }
    }
    private void frmmain_FormClosed(object sender, FormClosedEventArgs e)
    {

```

```

Application.Exit();
}
}
}

Frmregistrationform
using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Drawing;
using System.Linq; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
public partial class frmregistration : Form
{
public frmregistration()
{
InitializeComponent();
}
private void button3_Click(object sender, EventArgs e)
{
txtname.Clear(); txtlname.Clear(); txtid.Clear(); txtemail.Clear();
txttel.Clear(); txtpass.Clear(); txtconpass.Clear(); txtusername.Focus();
txtname.Focus();
}
private void btnconfirm_Click(object sender, EventArgs e)
{
SqlConnection con = new SqlConnection("Removed");
//insert the information to the database
SqlCommand cmd = new SqlCommand("Insert into reginfo(Name,lname,username,
PNo,TelNo,Email>Password)values(@Name,@lname,@username,@PNo,@TelNo,
@Email,@Password)", con);

```

```

//Console.Write("Enter the Id:");
cmd.Parameters.Add("@name", SqlDbType.NVarChar, 50).Value = txtname.Text;
cmd.Parameters.Add("@lName",    SqlDbType.NVarChar,    50).Value    =
txtlname.Text;
cmd.Parameters.Add("@username",    SqlDbType.NVarChar,    50).Value    =
txtusername.Text;
cmd.Parameters.Add("@PNo", SqlDbType.NVarChar, 50).Value = txtid.Text;
cmd.Parameters.Add("@TelNo",    SqlDbType.BigInt).Value    =    txttel.Text;
cmd.Parameters.Add("@Email", SqlDbType.NVarChar, 50).Value =
txtemail.Text;
cmd.Parameters.Add("@Password",    SqlDbType.NVarChar,    50).Value    =
txtpass.Text;
if (con.State == ConnectionState.Closed)
{
con.Open();
}
int i = cmd.ExecuteNonQuery();
if (i > 0)
{
if (txtpass.Text != txtconpass.Text)
{
MessageBox.Show("Enter Password is not Match"); txtpass.Focus();
//txtpass.Text = "    ";
}
else MessageBox.Show("Success");
}
else
{
MessageBox.Show("Your password fileds are not match");
}
}

```

```

private void frmregistration_Load(object sender, EventArgs e)
{
    frmlogin frm1 = new frmlogin(); frm1.Hide();
}
}
}

Frmupload
using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Drawing;
using System.IO; using System.Linq;
using System.Security.Cryptography; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
    public partial class frmupload : Form
    {
        public static string PictureFileNameGlobal; public static Int32[] RandArray = null;
        public static string[] CalcGLOBAL;
        public static byte[] picturebyteGLOBAL;

        //public static string x;

        public static string HashGLOBAL; public static int UPIDGlobal;
        public static int randomNumberGLOBAL; public static string ImageName;
        public frmupload()
        {
            InitializeComponent();
        }
    }
}

```

```

private void btnupload_Click(object sender, EventArgs e)
{
    openFileDialog1.ShowDialog();          pictureBox1.ImageLocation          =
    openFileDialog1.FileName; PictureFileNameGlobal = openFileDialog1.FileName;
    txtbrowse.Text = openFileDialog1.FileName;
    ImageName = openFileDialog1.SafeFileName;
}
public bool ThumbnailCallback()
{
    return false;
}
private void btnupload_Click_1(object sender, EventArgs e)
{
    SqlConnection con = new SqlConnection("Removed");
    SqlCommand cmd = new SqlCommand("Insert into
upload(Image,hash,Calc,RegID)values(@Image,@hash,@Calc,@RegID)", con);
    con.Open();
    if (openFileDialog1.FileName != null &&
System.IO.File.Exists(openFileDialog1.FileName))
    {
        FileStream fs;
        fs = new FileStream(openFileDialog1.FileName, FileMode.Open,
        FileAccess.Read);
        byte[] picbyte = new byte[fs.Length];
        fs.Read(picbyte, 0, System.Convert.ToInt32(fs.Length));
        MemoryStream ms = new MemoryStream(); Bitmap.GetThumbnailImageAbort
myCallback = new
        Bitmap.GetThumbnailImageAbort(ThumbnailCallback);
        Image img = Bitmap.FromStream(fs).GetThumbnailImage(120, 80, myCallback,
        IntPtr.Zero);
        img.Save(ms, System.Drawing.Imaging.ImageFormat.Bmp);
        Image.FromStream(ms);
    }
}

```



