Comparative Evaluations of Privacy on Digital Images

Xue Zhang

A thesis submitted to Auckland University of Technology
in partial fulfilment of the requirements for the degree of
Master of Computer and Information Sciences (MCIS)

2018

School of Engineering, Computer and Mathematical Sciences

Abstract

Privacy preservation on social media is a societal issue nowadays. In recent years, with the continuous occurrence of the privacy leaks of user information and file, privacy and security issues have received unprecedented attention. Albeit a slew of mechanisms one available in protecting sensitive individual data, there are inadequate solutions to the critical concerns on privacy violations. Furthermore, the approaches of evaluating the potential privacy risks on social networking activities have not been yet paid enough attention.

In order to preserve privacy effectively, the content is released safely on social media. This thesis introduces the necessity of protecting the image privacy and effective protection methods. The problems to be investigated that need to be solved urgently are put forward. The key factors affecting privacy are probed in depth. Also, the computer vision technology plays an essential role in the image privacy. Moreover, the theory of differential privacy is adopted, which can protect the image analysis data for broader research and cooperation. We combine qualitative method with AHP (Analytic Hierarchy Process) model to provide a more reasonable measure of privacy weights. Resultant analysis of the survey also provides metrics for evaluating privacy accuracy. The experimental results demonstrate that the model of image privacy evaluation proposed in this thesis can effectively and accurately measure the level of image privacy. Thus, the degree of picture privacy can be intuitively measured and the privacy can be adequately protected.

Keywords: privacy preservation, image privacy scale, privacy concern, privacy scale, Analytic Hierarchy Process modelling, Convolutional Neural Network, differential privacy

Table of Contents

List of Figures

List of Tables

List of Algorithms

Attestation of Authorship

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 (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature:  Date: 26 July 2018

Acknowledgement

This research work was accomplished as the part of the Master of Computer and Information Sciences (MCIS) course at the School of Computer and Mathematical Sciences (SCMS) in the Faculty of Design and Creative Technologies (DCT) at the Auckland University of Technology (AUT) in New Zealand.

I would like to thank my supervisor Dr. Wei Qi Yan for providing me the opportunity to pursue this thesis and for his support and guidance throughout the year. In addition, I would also like to thank all my faculty lecturers, friends and family for their continued support and encouragement.

Xue Zhang

Auckland, New Zealand

July 2018

Chapter 1
Introduction

The introduction sets the stage by emphasising the relevance on the research topic. The first chapter of this thesis is divided into five parts. To begin with, we will provide a concise background and motivation for the preservation of image privacy. This chapter also includes the details of this study. Then, the next section lists the main topics we will discuss. In Section 2, we will illuminate the contributions. Finally, we will summarise the structure of this thesis in Section 4.

1.1 Background and Motivation

In recent years, with the advances in social networking platform and the rapid growth of graphical data, various innovations of image processing applications and techniques are continually emerging. The growing amount of online personal content sharing exposes users to a series of privacy issues (Ahern, Eckles, Good, King, Naaman, & Nair, 2007), including general privacy issues and identity information disclosure concerns. The term privacy constellates the combination of public attitudes, technical affordances and legal arguments (Houghton, & Joinson, 2010). The potential security threats caused by the abuse of sensitive information in the user-generated content remained an overarching privacy concern for more and more people (Ren, 2016). Without appropriate privacy protection, shared images can uncover user's individual and social situations, as well as their private lives, since pictures can outwardly tell when and where a particular moment happens, the participants, and their relationships (Yu, Zhang, Kuang, Lin, & Fan, 2017).

Because of the sharing nature of social media, preserving privacy is vitally important for the widely accessible shared content such as user-generated graphics (Ahern et al. 2007). The prominence of photo-sharing social networking services like Flickr and Instagram reaps the benefits of the increasing performance of smartphone's photographing function (Sun, Luo, & Sun, 2017) and the popularisation of wearable devices (Yan, Lu, & Zhang, 2015) so that people can take pictures and share them anytime and anywhere. Users enjoy the advantage of sharing content conveniently (Sondhi & Sloane, 2007). Wearable equipment empowers users to make the photo-taking process more covert (Yan et al., 2015). Once a photo containing sensitive information posted to the Internet without processing, it is easy to invade the owners' private data. Facebook, for example, aroused controversy in 2010 by introducing image recognition technology into its social networking platform (Litt, Spottswood, Birnholtz, Hancock, Smith, & Reynolds, 2014). The reason is that users' photos which contain faces and the license plate number can be automatically recognised and recorded by the system, and can be caught by various image search engines (Litt & Hargittai, 2014). Although it led Facebook to

suspend its facial recognition service in 2012, it restarted the service as there was high demand for image search afterwards.

On the contrary, they worry about the risks of the personal information leak. Once personal privacy spreads malicious, it may bring threats to personal property safety also (Rajpoot, & Jensen, 2014; Mohamadi, 2013). It is unquestionably beneficial for users to intuitively get the hint to know the privacy risk rating on the shared content before they publish a new post. Assessing the privacy risk could assist data holders to know about whether they should share it or take extra actions to protect the privacy information. With this motivation, the method for evaluation privacy of social media could provide the users with intuitive value of the privacy risk level of the user-shared images.

1.2 Research Questions

As we mentioned, the goal of this thesis is to develop a method for the evaluation of the privacy of digital images. It is the core of this method to build a privacy scoring mechanism using the technology of image processing. The privacy evaluation investigates the issue of the antithesis of privacy preservation and the topic of utilising the differential privacy to protect the metadata which generated by image analysis. It aims to answer the following research questions:

Question 1: *How are image processing methods implemented to identify and analysis objects?*

The process of image recognition technology is divided into information acquisition, pre-processing, feature extraction and selection, classifier design and classification decision-making. Proper methods should be applied to get the metadata for the privacy evaluation.

Question 2: *How to design scoring algorithm influenced by multiple factors?*

Since the scores of each influence condition are different, it requires adjusting the score of each condition first and multiplying it by the percentage of each condition. The proportion can be adjusted according to the weight coefficient.

1.3 Contributions

Different from the traditional post-processing of the privacy part of pictures, letting users recognise the privacy degree of pictures in advance so as to interfere with the users' publishing of pictures can more effectively protect the privacy of pictures. In this thesis, we address the evaluation problem of digital image privacy.

Consider the two kinds of privacy protection solutions for post-processing, one is the direct image processing on the sensitive content, including image encryption and pixel replacement. Nevertheless, this is an irreversible process, and the image quality is also degraded. The second is the privacy preference of social networking websites. Yet, setting those privacy options is both time-consuming and unfriendly. In this thesis, we present a novel mechanism of scoring the privacy of pictures to give users an intuitive privacy evaluation before releasing digital images in order to preserve the privacy from the source. We provide the specification and implementation of the algorithms.

The second contribution is the strategy for evaluating complex problems. The logic of the image privacy scoring mechanism is relatively complicated. The convoluted problems are subdivided into major influencing factors. The weight of the factors is scientifically measured. An exclusive APH privacy scoring model is designed, which has great reference value. Therefore, among the results obtained, the higher the score, the more sensitive the privacy is.

The third contribution is the adoption of the cryptograph method, that is, differential privacy, in the analysis results of privacy. This thesis makes a detailed analysis and research on differential privacy. Whereas differential privacy is still being explored in

scientific research and has not been widely adopted, we have implemented it in this project. The data generated by our privacy rating of pictures are processed by the Laplace mechanism that injects noise. This makes the data to be published cannot be traced to any identity, thus so as to protect the privacy of pictures.

1.4 Structure of This Thesis

In this dissertation, we mainly study the method of privacy assessment on social media. The structure of the thesis is as follows:

The first chapter summarises research background and discusses the characteristics, function modules and general workflow of privacy protection based on object recognition technology; then it introduces the research content and the organisational structure of this thesis.

The second chapter studies research status of the privacy on social media, analyses the main research direction corresponding characteristics of privacy and object recognition technology.

The third chapter is the key technology of the privacy protection evaluation scheme, focusing on how to combine object recognition to achieve privacy scoring algorithm and specific programs. Additionally, differential privacy is applied to protect the privacy of related analysis data generated by graphics.

The fourth chapter is the privacy scoring function test and performance test. The function test includes the comparison of the results and the accuracy analysis with ROC curve. The application of anti-privacy and differential privacy is discussed again.

The fifth chapter is the summary of full text and the prospect of future work.

Finally, a reference list is given.

Chapter 2
Literature Review

On the basis of in-depth analysis of research problems and review of previous studies, the focus of this thesis is on the overview of previous research based on the image privacy. It is essential to set the context of literature review work by firstly introducing the factors affecting privacy, which is the primary focus of the study described in this thesis. Moreover, the theory and applications of object detection will be discussed, as well as the advantages and disadvantages behind each technique. The state-of-the-art face recognition and license plate recognition methods will be reviewed in this chapter. The last part we introduce a significant approach to privacy protection, that is, differential privacy.

2.1 Introduction

In this chapter, we briefly review the most relevant research on privacy preservation measures, the factors of privacy scoring standard and privacy object detection methods.

2.2 Privacy Preservation Measures

Nowadays, mainstream solutions to image privacy protection on social media focus on the post-processing of user-shared content. In general, there are two main genres of the post-processing on privacy preservation strategies. One is the direct image processing on sensitive content which includes image encryption and pixel substitution. The other is privacy preferences in social networking sites.

Initially, many research studies have been carried out on the direct image processing. The first way is to substitute the private section of the photo directly (Duan, Du, & Phuoc, 2005; Ling & Fend, 2011). The drawback of this approach is inefficient and the replacement field is irreversible. The second one is to remove the privacy filed, and a watermark will be embedded into the back scene. The restrict information is erased from the photos. Besides, image quality has been affected as watermarks embedded. The third kind is the method to scramble or blur the sensitive field with the encryption process (Zhang, & Cheung, 2005; Cheung, Paruchuri, & Nguyen, 2008). It is an irrecoverable process so that the image quality has dropped as well. An image classification method with the consideration of privacy protection and Bag-of-Features algorithm on feature extraction (Liu, Shang, & Tang, 2016). A system named Cyptagram is designed to preserve online image privacy (Tierney, Spiro, Bregler, & Subramanian, 2013). Encoding and encryption methods as well as recoverability are applied to this system. It encrypts the whole JPEG image which allows sharing between end-to-end users only. The process also led to instability and compatibility problems among other social networking sites.

Internet privacy deals with the control right over how personal data is collected, kept, used and deleted (Sen, 2014). Privacy management settings are designed to restrict the flow of personal information which users shared on social networking profiles (Boyd, & Hargittai, 2010). Social media sites take their politics privacy policies and settings exceptionally seriously and have been keeping updating all the terms and regulations. Those settings rules are predefined so that it aims to reduce the risk of privacy leaks from the setup of access right permission. This mechanism provides the users with the opportunity to choose and meet their personal privacy need to preserve sensitive information. However, half of the social networking users said they had difficulties in managing privacy controls (Min, & Kim, 2015).