```

byte[] picbyte_small = new byte[ms.Length]; ms.Read(picbyte_small, 0,
System.Convert.ToInt32(ms.Length));
//if (picturebyteGLOBAL != null)
//{
//    for (int i = 0; i < picbyte_small.Length; i++)
//    {
//        if (picbyte_small[i] != picturebyteGLOBAL[i])
//        {
//            MessageBox.Show("shit!");
//            break;
//        }
//    }
//}

```

```

picturebyteGLOBAL = null; picturebyteGLOBAL = picbyte_small; ms.Close();
//return;

```

```

//*** Create the Calculation of Random Points -----

```

```

SqlDataReader Reader = null;
SqlCommand cmdCALC = new SqlCommand("select Array from GlobalArray",
con);
Reader = cmdCALC.ExecuteReader(); Int32[] upImageArray = null; upImageArray
= new Int32[9600]; CalcGLOBAL = new string[9600]; while (Reader.Read())
{
String x = Reader["Array"].ToString(); String[] xarray = x.Split(',');
//int sum =0;

```

```

for (int i = 0; i < 9600; i++)
{
    CalcGLOBAL[i] = picbyte_small[Int32.Parse(xarray[i]).ToString();
    //CalcGLOBAL = xarray;
    //int arrVal = Int32.Parse(xarray[i]);
    //if(arrVal < picturebyteGLOBAL.Length - 1)
    // sum++;
    //upImageArray[i] = Convert.ToInt32(picturebyteGLOBAL[(arrVal <
    picturebyteGLOBAL.Length - 1) ? arrVal : 0]);
    //CalcGLOBAL += upImageArray[i];
}
//return;
//MessageBox.Show(sum.ToString());
}
Reader.Close();

//-----

```

```

/**Create 100 Random point of the Uploaded Image-----
-----

//Random random = new Random();
//RandArray = new Int32[100];
//// Dont forget to clear Calc Global here
//for (int i = 0; i < 100; i++)
//{
//    /** I put 800,000 so i should put a policy that no pic more than
~1MP to Upload

//    int randomNumber = random.Next(1, 999999);
//    RandArray[i] += randomNumber;
//    //int randomNumber = random.Next(1, Convert.ToInt32(fs.Length));
//    //int Calc = picbyte[randomNumber];

//    //CalcGLOBAL = Calc + CalcGLOBAL;

//}

//-----

/**Create Hash-----
byte[] hash = MD5.Create().ComputeHash(picbyte); string strhash = "";
for (int i = 0; i < hash.Length; i++)
{
strhash += hash[i].ToString("x2");
}

//-----

```

```
cmd.Parameters.Add("@hash", SqlDbType.NVarChar).Value = strhash;
HashGLOBAL = strhash;
cmd.Parameters.Add("@Image", SqlDbType.Image).Value = picbyte;
```

```
cmd.Parameters.Add("@Calc", SqlDbType.NVarChar).Value = String.Join(",",
CalcGLOBAL);
cmd.Parameters.Add("@RegID", SqlDbType.NVarChar).Value = frmlogin.userID;
cmd.ExecuteNonQuery();
```

```
MessageBox.Show("Your file has been uploaded successfully"); fs.Close();
SqlCommand cmdimageID = new SqlCommand("select UPID from Upload where
hash = @hash and RegID = @RegID", con);
```

```
strhash;
cmdimageID.Parameters.Add("@hash", SqlDbType.NVarChar).Value =
cmdimageID.Parameters.Add("@RegID", SqlDbType.NVarChar).Value =
frmlogin.userID;
SqlDataAdapter sqlda = new SqlDataAdapter(cmdimageID); DataSet ds = new
DataSet();
sqlda.Fill(ds);
```

```
frmupload.UPIDGlobal = (int)ds.Tables[0].Rows[ds.Tables[0].Rows.Count - 1][0];
ds.Dispose();
```

```

//-----SAVE IMAGE INTO FILE FOR MATLAB CHECKING-----
picbyte);
System.IO.File.WriteAllBytes(@"C:\123\matlab\Coverimage.tif",
//-----END-----

}

else

MessageBox.Show("Sorry Something went Wrong"); con.Close();
}

private void button1_Click(object sender, EventArgs e)

{

/** Send the HASH from Secure Line

SqlConnection con1 = new SqlConnection("Removed");
SqlCommand cmd1 = new SqlCommand("Insert into
HashTable(Hash,RegID)values(@Hash,@RegID)", con1);
con1.Open();

cmd1.Parameters.Add("@Hash", SqlDbType.NVarChar, 50).Value =
HashGLOBAL;
cmd1.Parameters.Add("@RegID", SqlDbType.Int, 32).Value =
Int32.Parse(frmlogin.userID);
cmd1.ExecuteNonQuery(); con1.Close();
if (randomNumberGLOBAL == int.Parse(txtDYN.Text))
{
MessageBox.Show("Your Hash Has Been Sent Through a Secure Channel");
randomNumberGLOBAL = int.Parse(txtDYN.Text); frmexistencecheck existence =
new frmexistencecheck(); existence.Show();
}
}

```

```

    }
    else
    {
        MessageBox.Show("DYN CODE IS INCORRECT !!!");
    }
}

private void frmupload_Load(object sender, EventArgs e)

{

}

private void button2_Click(object sender, EventArgs e)
{
    //SqlDataReader Reader = null;
    //SqlConnection conCALC = new SqlConnection("server=WIN-
    QGNJPMMAALQ;uid=sa;pwd=reza123456;database=cloud");
    //SqlCommand cmdCALC = new SqlCommand("select Array from GlobalArray",
    conCALC);
    //conCALC.Open();
    ///cmdCALC.Parameters.Add(new SqlParameter("Array", frmlogin.userID));
    //Reader = cmdCALC.ExecuteReader();

    //Int32[] upImageArray = null;

    //upImageArray = new Int32[50];

    //while (Reader.Read())

    //{
    //    String x = Reader["Array"].ToString();
    //    String[] xarray = x.Split(',');
    //    for (int i = 0; i < 50; i++)

```

```

//      {
//      upImageArray[i]                                     =
Convert.ToInt32(picturebyteGLOBAL[Int32.Parse(xarray[i]))]);
//      CalcGLOBAL += upImageArray[i];
//      }
//}

//conCALC.Close();

////***Insert The Similarity Pattern ----- Random
random = new Random();
RandArray = new Int32[9600];

//// Dont forget to clear Calc Global here for (int i = 0; i < 9600; i++)
{
//int randomNumber = random.Next(0, 960053); RandArray[i] = (i * 4);
////int randomNumber = random.Next(1, Convert.ToInt32(fs.Length));
////int Calc = picbyte[randomNumber];
////CalcGLOBAL = Calc + CalcGLOBAL;
}

////-----
////***Add Array Global into DataBase----- SqlConnection con1
= new
SqlConnection("server=192.168.91.130;uid=sa;pwd=reza123456;database=cloud")
;
SqlCommand cmd1 = new SqlCommand("Insert into
GlobalArray(Array)values(@Array)", con1);
con1.Open();
cmd1.Parameters.Add("@Array", SqlDbType.NVarChar).Value = String.Join(",",
RandArray);
cmd1.ExecuteNonQuery(); con1.Close();

```

```

///

---


//String x = "a";
//string[] xArray = x.Split(',');