Database of social networking sites needs data input from data holders, while on the other hand, it harms users when it fails to protect the data with a safe release to the public. The new Internet technology may cause unexpected issues when it comes to privacy (Wicker, 2013). Although the users choose to share online is controlled under privacy settings, it still could not entirely protect users' shared content from malicious usage by the content holders or someone with harmful attempt or unjustified spying. As a proverb says, a picture is worth a thousand words. An image may reveal things effectively and can also pose risks to personal data and assets. It is vital that users need to realise that they should keep the routine of identifying the hidden privacy threats in every single post social networking websites and mobile apps to avoid leaking private information without realising it. It goes without saying that it is time-consuming and user-unfriendly which may also against the sharing nature of social media.

Social networking sites are great places for staying connected with family and friends and letting the public know what the status. To keep users' private information safe, always think before user share online (Lopez, Huang, & Sandhu, 2013). In order to preserve private information in the first place, users ought to evaluate the content before it exposed to the public. Albeit users may consider whether there is any possibility of disclosing identifying information when they are going to publish a post, as long as the personal information exposed in the public space, there is the possibility of being

compromised. The problem of privacy security boils down to the privacy risk caused by the internet users' active sharing (Ananthula, Abuzaghleh, Alla, Chaganti, Kaja, & Mogilineedi, 2015). The ability to manage and control the personal information can effectively reduce the probability of privacy leakage. The protection by the law is generally the remedy and reparation afterwards. To be avoid the losses caused by privacy disclosure, privacy preservation measures should be taken in advance (Gulzar, Abbasi, Wu, Ozbal, & Yan, 2013). Whereas, so far, there has not been any application that can reveal the privacy level of pictures. The method for evaluating privacy of social images indicates the rating of privacy risk on the photo. The rating is intuitive, and it lets the user know what the risk level should be so as to assist users to make more reasonable and safer decisions so that it is better to evade the problems that may arise.

2.3 Factors of Privacy Scoring Standard

Privacy rights and scope have always been a significant problem in law, network technology and industry norms (DeVries, 2003). With the rapid development of social media, the operational definition and measurement of data privacy are becoming more and more difficult (Hwang, 2015). A variety of factors causes the privacy intrusion in social media. Generally, researchers will transfer the privacy analysis to specific influencing factors.

The first factor is the detection accuracy. Seeing that an object must be identified from a scene image containing multiple items, the difficulty of object recognition rested with several factors like camera parameters, location and illumination (Jain, Kasturi, & Schunck, 1995). Those factors influencing camera perspectives and video images affect the performance of object detection and analysis. In addition, the accuracy of face detection can be interfered by many aspects, such as the problem of image acquisition equipment, the problem of face posture, the problem of intentional or unintentional occlusion, which will affect the result of face detection. When people deliberately do not want to be exposed, they will obscure and pixelize the easily exposed parts of the private information. This is a conventional method for people to protect their privacy. When the

accuracy rate of system detection drops, at the same time, the amount of information that can be found easily will be reduced, and the leakage of privacy will also be decreased. According to the result of Euler Angles calculation, when the angle of an object is not ideal, the information available to the object detection system will become less (Fanelli, Weise, Gall, & Gool, 2011). Hence, the accuracy of detecting the object will be decreased. Therefore, the higher the angle the object shows, the more information it will have and the higher its privacy higher will be.

The second factor is the object rectangle ratio. Image alignment transforms a source image to the coordinate system (Hui, Zhi, & Ahmad, 2018). As many detection algorithms depend on the positioning of an object into a rectangle, the position of features related to a fixed coordinate system can be measured (Davison, 2003). The rectangle is in the form "left, top, width, height" in pixels. Hence, the rectangle region to the image area ratio could be achieved. According to visual attractiveness research and visual merchandising, people are effortlessly attractive and remembered by the presence of bright colours and the accurate visual information. The eye has two axes; one is the optical axis, the other is the visual axis of sight during observation. The intersection of retina and visual axis can be divided into central fovea, sub-central fovea and peripheral vision from inside to outside. With the increase of distance between the central concave and the centre, the visual acuity decreased significantly, and the ability to extract the information reduced significantly too (Hu, Bai, & Yan, 2010). Therefore, similarly, if the proportion of objects in the same picture gets smaller or the position becomes biased, the exposure rate will decrease. Since in the visual effect, when the proportion of the object is smaller, the less intuitive information provided to the viewer, the lower the memory point of people. The less privacy can be exposed.

The third factor is sensitivity. The facial attribute is a technique to identify the attribute values of a person's face such as sex, age, posture, expression, and so forth. The input of facial recognition algorithm is the face map and the key point coordinates of facial features (Yang, Luo, Loy, & Tang, 2017). Moreover, the output is the corresponding face attribute value. Face attribute recognition algorithms generally align faces according to the coordinates of key points of facial features and then perform

attribute analysis (Mahbub, Sarkar, & Chellappa, 2018). It is a general designation for a class of algorithms, including gender recognition, age estimation, attitude estimation and expression recognition. Hereinafter, the privacy protection for the minors ought to be highlighted. Under the United Nations Convention on the Rights of the Child and New Zealand's relevant child convention law, minors are before the age of 17 (Lundy, 2007). However, when children do not have independent discernment until the age of 10, parents need to act as guardians of their children's privacy rights. When a child is more than 14 years old when he has enough knowledge and discernment, even parents cannot publish any child-related photos without the consent of the child, which also violates the child's right to portrait and information. In law, the right protection law of minors is more severe. Hence, in our privacy protection, if a minor was detected in a photo, the risk of privacy violations in this photo is even higher.

Moreover, in the end, it is the factor timeliness. According to the Ebbinghaus Forgetting Curve, people's memory has a forgotten curve. People tend to forget about a word, a picture or a video, usually after 20 minutes and 42% were forgotten, 58% were remembered; one hour later, 56% were forgotten, 44% were remembered; one day later, 74% were forgotten, 26% were remembered; one week later, 77% were forgotten and 23% were remembered, one month later, 79% were forgotten just 21% were remembered (Ebbinghaus, 1985). Thus, when photos or videos are published on social media, over time, the less likely those are to be remembered, and the less privacy level it can expose.

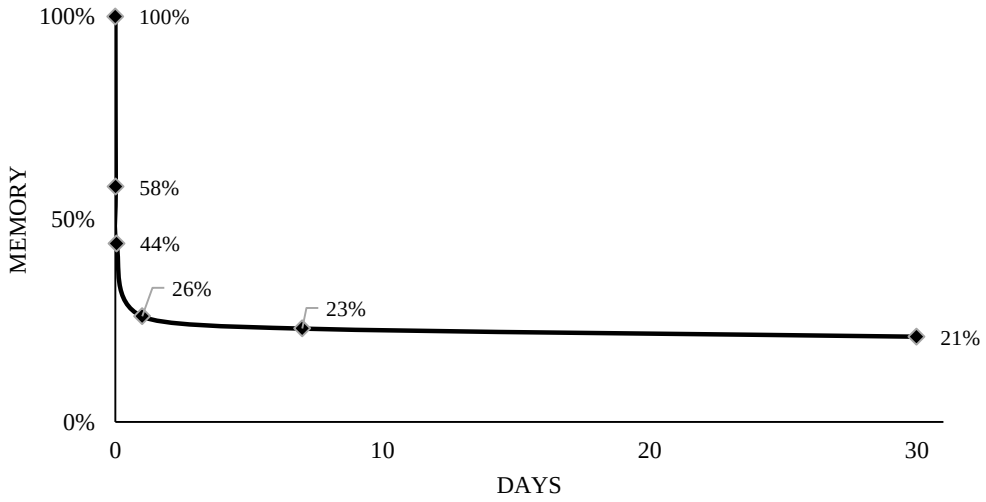


Figure 2.1 The Ebbinghaus forgetting curve

2.4 Object Detection Methods

In this section, we briefly review the most relevant research on geometric feature-based method and the convolutional neural network.

2.4.1 Geometric Feature-Based Method

The geometrical feature is firstly used to describe and recognise the profile of the human face. First, some salient points are determined according to the profile curve. From these salient points, we derive a set of feature metrics for identification, such as distance, angle, and so on. The geometric features of the frontal face recognition are generally based on the extraction of position of the critical characteristic points such as human eyes, mouth and nose, and the geometrical shapes of essential organs such as eyes (Pun, Yuan, & Chen, 2011). The deformable template can be regarded as an improvement of the geometrical feature method. The basic idea is to design a model with adjustable parameters to define an energy function. The energy function is minimized by adjusting the model parameters.

However, this method has two shortcomings. Firstly, the weighting coefficients of the various costs in energy function can only be determined by experience, which is challenging to public. The second is that the energy function optimisation process is time-consuming and demanding to be applied in practice. The human face representation based on parameters can achieve an efficient description of the characteristic of the face. Nevertheless, it requires a lot of pre-treatment as well as a fine selection of parameters. At the same time, the general geometrical features are used to describe only the basic shape and structure. It ignores local nuances and causes some loss of information. It is more suitable for coarse classification. At present, the existing feature point detection technology is far from satisfying the requirement in precision rate, and the computation quantity is also considerable (Korobiichuk, I., Podchashinskiy, Shapovalova, Shadura, Nowicki, & Szewczyk, 2016).

2.4.2 Convolutional Neural Network

According to the way that neural networks are constructed, a relatively simple change can make larger images better processed (Goodfellow, Bulatov, Ibarz, Arnoud, & Shet, 2013). The result of the change is the CNN (Convolutional Neural Network). The extensive adaptability of neural networks is one of its advantages. Contrary to what would be expected, this advantage becomes a burden when image processing. The convolutional neural network has made a particular compromise on this. If a network is specially designed to process images, some adaptabilities need to compromise on more feasible solutions.

For any images, the distance between pixels has a healthy relationship with their similarity (Zhong, Squicciarini, Miller, & Caragea, 2017). In addition, the design of a convolutional neural network makes full use of this feature. This means that for a given image, two pixels that are closer to each other are more similar than those that are farther apart (Levi, & Hassner, 2015). Whereas in general neural networks, each pixel is connected to a single neuron. In this case, the additional computational load makes the network less accurate.

Convolutional neural network solves this problem by eliminating a large number of similar unimportant connections. Technically, CNN filters through the connections between neurons based on similarity, making image processing controllable at the computational level (Liang, & Hu, 2015).). For a given layer, the CNN does not connect each input to each neuron, but it restricts the connection explicitly. It allows any neuron to accept a fraction of the input from the previous layer. Therefore, each neuron is responsible for processing only a specific part of an image.