//int.Parse(xArray[2]);
}
private void button3_Click(object sender, EventArgs e)
{
    Random random = new Random();    randomNumberGLOBAL =
    random.Next(100000, 999999);
    MessageBox.Show(randomNumberGLOBAL.ToString(),"DYN CODE WILL BE
    EXPIRED IN 3 MINUTE");
}
}
}

Frmwatermarkexistencheck
using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Diagnostics; using System.Drawing;
using System.IO; using System.Linq; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
    public partial class frmexistencecheck : Form
    {
        public frmexistencecheck()
        {
            InitializeComponent();
        }
    }
}

```



```

private void label1_Click(object sender, EventArgs e)
{

}

private void timer1_Tick(object sender, EventArgs e)
{
progressBar1.Increment(+20);
}

private void frmexistencecheck_Load(object sender, EventArgs e)
{
timer1.Start();
}

private void btncontinue_Click(object sender, EventArgs e)
{
if (progressBar1.Value >= 99)
{
timer1.Stop();

//MessageBox.Show("Your image has been watermark before"); frmSimilarity SIM
= new frmSimilarity();
SIM.Show();
}
}

```

```

private void button1_Click(object sender, EventArgs e)
{
//MemoryStream ms; SqlDataReader Reader = null;
SqlConnection con = new
SqlConnection("server=192.168.91.130;uid=sa;pwd=reza123456;database=cloud")
;
SqlCommand cmd = new SqlCommand("select [Hash], [Image] from [Full] where
[Hash] = @Hash", con);
con.Open();

cmd.Parameters.Add(new SqlParameter("Hash", frmupload.HashGLOBAL));
Reader = cmd.ExecuteReader();
if (Reader.HasRows)
{
while (Reader.Read())
{
MemoryStream imageStream = new MemoryStream((byte[])Reader["Image"]);
//ms = imageStream;
pictureBox2.Image = Image.FromStream(imageStream); btncontinue.Enabled =
false;
}
MessageBox.Show("Your Image is Already Exist in Database");
}
else
{
MessageBox.Show("No Similar Image found, Good to GO"); btncontinue.Enabled
= true;
}
}

```

```

con.Close();
}
private void btnexit_Click(object sender, EventArgs e)
{
this.Close();
}
private void button1_Click_1(object sender, EventArgs e)
{
Process.Start(@"C:\Program Files\MATLAB\R2012a\bin\matlab.exe");
}
}
}
Frmsimilarity

```

```

using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Drawing;
using System.IO; using System.Linq; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;
namespace WindowsFormsApplication2
{
public partial class frmSimilarity : Form
{
List<FullImage> lstImages;
public frmSimilarity()
{
InitializeComponent();
}
}

```

```

private void button1_Click(object sender, EventArgs e)
{
    SqlDataReader Reader = null; lstImages = new List<FullImage>();
    picboroginal.ImageLocation = frmupload.PictureFileNameGlobal;
    SqlConnection con = new SqlConnection("Removed");
    SqlCommand cmd = new SqlCommand("SELECT Calc, Image, ImageName FROM
    dbo.[Full]", con);
    //SqlCommand cmd1 = new SqlCommand("SELECT Calc, Image FROM dbo.[Full]
    where calc = @calc1", con);
    con.Open();
    //try
    //{
    //cmd.Parameters.Add(new SqlParameter("@Calc", frmlogin.userID)); Reader =
    cmd.ExecuteReader();
    //int i = 0; string[] x2 = null;
    x2 = new string[9600]; int similarity = 0; MemoryStream ms;
    //String[] Calc = new String[50];
    //List<String[]> lstCalcs = new List<string[]>();
    //int x2count = 0;
    while (Reader.Read())
    {
        //lstCalcs.Add(Reader["Calc"].ToString().Split(',')); ms = new
        MemoryStream((byte[])Reader["Image"]); byte[] picbyte = new byte[ms.Length];

        //ms = imageStream;
        //byte[] picbyte = new byte[ms.Length];
        ms.Read(picbyte, 0, System.Convert.ToInt32(ms.Length)); lstImages.Add(new
        FullImage(Reader["ImageName"].ToString(),
        Reader["Calc"].ToString().Split(','), Image.FromStream(ms)));
        //for (int ii = 0; ii < 50; ii++)
        //{

```

```

//String xx = "a";
//string[] xArray = xx.Split(',');
//}
//if (frmupload.CalcGLOBAL >= (Calc - int.Parse(textBox1.Text)) &&
frmupload.CalcGLOBAL <= (Calc + int.Parse(textBox1.Text)))
//{
//    x2[i] = String.Join(",", Reader["Calc"].ToString());
//    if (x2[i] != null)
//    x2count++;
//}
//i++;
////String x = Reader["Calc"].ToString();
////String[] xarray = x.Split(',');
//}
int similarCount = 0;
//int similarcount1 = 0;
foreach (FullImage myImage in lstImages)
{
String[] calc = myImage.calc; similarity = 0;
for (int ii = 0; ii < 9600; ii++)
{
myImage.blockSimilarity[ii] = false;

if (frmupload.CalcGLOBAL[ii] == calc[ii])

{

similarity++; myImage.blockSimilarity[ii] = true;
}
}
if (similarity >= 500)

{

```

```

similarCount++;

if (!cmbImage.Items.Contains(myImage.name))
{
    cmbImage.Items.Add(myImage.name);
}
myImage.similarity = similarity;
}
//if (similarCount >= 1500)

//    similarcount1++;

}

%";

//txtsimilarity1.Text = ((similarity / lstImages.Count) / 500).ToString() + "

txtOriCalc1.Text = similarCount.ToString();

//txtoricalc2.Text = similarcount1.ToString();

//double x2countbool = double.Parse(x2count.ToString());

//txtOriCalc1.Text = x2count.ToString();

//txtUpCalc1.Text = frmupload.CalcGLOBAL.ToString();

//txtsimilarity1.Text = (x2countbool / 100).ToString() + " %";

//MessageBox.Show(x2[i].ToString());

```

```

//}

//catch (Exception ex) { MessageBox.Show(ex.Message); }

//finally

//{ con.Close();
//}

}
private void button2_Click(object sender, EventArgs e)

{

frmWatermarking WR = new frmWatermarking(); WR.Show();
this.Hide();

}

private void cmbImage_SelectedIndexChanged(object sender, EventArgs e)
{
foreach (FullImage myImage in lstImages)
{
if (myImage.name == cmbImage.SelectedItem.ToString())
{
picDifferential.Image = null; Graphics graphicsObj;
Bitmap tmp = new Bitmap(600, 400); graphicsObj = Graphics.FromImage(tmp);
graphicsObj.DrawImage(myImage.fullImage, 0, 0, 600, 400);
//Pen myPen = new Pen(System.Drawing.Color.Red, 3);

//Rectangle rectangleObj = new Rectangle(10, 10, 200, 200);

//Rectangle[] rects;

```

```

for (int i = 0; i < 9600; i++)
{
    if (!myImage.blockSimilarity[i])
    {
        int x = (i % 120) * 5;

        int y = 390 - ((i / 120) * 5);

        Rectangle rect = new Rectangle(x, y, 5, 5);

        //Rectangle rect = new Rectangle(((i % (600 / 30)) * 600 / 30), ((i
        % (400 / 20)) * 400 / 20), (600 / 30), (400 / 20));

        Brush brush = new SolidBrush(Color.FromArgb(200, 255, 0, 0));
        graphicsObj.FillRectangle(brush, rect);

    }

}

picDifferential.Image = tmp; graphicsObj.Dispose();

//pictureBox1.Image = myImage.fullImage; txtsimilarity1.Text =
myImage.similarity.ToString();
txtUpCalc1.Text = (myImage.similarity / 96).ToString() + " %"; break;
}

}

}

```



```

}

class FullImage

{

public FullImage(string _name, string[] _calc, Image _fullImage)

{

name = _name; calc = _calc;
fullImage = (Image)_fullImage.Clone(); blockSimilarity = new bool[9600];
}

public string name; public string[] calc;
public Image fullImage; public int similarity;
public bool[] blockSimilarity;