2.5 Differential Privacy

Individuals are accustomed to the thought that they are sending a significant amount of individual data to a range of applications they utilise in their daily lives. Numerous users rest on machine learning and information collection for everything from tagging the

uploaded photos of friends on social networking to keep shopping selections. Even though this can be useful and handy, it can be a personal privacy disaster as well (Bannister, 2005). Aggarwal and Philip (2008) found that surveys indicate that users are beginning to feel anxious and powerless that individual user data may be abused. The preservation of personal privacy data is a bottleneck restricting the development of big data. Nevertheless, from time to time there are strong demands for collecting usage statistics data. The essential security issue for companies that they are not permitted to use the majority of personal records in the database (Shokri, & Shmatikov, 2015). It needs more privacy-respecting ways to offer these sorts of services and gather the related individual user data. If a data set is to be published, merely removing sensitive information such as an Id is not safe enough to protect privacy.

Differential privacy, generally speaking, is a method for analysing large-scale databases both accurate and anonymous (Yang, Soboroff, Xiong, Clarke, & Garfinkel, 2016). Differential privacy could assist companies to get insight into their users in general statistical analysis without leaking sensitive and identifiable information of an individual.

Differential privacy could solve the two flaws of traditional privacy protection model. First, the differential privacy protection model assumes that attackers can obtain information from all other records except the target one (Aldeen, Salleh, & Razzaque, 2015). The sum of this information can be understood as the maximum background knowledge that attackers are able to collect. Under that assumption, differential privacy protection does not need to consider any potential background knowledge of the attacker, because these background knowledge cannot provide richer information than the maximum one (Naghizade, Bailey, Kulik, & Tanin, 2017). On this account, differential privacy gives an additional shield against re-identification arbitrary queries and attacks which utilises additional information from the user's other online activity records (Li, Qardaji, & Su, 2012). When the third part accesses user's data, they find another user who has the similar properties and compares his data with users. Thus, users are represented by a cluster, rather than an individual, without personal privacy compromised. Therefore, they analyse the group of users with whatever extracts the most significant.

Whether a user exists in the dataset ought to make small deviations of analytical results (Dwork, 2006).

Secondly, differential privacy is on a solid mathematical foundation basis. It defines privacy protection strictly and provides a quantitative evaluation method (Mashima, Serikova, Cheng, & Chen, 2018). This makes it possible to compare the privacy protection level of datasets provided by different parameter processing. The academic community has proposed various methods of privacy protection and measures to measure privacy disclosure, such as *k*-anonymity, *l*-diversity, *t*-closeness, ε-differential privacy, homomorphic encryption and zero-knowledge proof (Abdalaal, Nergiz, & Saygin, 2013). These methods measure the privacy of public data from an intuitive point of view. Thus, the use of cryptography, statistics and other tools ensure the privacy of the data. As a strict mathematical definition of privacy protection framework, differential privacy has theoretical research significance. Differential privacy can also delete personal information without affecting the output of the result. It neither leaks any information nor allows people to find anything associated with it through the information released.

There are two methods that are commonly used at present. One is the Laplace mechanism. Adding Laplace distribution noise to the query results is suitable for the numerical output (Sarathy, & Muralidhar, 2011). The other is the exponential mechanism. In the query result, the exponential distribution is used to adjust the probability, which is suitable for the output of nonnumeric type. In the study of this thesis, we are more suitable for the Laplace mechanism.

Differential privacy balances the feasibility and privacy of data. Users can adjust the feasibility and privacy of data by setting their privacy budget. However, the differential privacy is not omnipotent, in which many of these algorithms of adding noise needs to be applied to a large number of datasets (Domingo-Ferrer, & Soria-Comas, 2015). In addition, adjusting the proper setting of privacy budget is also a problem. These are the problems and challenges faced by differential privacy. Moreover, as the requirement of differential privacy for background knowledge is too strong, it is necessary to add a significant amount of randomisation to the results, resulting in a decline in the utility of the data. Especially for those complicated queries, sometimes randomised results almost

conceal the real results. However, like an exquisite mathematical tool, differential privacy is a future development direction of privacy protection research.

Chapter 3
Methodology

This chapter summarises the research methods followed in this study. The main content of this chapter is to clearly explain the methods applied to meet the objectives of this thesis. In this chapter, we give the design view of this project and some essential block diagrams that must be followed in the implementation process. It also gives an account of the methods used for data collection and the procedures followed in carrying out the study. Besides, we proposed the methods used to analyse the data. Finally, we expound the method of protecting the data generated by using image analysis with differential privacy.

3.1 Introduction

The mechanism for evaluating privacy of social images is designed to let users be recognised what the privacy level is on the shared images by evaluating the privacy risk automatically and intelligently. The features of image privacy in this project are limited to the scopes of face and car plate number detections. The dataset contains 26 videos which generate 7648 images were divided into two groups according to the domains in which they belong. The records of privacy evaluation on each image are marked manually on the worksheets in Microsoft Excel firstly. Qualitative research of the savvy method carried through the assessment to collect the weights of scoring image privacy and the privacy levels of 20 images. 52 participants took part in the survey and completed questionnaires online. According to marking records as well as by comparing the summarisation on the savvy result, scoring criteria of image privacy level was decided with the modelling of Analytic Hierarchy Process (AHP).

3.2 The Criteria of Image Privacy

Defined features will be counted and examined based on each criterion. Five main factors defined in this project are accuracy, ratio, angle, sensitivity and timeliness. If there are no sensitive objects detected, the system will show no privacy issue.

In this rating standard, a feature that meets the privacy requirement should be picked up. When the associated privacy feature is identified, the privacy score goes high. If there is no one which matches the criterion, this picture is marked 0 which shows there is no privacy risk for this system.

The high exposure, located typically at the centre of the photo, draws more attention. People could not get all the details of the picture, and the edge area may get low exposure.

Detection angle is also one of the essential parts of privacy concern. Angle diversity mainly refers to rotation of the detected object due to different shooting angles and rotation. Changes in the angle of the shot also lead to different contours of the object.

Also, due to the change of angles, some features of the object cannot be extracted correctly, which leads to detection error.

Every photo has own timeliness. Generally, as time goes by, an image posted online will gradually lose attention and reduce exposure. People often observe a photo only at this moment when it was just published. However, sometimes, a social event may draw attention to previous posts, and many others may mine it. According to human psychology, the current happening events get the highest degree of attention. Over time, public attention will gradually decline.

Facial region is the most sensitive part of image privacy. Children and adults are the two different aspects of this assessment. According to the child protection law, child's privacy is much more critical. So, their privacy ratio will be higher than that of an adult.

3.2.1 Factor Accuracy

OpenFace is an open source library. It has the performance and accuracy of a patent model. The library was created with the consideration of mobile performance. Consequently, the library has a fast and accurate internal structure (Baltrusaitis, Robinson, & Morency, 2016). In this project, OpenFace is applied to achieve the accuracy of face detection.

There is a pipeline for face recognition in OpenFace, as illustrated in Figure 3.1. The pipeline is a basic framework for dealing with face problems using convolutional neural networks. The existing face detection methods of dlib and OpenCV are used inside OpenFace. These methods have nothing to do with deep learning. HOG and Haar features are employed to the traditional methods of computer vision.

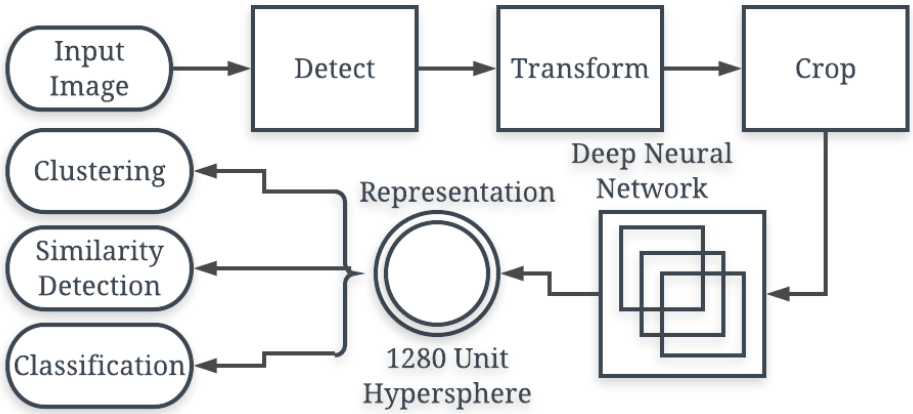


Figure 3.1 The flowchart of pipeline for face recognition in OpenFace

The next step is called face alignment process. For the output of original image in the first step with the bounding box, the thing to do in this step is to detect the key points in the face, then, aligning and calibrating the face according to these key points. The key points are usually located at the corner of eyes, nose, the contour points of the face, and so on so forth. With these key points, we can align the faces. Hence, human face is uniformly set with an Affine transformation to eliminate the errors caused by different posture. This step is also used in the traditional method, which is characterised by a relatively fast speed (Kazemi, & Sullivan, 2014).

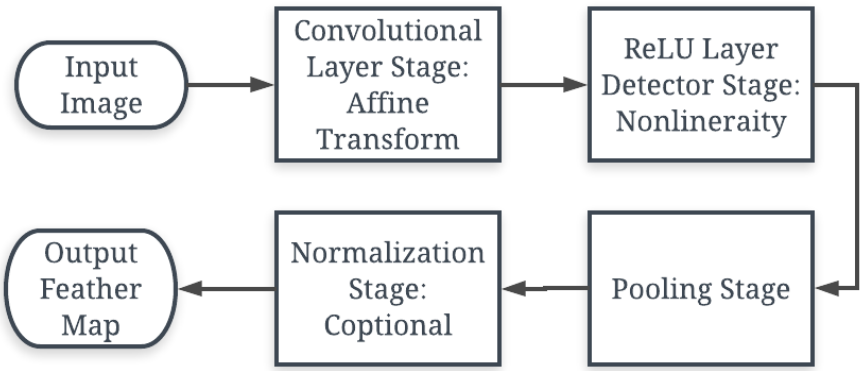


Figure 3.2 The flowchart of the layers of the convolutional neural network

This step is to use the convolution neural network. In CNN, there are often many different network layers that are alternately composed, mainly including convolutional layer, pooling layer, ReLU layer, fully connected layer, and so on. Its structure is shown in Figure 3.3. The input face image is converted into a vector representation. The vector

used in OpenFace is 128×1, which is a 128-dimensional vector. The VGG-16 network architecture is a relatively simple and basic model in deep learning, as demonstrated in the figure below. The input of this neural network is the image. After a series of convolution, the complete classification will generate the category probability.