}

}

Frmwatermarking

using System;
using System.Collections.Generic; using System.ComponentModel; using
System.Data;
using System.Data.SqlClient; using System.Diagnostics; using System.Drawing;
using System.IO; using System.Linq;
using System.Security.Cryptography; using System.Text;
using System.Threading.Tasks; using System.Windows.Forms;

```

```

namespace WindowsFormsApplication2
{
    public partial class frmWatermarking : Form
    {
        public static string sha;
        //public static MemoryStream ms; byte[] selectedPicbyte;
        string sGLOBAL; private int _tick;
        public frmWatermarking()
        {

            InitializeComponent();
        }

        private void frmWatermarking_Load(object sender, EventArgs e)
        {
        }

        private void btnret_Click(object sender, EventArgs e)

        {
            timer1.Start();
        }

        private void progressBar1_Click(object sender, EventArgs e)
        {
        }

        private void button1_Click(object sender, EventArgs e)
        {
            timer1.Stop(); MessageBox.Show(sGLOBAL); SqlConnection con = new
            SqlConnection("Removed");

```

```

SqlCommand cmd = new SqlCommand("Insert into [Full] (RegID, Fixpass,
DynamicPass, Hash, Mixpass, Image, Calc, ImageName)values(@RegID,
@Fixpass,
@DynamicPass, @Hash, @Mixpass, @Image, @Calc, @ImageName)", con);

con.Open();

//if (openFileDialog1.FileName != null)

//{

//FileStream fs;
//fs = new FileStream(openFileDialog1.FileName, FileMode.Open,
FileAccess.Read);
//byte[] picbyte = new byte[ms.Length];

//ms.Read(picbyte, 0, System.Convert.ToInt32(ms.Length));
//Hash = MD5.Create(fs.ToString()).ToString();
cmd.Parameters.Add("@RegID", SqlDbType.Int).Value = int.Parse(
frmlogin.userID);
cmd.Parameters.Add("@Fixpass", SqlDbType.NVarChar, 50).Value =
txtFixPass.Text;
cmd.Parameters.Add("@DynamicPass", SqlDbType.NVarChar, 50).Value
= txtDynamic.Text;

cmd.Parameters.Add("@Hash", SqlDbType.NVarChar, 50).Value = txtHash.Text;
cmd.Parameters.Add("@Mixpass", SqlDbType.NVarChar, 550).Value =
txtMix.Text;
cmd.Parameters.Add("@Image", SqlDbType.Image).Value = selectedPicbyte;
cmd.Parameters.Add("@Calc", SqlDbType.NVarChar).Value = String.Join(",",
frmupload.CalcGLOBAL);

```

```

cmd.Parameters.Add("@ImageName", SqlDbType.NVarChar).Value =
frmupload.ImageName;
cmd.ExecuteNonQuery();
MessageBox.Show("Your Image Has Been Successfully Watermarked");
//fs.Close();

//}
//else
//    MessageBox.Show("Sorry something went wrong"); con.Close();
//}

private void timer1_Tick(object sender, EventArgs e)

{

progressBar1.Increment(+10);

_tick++;

if (_tick == 20)

{

SqlDataReader Reader = null; MemoryStream ms;
//pictureBox1.ImageLocation = frmupload.x;

SqlConnection con = new
SqlConnection("server=192.168.91.130;uid=sa;pwd=reza123456;database=cloud")
;
con.Open();

```

```
SqlCommand cmd = new SqlCommand("SELECT dbo.Upload.Image,
dbo.Upload.hash, dbo.RegInfo.Password FROM dbo.RegInfo INNER JOIN
dbo.Upload ON dbo.RegInfo.RegID = dbo.Upload.RegID where dbo.Upload.UPID
= @UPID", con);
```

```
cmd.Parameters.Add(new SqlParameter("UPID", frmupload.UPIDGlobal));
Reader = cmd.ExecuteReader(); while (Reader.Read())
{
```