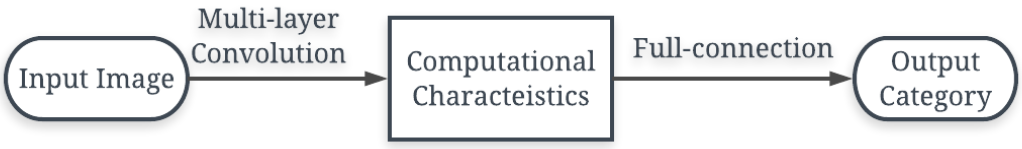


Figure 3.3 The flowchart of the VGG-16 network architecture

Under an ideal circumstance, the distance between vector representations can directly reflect the similarity of human faces. For face images of the same person, the Euclidean distance of the corresponding vector should be relatively small. For face images of different people, the distance between corresponding vectors should be relatively large. In the original VGG16 model, Softmax loss was applied. Nonetheless, there is no requirement for the distance between the vector representations of each class. Therefore, it cannot be used directly as a face representation. Centre loss actually adds another loss to the Softmax loss, which sets a centre point for each category (Wen, Zhang, Li, & Qiao, 2016). Each category of features should be closer to this centre point, while the centres of different categories are far away.

In this thesis, we use an open source library called OpenALPR which has low-pass filtering in spatial domain. From the knowledge of signal spectrum analysis, the slow part of the signal is one of the low-frequency parts of the frequency domain. Moreover, the fast variable part of the signal is the high-frequency parts in frequency domain. For the image, its edge and noise frequency components are in the higher frequency part. Hence, the low-pass filter method can be used to remove the noises. Filtering operations can be conducted from spatial domain to reduce noise. Suppose an image $f(x, y)$, the filtered image is $g(x, y)$.

$$g(\mathrm{x},\mathrm{y}) = \Sigma_{\mathrm{i}}\Sigma_{\mathrm{j}} f(i,j)h(x-i+1, y-j+1) \tag{3.1}$$

The H matrix is a small-size convolution kernel:

$$\mathbf{H} = \frac{1}{16}\begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix} \tag{3.2}$$

The fundamental principle for the system of vehicle license plate recognition is as presented in Figure 3.4. Firstly, the image containing a vehicle license plate captured by the camera is input into the computer through video card to be preprocessed. Then, the license plate is detected and located by using the retrieval module. Thirdly, the rectangular area containing license plate character is segmented. Figure 3.5 illustrates the frames of car plate detection in different angles. At last, the license plate is binarized and segmented into single characters; finally the segmented characters will be used as input for recognition, the recognized results will be output.

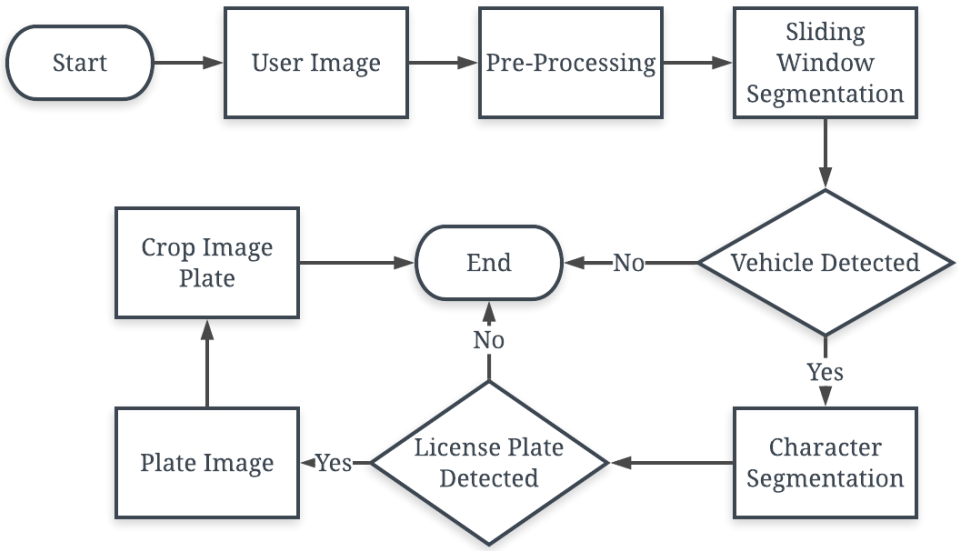


Figure 3.4 The flowchart of the license plate identification

Figure 3.5 Video frames for car plate detection in various angles

Figure 3.6 The best view of the car plate

The input image contains rich colour information. It takes up more storage space and processing, which may slow down the execution response time of the system. Therefore, image recognition and other image processing usually convert the original image into greyscale images so as to speed up the processing. License plate locating uses greyscale image processing, edge extraction and morphological methods. The specific steps are as follows: firstly, greyscale conversion and binarization processing are carried out on the original images, then 4×1 structural elements are adapted to corrode the image so as to remove image noises. Using the 25×25 structural element, the image should be turned off to connect the license plate area. Morphological filtering is performed to remove other regions.

Throughout the Gaussian blurring step, the image becomes blurry. The purpose of this step is to eliminate the added noises by using Sobel operator. The image is converted to grayscale, whether pro or con, this step is a watershed, meaning that all subsequent operations are no longer based on colour information (Saglam, & Baykan, 2017). The first order horizontal derivative of the image is obtained by applying a Sobel operator. After this step, the license plate will be clearly distinguished.

This step is to find contour of the license plate. When figuring out the shapes of all the objects in the picture, we should filter out all the rectangles that are not suitable for detection. After this step, only the rectangles with six yellow borders passed the filter.

Figure 3.7 Image after processed

With regard to viewpoint and rotation for plate detection, we discard the rectangle whose tilt angle which is higher than the threshold (30° to -30°). The first, second, third and fifth rectangle on the left are discarded. The remaining rectangle is rotated slightly to make it in horizontal.

After normalised the size of images, the size obtained in the previous step is not same. With the intention of matching machine learning models, a uniform size is required. The standard width of the uniform size is 136, and the length is 36. This standard is a typical value of test plates obtained after the average.

These licenses have two primary functions. First, it is accumulated as a training set to train a license plate judgment model. Secondly, in real license plate detection, these candidate license plates are judged by using a well-trained model. If the license plate judgment model recognises that it is a license plate, it will enter the next step, i.e., the character recognition process; otherwise, it will be abandoned.

The pseudo code for this algorithm to get the detection accuracy for face and plate number is outlined in Algorithm 3.1.

Algorithm 3.1 Factor Accuracy

Input: type and image
Output: confidence value and pitch, yaw and roll angles in radian

```
1: procedure ACCURACY(a, b)
2:     type ← a
3:     image ← b
4:     result ← confidence value and pitch yaw and roll
5:     if type = face then
6:         run OpenFace(image)
7:     end if
8:     if type = car then
9:         run OpenALPR(image)
10:    end if
11:    return result
12: end procedure
```

Algorithm 3.1 The algorithm of factor accuracy

3.2.2 Factor Ratio

The purpose of this section is to calculate the proportion of face-detected region to this photo. Since we are unable to get coordinates for facial feature points from OpenFace, we need to use another tool to measure this part. The coordinates of the facial region are obtained from Face++ which is a service provider for face recognition. It consists of a group numbers with four integers, separated by commas. It sequentially represents the ordinates of the upper left corner of the facial bounding box, abscissa value of the upper left corner, width of the face frame and height of the face frame. The high exposure typically at the centre of the photo draws more attention, and the edge area may get low exposure. Table 3.1 illuminates the scores we defined based on the exposure rate.

Table 3.1 Different positions for the factor ratio

0.3	**0.5**	**0.3**
0.5	**0.8**	**0.5**
0.3	**0.5**	**0.3**

Since the given points are coordinates related to the origin, each point can be treated as a vector to the origin. The coordinates of the known 4 points are (x_1, y_1), $(x_2, y_2), (x_3, y_3)$ and (x_4, y_4). If the area of face-detected region is $\boldsymbol{S_f}$, the area formula of $\boldsymbol{S_f}$ shows as below:

$$S_f = \sum_{k=1}^{4} s = \frac{1}{2}\sum_{k=0}^{4}(x_k y_{k+1} - x_{k+1} y_k) \tag{3.3}$$

The area of the photo *S* is easily obtained in MATLAB. As a result, the proportion of face-detected region is $\boldsymbol{P}=\frac{Sf}{S}$. The pseudocode for the ratio algorithm is outlined in Algorithm 3.2.

Algorithm 3.2 Factor Ratio

Input: four vertices of the bounding box and image dimension
Output: the proportion of ratio

procedure RATIO($x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4, width, height$)
    $x_0 \leftarrow \frac{x_1+x_2}{2}$
    $y_0 \leftarrow \frac{y_1+y_4}{2}$
    $result \leftarrow 0$
    if $\frac{width}{3} \leq x_0 \leq \frac{2width}{3}$ || $\frac{height}{3} \leq y_0 \leq \frac{2height}{3}$ **then**
        if $\frac{width}{3} \leq x_0 \leq \frac{2width}{3}$ & $\frac{height}{3} \leq y_0 \leq \frac{2height}{3}$ **then**
            $result \leftarrow 0.8$
        else
            $result \leftarrow 0.5$
        end if
    else
        $result \leftarrow 0.3$
    end if
    return *result*
end procedure

Algorithm 3.2 The algorithm of factor ratio

3.2.3 Factor Angle

The first step is to detect the feature points within the bounding box of the face from the input image or video, then align the detected face according to feature points on the face. The so-called feature points are the yellow key points shown in Fig 3.8. Those detected key points usually include the corners of the eyes, the locations of the nose, the contour of the face, and so on (Valstar, Martinez, Binefa, & Pantic, 2010). With these key

points, we can get face calibration or facial alignment. The original face may be rotated at different angles and relatively twisted. According to the feature points, the use of Affine transformation will analyse it just like the front face to eliminate the failure rate of the different head postures. Figure 3.9 demonstrates the snapshots of face detection in different head postures.