```
txtFixPass.Text = Reader["Password"].ToString(); txtHash.Text =
Reader["hash"].ToString();
ms = new MemoryStream((byte[])Reader["Image"]); selectedPicbyte = new
byte[ms.Length];
```

```
//ms = imageStream;
```

```
//byte[] picbyte = new byte[ms.Length];
```

```
ms.Read(selectedPicbyte, 0, System.Convert.ToInt32(ms.Length));
pictureBox1.Image = Image.FromStream(ms);
//Reader["Image"].ToString() as Stream);
```

```
}
```

```
//ms.Close();
```

```
con.Close();
```

```
//cmd.Parameters.Add(new SqlParameter("openidurl", txturl.Text));
```

```
//cmd.Parameters.Add("@name", SqlDbType.NVarChar, 50).Value = txtname.Text;  
Random random = new Random();
```

```
txtDynamic.Text = frmupload.randomNumberGLOBAL.ToString(); txtMix.Text =  
txtFixPass.Text + txtDynamic.Text + txtHash.Text;
```

```
SHA512 shaM = new SHA512Managed(); byte[] hash =  
shaM.ComputeHash(Encoding.ASCII.GetBytes(txtMix.Text));
```

```
//string[] testtext;
```

```
StringBuilder stringBuilder = new StringBuilder(); byte[] a = new byte[64];  
int i = 0;
```

```
foreach (byte b in hash)
```

```
{
```

```
    stringBuilder.AppendFormat("{0:x2}", b); a[i] = b;  
    i++;
```

```
}
```

```
'0')));
```

```
string s = string.Join("", a.Select(x => Convert.ToString(x, 2).PadLeft(8,
```

```
'0');
```

```
//string yourByteString = Convert.ToString(stringBuilder, 2).PadLeft(8,
```

```
sGLOBAL = s;
```

```
txtMix.Text = stringBuilder.ToString();
```

```
File.AppendAllText(@"c:\123\matlab\MESSAGE.txt",s);
```

```
//}
```

```
}
```

```
}
```

```
private void btnexit_Click(object sender, EventArgs e)
```

```
{
```

```
Application.Exit();
```

```
}
```

```
private void btnback_Click(object sender, EventArgs e)
```

```
{
```

```
this.Close();
```

```
frmSimilarity sim = new frmSimilarity(); sim.Show();
```

```
}
```

```
private void btnMatlab_Click(object sender, EventArgs e)

{
    Process.Start(@"C:\Program Files\MATLAB\R2012a\bin\matlab.exe");
}
}
}
```


MATLAB CODE

```
close all clear all clc
c=uiigetfile('*.','Select the cover'); m=uiigetfile('*.','Select the mark');
cover=imread(c);

[LL,LH,HL,HH]=dwt2(cover,'haar','mod','sym');

fid=fopen(m); w=fread(fid,[512,1]); for j=1:512
if w(j)==48 w(j)=0;
else

w(j)=1;

end end

%-----Embedding----- newHH=HH;

i=1;

for k=1:128:65535

newHH(k)=w(i); i=i+1;
end

watermarked_cover=idwt2(LL,LH,HL,newHH,'haar','mod','sym');
watermarked_cover0=uint8(watermarked_cover);
imwrite(watermarked_cover0,'CoverimageEmbedded.png');
```

```

% check psnr

[row,col] = size(cover); size_host = row*col; o_double = double(cover);
w_double = double(watermarked_cover); s=0;
for j = 1:size_host;

s = s+(w_double(j) - o_double(j))^2 ; end
mes=s/size_host;

psnr =10*log10((255)^2/mes);

[PSNR,MSE]=measerr(watermarked_cover,cover);

%Extracting [LL,LH,HL,HH]=dwt2(watermarked_cover,'haar','mod','sym');

fid=fopen('512-2.txt','w'); j=1;
ew=zeros(512,1); for k=1:128:65535
ew(j)=HH(k);

%---these lines are for writing the extracted message into a text file ew0=int8(ew(j));
fprintf(fid,num2str(ew0));

%-----

j=j+1; end

ew2=int8(ew);

disp('Done')

```