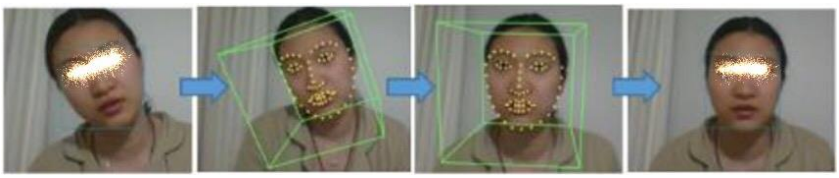


Figure 3.8 Different head postures

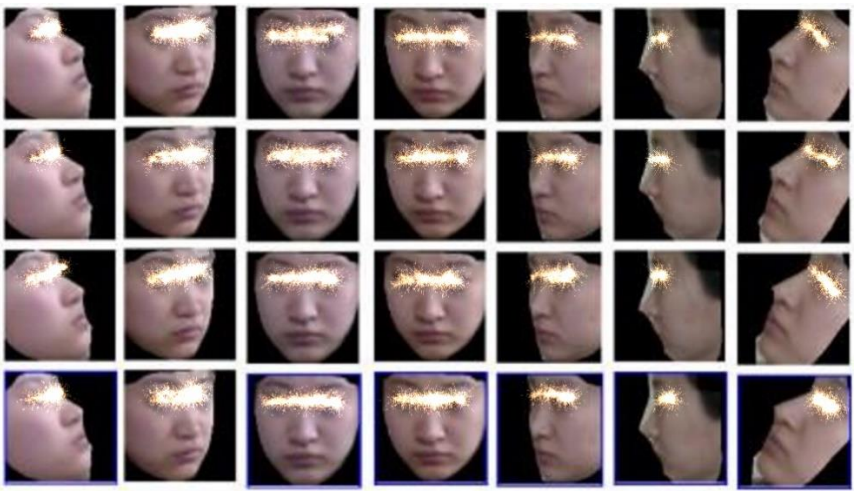


Figure 3.9 Snapshots of face detection in different head postures

Euler angle is made up of three angles: yaw, pitch, and roll. The angles are used to measure the angular relationship between the face and the camera. Roll represents the angle $\boldsymbol{\alpha}$ that rotates around the ***z***-axis. Yaw indicates the angle $\boldsymbol{\beta}$ of rotation around the ***y***-axis. Pitch indicates the angle $\boldsymbol{\gamma}$ of rotation around the ***x***-axis. These three rotations can obtain any rotation angle in sequential order. Rotate around the correlation axis multiplies the correlation matrix. In other words, Euler angles will eventually be converted into matrix multiplication.

- Rotation around *z*-axis: $\mathrm{R}_z(\alpha) = \begin{bmatrix} \cos\alpha & \sin\alpha & 0 \\ -\sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$ (3.4)

- Rotation around *y*-axis: $\mathrm{R}_y(\beta) = \begin{bmatrix} \cos\beta & 0 & -\sin\beta \\ 0 & 1 & 0 \\ \sin\beta & 0 & \cos\beta \end{bmatrix}$ (3.5)

- Rotation around *x*-axis: $\mathrm{R}_x(\gamma) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma & \sin\gamma \\ 0 & -\sin\gamma & \cos\gamma \end{bmatrix}$ (3.6)

Hence, the transformation matrix for Roll-pitch-yaw representation would be $\mathrm{R}_z(\alpha) \cdot \mathrm{R}_y(\beta) \cdot \mathrm{R}_x(\gamma)$.

Detectable range of facial poses spans from -30˚ to 30˚ in pitch, from -20˚ to 20˚ in roll, and from -40˚ to 40˚ in yaw (Saeed, Al-Hamadi, & Ghoneim, 2015). If the angle of facial gesture activity is within this range, the possibility of privacy exposure is relatively high. The pseudocode for the angle algorithm is outlined in Algorithm 3.3.

Algorithm 3.3 Factor Angle

Input: pitch, yaw and roll angles in radian from Algorithm 1
Output: angle ratio in percentage

procedure ANGLE($pitch, yaw, roll$)
  $\alpha \leftarrow roll$
  $\beta \leftarrow pitch$
  $\gamma \leftarrow yaw$
  $rollResult \leftarrow 0$
  $pitchResult \leftarrow 0$
  $yawResult \leftarrow 0$
  $result \leftarrow 0$
  if $-\frac{\pi}{9} \leq \alpha \leq \frac{\pi}{9}$ **then**
    $rollResult \leftarrow -\frac{9}{\pi}|x| + 1$
  else
    $rollResult \leftarrow 0$
  end if
  if $-\frac{\pi}{6} \leq \beta \leq \frac{\pi}{6}$ **then**
    $pitchResult \leftarrow -\frac{6}{\pi}|x| + 1$
  else
    $pitchResult \leftarrow 0$
  end if
  if $-\frac{2\pi}{9} \leq \gamma \leq \frac{2\pi}{9}$ **then**
    $yawResult \leftarrow -\frac{9}{2\pi}|x| + 1$
  else
    $yawResult \leftarrow 0$
  end if
  $result \leftarrow \min(rollResult, pittchResult, yawResult)$
  return $result$
end procedure

Algorithm 3.3 The algorithm of factor angle

3.2.4 Factor Sensitivity

The convolutional activation feature is extracted through the CNN. The colour, texture, shape and other information of a person's face is extracted as a feature representation. Then the feature is set as an input to the age estimation model. The age estimation model uses the extracted face feature representation and specific age labels or age groups. The age estimation model is learned through machine learning. By using this model, through several steps, age estimation of the face image can be carried out. Figure 3.10 illustrates the facial age estimation flowchart.

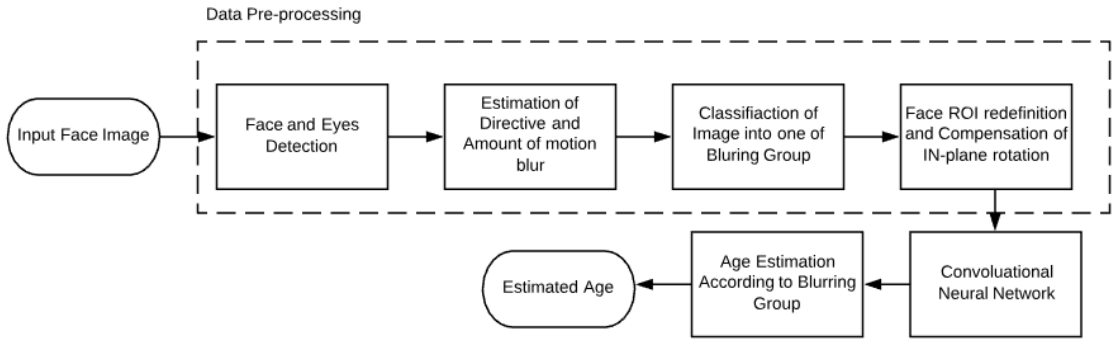


Figure 3.10 The flowchart of facial age estimation

The pseudo code for the sensitivity algorithm is outlined in Algorithm 3.4.

Algorithm 3.4 Factor Sensitivity

Input: type and value
Output: sensitivity ratio in percentage

```
procedure SENSITIVITY(type, value)
    result ← 0
    if type = age & value ≤ 17 then
        result ← 1
    else if type = age & value > 17 then
        result ← 0.5
    else if type = plate & value = 1 then
        result ← 0.3
    else
        result ← 0
    end if
    return result
end procedure
```

Algorithm 3.4 The algorithm of factor sensitivity

3.2.5 Factor Timeliness

Everyone has a forgetting curve of user's himself (Averell, & Heathcote, 2011). A particular knowledge point of learning is not different to give itself an incentive. Nevertheless, the incentive is not immutable and will gradually decrease as time goes on. If we do not give this knowledge an incentive for a long time, it will become less till it is forgotten and then filtered out (Feriyanto, Saleh, Badri, Deros, & Pratama, 2015). Some people may have a good memory; others may have a poor memory. The forgetting curves between different people are dissimilar. However, this does not fundamentally affect human's cognition. That is to say, if there is a forgetting function, it is first in exponential form and then in practical process. The pseudocode for this timeline algorithm is outlined in Algorithm 3.5.

The forgetting curve can be applied to Newton's law of cooling (Emmons, 2016). If **M** is the memory value at time *t*, $\boldsymbol{M_s}$ is the forgotten threshold value, $\boldsymbol{M_0}$ is the initial memory value and k is the super parameter. Then the differential equation defined as below.

$$\mathrm{M} - M_s = (M_0 - M_s)\mathrm{e}^{-\mathrm{kt}} \tag{3.7}$$

Algorithm 3.5 Factor Timeliness

Input: created time of the image
Output: the proportion of timeliness

```
1: procedure TIMELINESS(time)
2:     currentTime ← clock
3:     dif ← etime(currentTime, time)          ▷ time difference is in seconds
4:     result ← 0
5:     if dif ≥ 0 & dif ≤ 1200 then            ▷ less than or equal to 20 minutes
6:         result ← 1
7:     else if dif > 1200 & dif ≤ 3600 then    ▷ after 20 minutes
8:         result ← 0.58
9:     else if dif > 3600 & dif ≤ 86400 then   ▷ after 1 hour
10:        result ← 0.44
11:    else if dif > 86400 & dif ≤ 604800 then ▷ after 1 day
12:        result ← 0.26
13:    else if dif > 604800 & dif ≤ 2592000 then ▷ after 1 week
14:        result ← 0.23
15:    else
16:        result ← 0.21                       ▷ after 1 month
17:    end if
18:    return result
19: end procedure
```

Algorithm 3.5 The algorithm of factor timeliness

3.3 APH-Based Privacy Scoring Hierarchy

Analytic Hierarchy Process is abbreviated to AHP. It is a simple method for making decisions on some complicated and fuzzy problems. It is especially suitable for those problems that are difficult to be analysed quantitatively. AHP deals with complicated and often lacks quantitative data problems composed of many interrelated and mutually restricted factors. It is a flexible and practical method of multiple criteria decision making. AHP is used to determine the weight of factors. The necessary steps of the AHP modelling are clarified as follows:

(1) Conceptualizing the complex problem and finding out the main factors involved in the research object.

(2) Analysing the subordinate relationship of each factor and constructing the ordered hierarchical structure model.

(3) Establishing the judgment matrix which compares the relative importance of each factor at the same level to a particular criterion at the previous level.

(4) Calculating the relative weights of the compared factors to the criterion at the upper level by using the judgment matrix. Moreover, the consistency test is carried out.

(5) Calculating the synthetic weights of each level which are related to the primary objective of the system and the hierarchical levels.

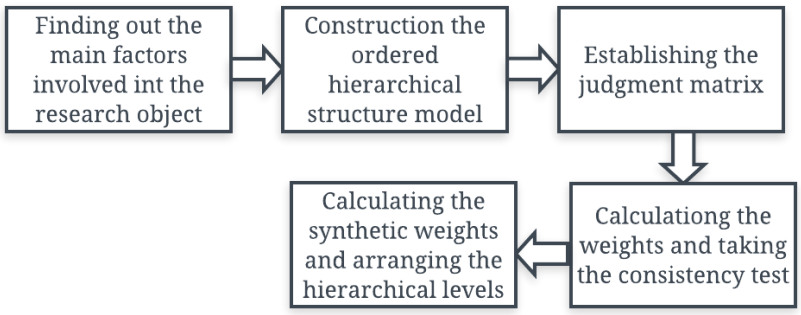


Figure 3.11 The flowchart of the necessary steps of the AHP modelling

When AHP is used to analyse the decision problem, the problem is organised and layered, and a hierarchical structure model is constructed (Bevilacqua, & Braglia, 2000). In this model, complex problems are decomposed into components of criteria. These factors are from numerous levels according to their attributes and relationships. The

factors of the previous level play a dominant role in the relevant derived factors of the next level. These levels can be divided into three categories the goal layer, the criteria layer and the sub-criteria layer (Baby, 2013). The ladder hierarchy model is shown in the diagram.

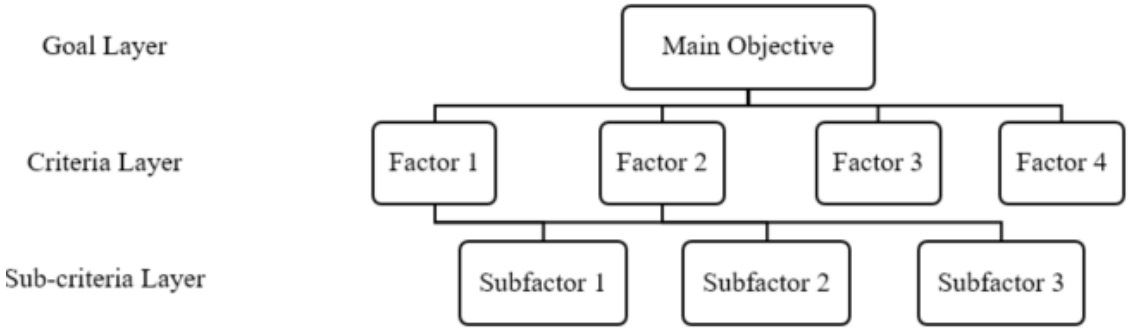


Figure 3.12 The ladder hierarchy model

The weight of privacy scoring hierarchy is divided into three levels. As the target of the picture's privacy score G belongs to the goal layer, the criteria layer contains five elements of the privacy score of the picture. There are Accuracy C_1, Ratio C_2, Angle C_3, Sensitivity C_4 and Timeliness C_5. The sub-criteria layer is the specific indicator item in this scoring system, including the Age S_1 of the face recognition module and the License Plate Number S_2 of the plate number recognition module. Hierarchical structure model is constructed to explain the subordinate relationship between the structure and factors (Schnetler, Steyn, & Van Staden, 2015). The hierarchical model is shown in Figure 3.13.

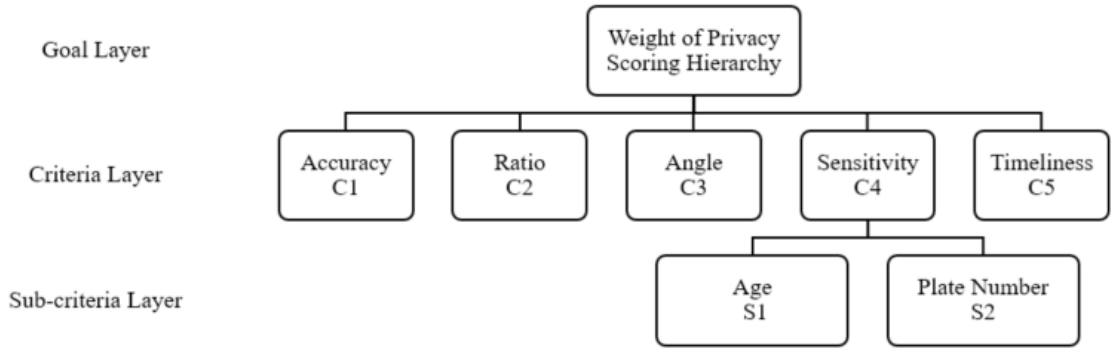


Figure 3.13 Weights of privacy scoring hierarchy

The hierarchical structure reflects the relationship between factors. However, the proportion of each criterion in the criteria layer in the measurement is not necessarily the same. Each criterion should have a certain proportion.

Suppose there are n factors in $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$, how to derive the influence of these factors on a factor **Y**? The pairwise comparison of factors can be adopted to establish a pair comparison matrix method. This step is a key process in the AHP method. To evaluate the relative importance of each relevant element in the hierarchy, the judgment matrix is evaluated for an element in the previous level. Its form is elaborated in equation 3.8. Two factors x_i and x_j are taken at a time. The ratio of the impact of $x_i$and x_j to **Y** is expressed in x_{ij}. All comparison results are expressed in matrix $\mathbf{A} = (a_{ij})_{n\times n}$. **A** is called the pairwise comparison judgment matrix between **Y** and **X**. It is easy to see that if the ratio of x_i to x_j affects **Y** is a_{ij}. Then the ratio of x_i to x_j to **Y** should be $a_{ji} = \frac{1}{a_{ij}}$.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \tag{3.8}$$

Regarding how to determine the value of a_{ij}, numbers 1 to 9 and their reciprocal value are used as scales. Table 3.2 lists the meanings of scales 1 to 9.

Table 3.2 The meanings of scales

Scale	Descriptions
1	It indicates that the two factors are of the same importance.
3	It indicates that the former is slightly more important than the latter.
5	It indicates that the former is apparently more important than the latter.
7	It indicates that the former is much more important than the latter.
9	It indicates that the former is extremely more important than the latter.
2, 4, 6, 8	It indicates the intermediate value of the adjacent scales.
reciprocal value	If the ratio of the importance of factor i to factor j is a_{ij}, the ratio of the importance of factor j to factor i is $a_{ji} = 1/a_{ij}$.

In the hierarchical analysis process, the relative importance weights between factors are computed by a single judgment matrix. The hierarchy sequence is obtained by solving

the following eigenvalue problem, $\boldsymbol{AV} = \lambda \boldsymbol{V}$. In the equation, $\mathbf{V}$ is a vector and $\mathbf{V} = (V_1, V_2, \dots, V_n)'$, λ is the eigenvalue of judgment matrix $\mathbf{A}$. $\mathbf{V}$ is the eigenvector corresponding to the eigenvalues. The equation which gets the maximum eigenvalue of judgement matrix is shown as the eq.(3.9), where $(\mathbf{AV})_i$ represents the *i*-th factor of the vector $\boldsymbol{AV}$. The component V_i of $\mathbf{V}$ is the weight value of the corresponding factor.

$$\lambda_{max} = \sum_{i=1}^{n} \frac{(AV)_i}{nV_i} \tag{3.9}$$

With the aim of testing the consistency of the judgment matrix, it is necessary to calculate the consistency index: $\boldsymbol{CI} = \frac{\lambda_{max} - n}{n-1}$, Check Coefficient: $\boldsymbol{CR} = \frac{CI}{RI}$.

When $\boldsymbol{CI} = 0$, the judgment matrix is fully consistent. Conversely, the larger the ***CI*** will be, the worse the consistency of the judgment matrix is. In order to verify the satisfactory consistency of the judgment matrix, it is necessary to compare ***CI*** and mean random consistency index ***RI***. To define the mean random ***RI***, there are 500 pairwise comparison judgment matrixes, $A_1, A_2, \dots, A_{500}$ and the respective consistency index *CI*, $CI_1, CI_2, \dots, CI_{500}$. Hence, $\boldsymbol{RI} = \frac{CI_1 + CI_2 + \cdots + CI_{500}}{500} = \frac{\frac{\lambda_1 + \lambda_2 \dots + \lambda_{500}}{500} - n}{n-1}$ and it shows in Table 3.3.

Table 3.3 The values of mean random consistency index

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

When $\boldsymbol{CR} < 0.10$, it is considered that the consistency of the judgment matrix is acceptable. Otherwise, when $\boldsymbol{CR} > 0.10$, it is necessary to adjust the judgment matrix until it is satisfied.

After calculating the eigenvector of each judgment matrix, the synthetic weights of each level for the leading factor can be calculated from top to bottom, and the formula shows as follow. Total sorting weight of lower layer B is shown in Table 3.4.

$$\sum_{i=1}^{n} \sum_{j=1}^{m} V_j b_{ij} = 1 \tag{3.10}$$

Table 3.4 Total sorting weight of the lower layer B

	$A_1, A_2, \dots, A_m$	Total Sorting Weight Value

B_1	$B_{11}, B_{12}, \dots, B_{1m}$	$\sum_{j=1}^{m} V_j b_j$
B_2	$B_{21}, B_{22}, \dots, B_{2m}$	$\sum_{j=1}^{m} V_j b_{2j}$
…	…	…
B_n	$B_{n1}, B_{n2}, \dots, B_{nm}$	$\sum_{j=1}^{m} V_j b_{nj}$

The pseudocode of the AHP-Based model for computing privacy scoring weights is outlined in Algorithm 3.6.

Algorithm 3.6 APH-Based Method for Privacy Scoring Weights

Input: comparison matrix n×n, for n criteria
Output: weight vectors

procedure APH($matrixA$)
  $X \leftarrow eigenvector$
  $x \leftarrow$the eigenvector of size $n \times 1$
  $result \leftarrow 0$
  $\breve{\omega}_{ij} \leftarrow \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}}$ ▷ Normalising each column vector of A
  $\breve{\omega}_i \leftarrow \sum_{i=1}^{n} \breve{\omega}_{ij}$ ▷ Sum $\breve{\omega}_{ij}$ line by line
  $\omega_i \leftarrow \frac{\breve{\omega}_{ij}}{\sum_{i=1}^{n} \breve{\omega}_i}, \omega = (\omega_1, \omega_2, ..., \omega_n)^T$ ▷ Normalising $\breve{\omega}_j$
  $\lambda_{max} \leftarrow \frac{1}{n} \sum_{i=1}^{n} \frac{(A\omega)_i}{\omega_i}$ ▷ λ_{max} is the eigenvalue
  $CI \leftarrow \frac{\lambda_{max}-n}{n-1}$ ▷ CI stands for Consistency Index
  if $n = 5$ **then**
    $RI \leftarrow 1.12$ ▷ RI stands for the value of Random Consistency Index
  end if
  $CR \leftarrow \frac{CI}{RI}$ ▷ CR stands for Consistency Ratio
  if $CR < 0.10$ **then**
    $CRResult \leftarrow Pass$
    $result \leftarrow \omega_i$
  else
    $CRResult \leftarrow Fail$
  end if
  return $result$
end procedure

Algorithm 3.6 APH-based method for privacy scoring weights

AHP is an effective method for calculating weights on the privacy scoring system influenced by the five privacy factors. It is suitable for this multiple criterion scoring that is intractable to be analysed quantitatively. Hence, we got the score and weight ratio of the five factors from Algorithm 3.1 to 3.6. The pseudocode for the mechanism of privacy evaluation algorithm is outlined in Algorithm 3.7.

Algorithm 3.7 The Scoring Schema of Image Privacy

Input: the results of 5 factors and the matrix of privacy weight vectors
Output: privacy level

1: **procedure** PRIVACY($accuracy, ratio, angle, sensitivity, timeliness, weights[]$)
2: $\rho_{accuracy} \leftarrow accuracy \times weights[1]$
3: $\rho_{ratio} \leftarrow ratio \times weights[2]$
4: $\rho_{angle} \leftarrow angle \times weights[3]$
5: $\rho_{sensitivity} \leftarrow sensitivity \times weights[4]$
6: $\rho_{timeliness} \leftarrow timeliness \times weights[5]$
7: $result \leftarrow 0$
8: $result \leftarrow \rho_{accuracy} + \rho_{ratio} + \rho_{angle} + \rho_{sensitivity} + \rho_{timeliness}$
9: **return** $result$
10: **end procedure**

Algorithm 3.7 The scoring schema of image privacy

3.4 Differential Privacy

Hashing and subsampling along with noise injection are the three commonly used research methods to make the query results anonymised (Geng, & Viswanath, 2016). Hashing is a cryptographic method with the intention irretrievably converts records into a unique data of random codes. Subsampling takes merely a segment of records from data sets. For noise injection, it inserts arbitrary data that obscures the original, sensitive identifiable individual information.

Let $\boldsymbol{\mathcal{A}}$ be a randomized algorithm on two neighboring datasets $\boldsymbol{D}$ and $\boldsymbol{D'}$, let $\boldsymbol{\mathcal{O}}$ be a random collection of likely outputs of $\boldsymbol{\mathcal{A}}$ (Dwork, 2011). Algorithm $\boldsymbol{\mathcal{A}}$ fulfils ε-differential privacy when it meets:

$$Pr[\mathcal{A}(D)\epsilon\mathcal{O}] \leq e^{\epsilon} Pr[\mathcal{A}(D')\epsilon\mathcal{O}] \tag{3.11}$$

Throughout this project, image processing like face detection and car plate recognition produces a significant amount of data. The application, named as diffpriv, is

an anonymisation tool with Laplace mechanism which fulfils ε-differential privacy (Rubinstein, & Alda, 2017).

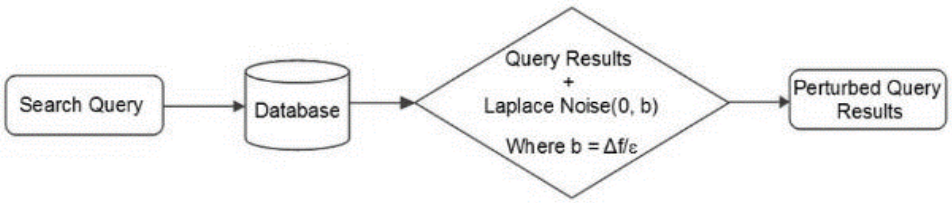


Figure 3.14 Flowchart of Laplace mechanism

The most common method to accomplish differential privacy is the Laplace mechanism which includes autonomous noise to the export of a numeric function f to satisfy ε-differential privacy of discharging f (Prasser, Kohlmayer, 2015).

$$\Delta f = max_{D,D'} ||f(D) - f(D')||_1. \quad (3.12)$$

It is sufficient to publish $f(D) + \boldsymbol{X}$ where $\boldsymbol{X}$ is drawn from Lap $(\frac{\Delta f}{\epsilon})$.

The weakness of differential privacy is apparent. Due to the assumption of background knowledge, we need to add a significant amount of randomisation to the aggregate results, leading to a sharp decline in the usability of analysing data. The answers might not be particularly valuable. Especially for those complex queries, sometimes the results of randomisation almost cover up the real results. This may be the reason why differential privacy is not much applied nowadays. The pseudocode for the algorithm of differential privacy is outlined in Algorithm 3.8. It introduces a differentially-private mechanism for releasing database. The algorithm takes advantage of the Bernstein polynomial of $\boldsymbol{F_D}$ as the noise injection of Laplace mechanism (Alda, & Rubinstein, 2017). This approximation consists of linear combination of the Bernstein polynomial. Its coefficients are evaluations of $\boldsymbol{D}$ on a cover $\boldsymbol{P}$.

Algorithm 3.8 Differential Privacy for Image Privacy Scoring

Input: Original dataset $D = (D_1, D_2, ..., D_n)$, privacy budget ϵ
Output: the publishing dataset D'

1: **procedure** DP(D, ϵ)
2: $record \leftarrow 0$
3: **for** $i \leftarrow 1, 2, .., n$ **do**
4: $record \leftarrow D(i) + \mathcal{L}aplace(\frac{2}{\epsilon})$
5: $D'.push(record)$
6: **end for**
7: **return** D'
8: **end procedure**

Algorithm 3.8 Differential privacy for image privacy scoring

Chapter 4
Results

This chapter presents the findings, analysis of data gathered, the primary objective is to accomplish the goal of this study by comparatively evaluating the experimental results. The findings which relate to the research questions guided our study. The data for each stage in privacy scoring will be detailed. Furthermore, data collections with the experimental environment will be articulated in this chapter, as well as the results of image privacy level will be clarified. The results and findings will be evaluated as well as the limitations of this thesis will be pointed out at the end of this chapter.

4.1 Privacy Factors

We investigated what the importance of each key factors of image privacy protection throughout an online questionnaire. This survey received 52 answer sheets. The interview questions are on a scale of 1 to 9 where nine indicates extremely important, and one is not at all critical. In this part, five charts will be present. Each chart represents the result of the corresponding question and followed by some explanations.

The factor accuracy is about whether an object can be accurately identified. Figure 4.1 shows nearly 80% believed that it plays a significant role in revealing image privacy. The average of the ratings is 7.29%.

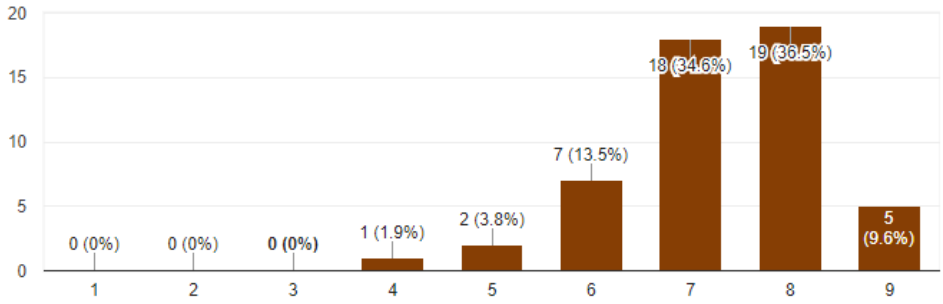


Figure 4.1 Survey result of factor accuracy

The factor ratio indicates the position and area ratio of an object. Figure 4.2 shows 73% of them thought that it is comparatively unimportant for this factor to determine the level of privacy disclosure. The average of these ratings is 3%.

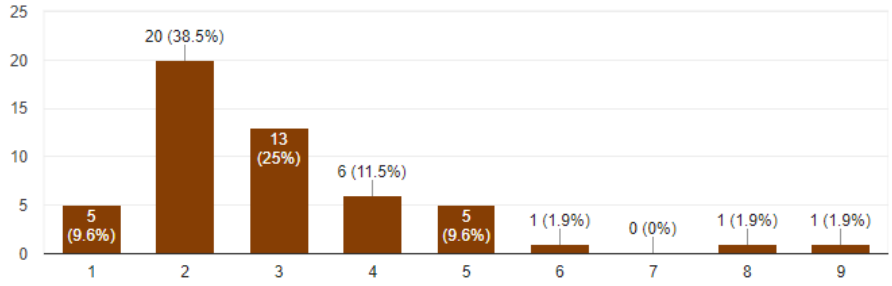


Figure 4.2 Survey result of factor ratio

The factor angle means the detected angle. According to the figures shown in the diagram, we see that Figure 4.3 shows 84.5% of them believed the detected angle is on the relative importance. The average of these ratings is 4.5%.

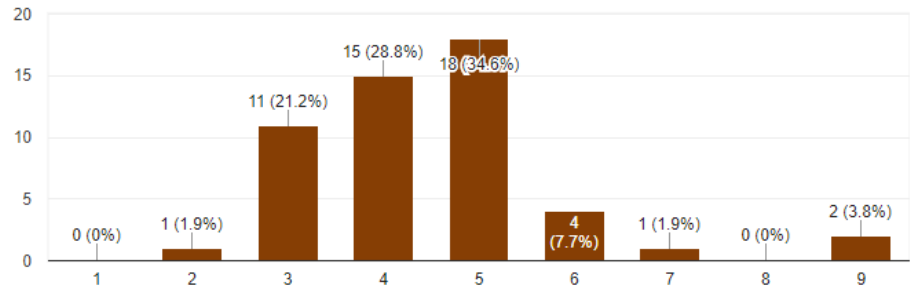


Figure 4.3 Survey result of factor angle

The factor sensitivity which represents whether the detected age is less than or equal to 17 or whether the car plate number is accurately recognised. The chart in Figure 4.4 reveals that more than three-quarters of respondents would opt for the factor sensitivity which is of great importance. The average of the ratings is 7.83%.

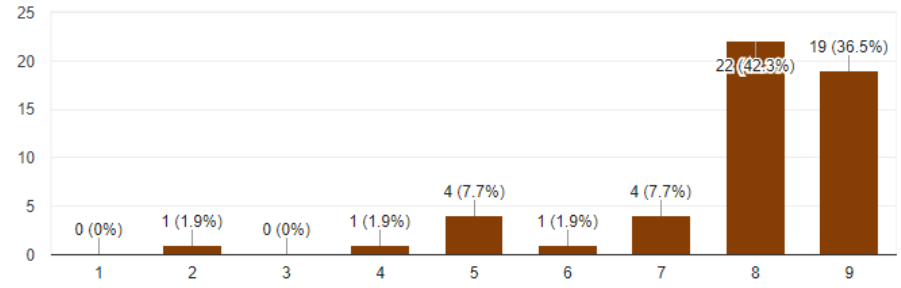


Figure 4.4 Survey result of factor sensitivity

The duration of time between the photos taken and published will affect the level of privacy. As we see in Figure 4.5, there is 32.7% who believed the factor timeliness is not at all critical. 48% of participants also praised for the factor being unimportant. The average of the ratings is 2.63%.

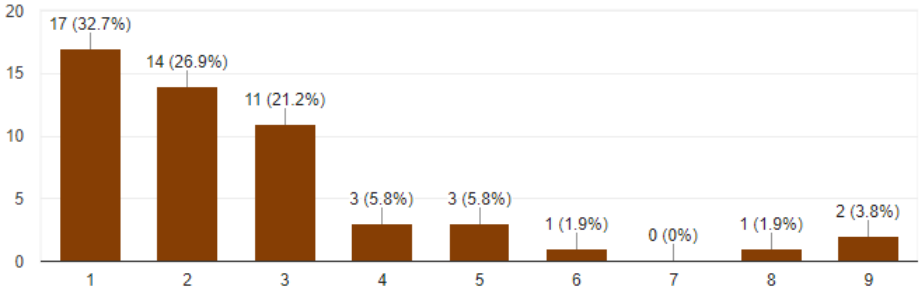


Figure 4.5 Survey result of factor timeliness

The questionnaire determined the score of each criterion in the judgement index. According to the principle of analytic hierarchy process, the results of each criterion are obtained, as illustrated in Table 4.1.

Table 4.1 The score of each criterion in the judgement index

	Accuracy	Ratio	Angle	Sensitivity	Timeliness
Accuracy	1	5	2	1	7
Ratio	1/5	1	1/3	1/4	2
Angle	1/2	3	1	1/3	4
Sensitivity	1	4	3	1	7
Timeliness	1/7	1/2	1/4	1/7	1

The matrix corresponding to this privacy scoring schema is shown as below:

$$\mathbf{C} = \begin{bmatrix} 1 & 5 & 2 & 1 & 7 \\ 1/5 & 1 & 1/3 & 1/4 & 2 \\ 1/2 & 3 & 1 & 1/3 & 4 \\ 3 & 4 & 3 & 1 & 7 \\ 1/7 & 1/2 & 1/4 & 1/7 & 1 \end{bmatrix} \tag{4.1}$$

Table 4.2 Weights of the privacy scoring schema

Names	**Weights**
Accuracy	34.43%
Ratio	7.55%
Angle	17.21%
Sensitivity	36.33%
Timeliness	4.48%

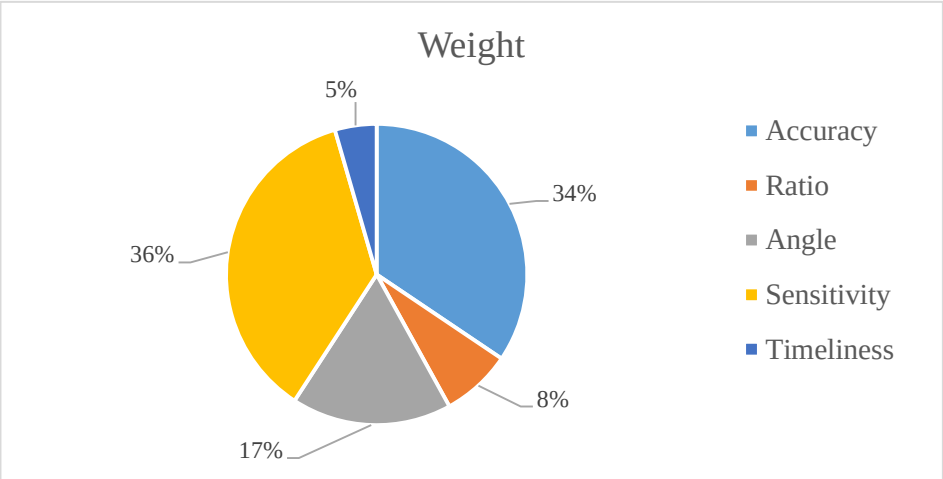


Figure 4.6 Weights of the privacy scoring schema

Privacy scoring method makes the privacy level of photos on a scale of 0 to 1.0, factoring in the five criteria, 1.0 indicates the maximum risk of privacy and 0 means there is no privacy issue. Then, each factor will be explained how to get their percentage.

Factor Accuracy C1 takes 34.43% in this privacy scoring method. OpenFace provides the confidence rate in percentage which is the input for the factor accuracy. The sample records show in Table 4.3. Confidence rate, between 0 and 1.0, is for the estimated detection rate.

Table 4.3 Sample records with confidence level value

	A	B	C	D	E	F	G	H	I
1	frame	success	confidence	pose_X(mm)	pose_Y(mm)	pose_Z(mm)	pitch(rad)	yaw(rad)	roll(rad)
2	0	1	0.421	101.984	19.779	707.863	0.221	0.274	0.112
3	1	0	0.231	101.069	20.669	715.464	0.22	0.252	0.173
4	2	0	0.537	98.818	20.771	711.298	0.214	0.241	0.197
5	3	0	0.54	97.386	20.653	708.471	0.223	0.229	0.197
6	4	0	0.585	95.68	20.716	705.372	0.224	0.227	0.196
7	5	1	0.911	87.012	21.191	722.713	0.09	-0.444	0.032
8	6	1	0.951	83.456	20.753	695.237	0.109	-0.706	0.057
9	7	1	0.956	81.818	20.553	687.665	0.103	-0.728	0.061
10	8	1	0.957	80.861	20.379	685.226	0.103	-0.724	0.061
11	9	1	0.959	79.963	20.333	683.863	0.104	-0.721	0.06
12	10	1	0.958	79.011	20.284	681.867	0.106	-0.716	0.059
13	11	1	0.958	78.224	19.951	680.488	0.104	-0.711	0.056
14	12	1	0.956	77.509	19.665	678.784	0.103	-0.708	0.052
15	13	1	0.955	77.048	19.493	678.196	0.103	-0.705	0.053
16	14	1	0.956	76.761	19.344	678.318	0.104	-0.704	0.054
17	15	1	0.96	76.625	19.025	679.54	0.103	-0.7	0.053
18	16	1	0.96	76.335	18.548	679.272	0.102	-0.697	0.055
19	17	1	0.96	75.9	17.958	678.578	0.104	-0.693	0.055
20	18	1	0.954	75.467	17.388	677.415	0.107	-0.69	0.055

For the factor Ratio C2 which shares 7.55% of the privacy scoring method, the proportion of the face-detected region in percentage to the photo could get from the method we proposed in previous chapter.

For the factor Angle C3 which shares 17.21% of the privacy scoring method, there are three kinds of rotations to be considered. The angle results are the output of OpenFace which are in radian. It needs to be converted into a degree. By definition, 360 degrees equal 2π radians. Hence, 1-degree equals $\frac{\pi}{180}$. As we mentioned previously, the detectable range of facial poses spans from -30˚ to 30˚ in pitch, from -20˚ to 20˚ in roll, and from -40˚ to 40˚ in yaw. Privacy level reaches its maximum value 1.0 as face turns roughly close to 0˚. Privacy level reaches its minima 0 when the face turns closely to the limit of this range. There are three linear equations listed as below:

$$\text{Rotation in roll: } y(\alpha) = \begin{cases} 0 & \alpha \notin (-\frac{\pi}{9}, \frac{\pi}{9}) \\ -\frac{9}{\pi} \cdot |\alpha| + 1 & \alpha \epsilon [-\frac{\pi}{9}, \frac{\pi}{9}] \end{cases} \tag{4.2}$$

$$\text{Rotation in pitch: } y(\beta) = \begin{cases} 0 & \beta \notin (-\frac{\pi}{6}, \frac{\pi}{6}) \\ -\frac{6}{\pi} \cdot |\beta| + 1 & \beta \epsilon [-\frac{\pi}{6}, \frac{\pi}{6}] \end{cases} \tag{4.3}$$

$$\text{Rotation in yaw: } y(\gamma) = \begin{cases} 0 & \gamma \notin \left(-\frac{2}{9}\pi, \frac{2}{9}\pi\right) \\ -\frac{9}{2\pi} \cdot |\gamma| + 1 & \gamma \epsilon \left[-\frac{2}{9}\pi, \frac{2}{9}\pi\right] \end{cases} \tag{4.4}$$

The factor sensitivity C4 shares the most essential 36.33% of the privacy scoring method. The age which is less than or equal to 17 has the most sensitivity whose privacy level at 1.0. Through comparisons, the detected age which is greater than 17 owns a normal sensitivity whose privacy level is at 0.5. Likewise, the privacy level is one as the confidence rate of car plate number detection is higher than 90% and otherwise it will be 0.

The factor Timeliness C5 shares the lowest 4.48% of the privacy scoring method. According to the Ebbinghaus Forgetting Curve, people tend to memorize 58% of the content after 20 minutes; one hour later, 44% was remembered; one day later, 26% were remembered; one week later, 23% were remembered, one month later, just 21% were remembered (Roediger,1985). By this rule, the interval of current time of the published

time can be mapped to the privacy level. At the moment when user shared a photo, the score is 1.0; after 20 minutes, the score is 0.58; one hour later, it is 0.44; one day later, it is 0.26; one week later, it is 0.23; one month later, it is 0.21.

4.2 Image Privacy

As the focus of this thesis is on implementing a method which can detect and analyse the object from an images to achieve the privacy level. In the experiment, the dataset of this project is a benchmark of 7648 frames of 26 recorded videos with variations of horizontal or vertical angles from -90 º to 90º. For each video, it is 10 seconds long and ranges from 20 FPS to 30 FPS. The size of the videos has 1280 pixels width and 720 pixels height. The data rate is 14560 kbps. The camera was set at a distance of 2 meters from the person. All videos were recorded by using this method. The background of these videos is relatively white and clean in order to focus on facial movement. There is a unique combination of face movement and camera location or angles in each video, as listed in Table 4.4.

Table 4.4 All the combinations of facial movements and position

Event	**Face Movement and Direction**	**Face Position**	**Camera Angle Relative to Face**	**Number of Frames**
1	Move horizontally from left 90° to the right 90°	Centre	Frontal position	203
2	Move horizontally from left 90° to the right 90°	Top	Frontal position	225
3	Move horizontally from left 90° to the right 90°	bottom	Frontal position	252
4	Move horizontally from left 90° to the right 90°	Right	Frontal position	220
5	Move horizontally from left 90° to the right 90°	Left	Frontal position	200

6	Move horizontally from left 90° to the right 90°	Top-right	Frontal position	311
7	Move horizontally from left 90° to the right 90°	Top-left	Frontal position	314
8	Move horizontally from left 90° to the right 90°	Bottom-right	Frontal position	310
9	Move horizontally from left 90° to the right 90°	Bottom-left	Frontal position	303
10	Move vertically from upward 90° to downward 90°	Centre	Frontal position	315
11	Move vertically from upward 90° to downward 90°	Top	Frontal position	330
12	Move vertically from upward 90° to downward 90°	Bottom	Frontal position	332
13	Move vertically from upward 90° to downward 90°	Right	Frontal position	305
14	Move vertically from upward 90° to downward 90°	Left	Frontal position	309
15	Move vertically from upward 90° to downward 90°	Top-right	Frontal position	315
16	Move vertically from upward 90° to downward 90°	Top-left	Frontal position	296
17	Move vertically from upward 90° to downward 90°	Bottom-right	Frontal position	326
18	Move vertically from upward 90° to downward 90°	Bottom-left	Frontal position	316
19	Move horizontally from left 90° to the right 90°	Centre	Move up and downwards by 30°	312

20	Move horizontally from left 90° to the right 90°	Centre	Move down and upwards by 30°	325
21	Move horizontally from left 90° to the right 90°	Centre	Move left and tilt by 30° towards the right	324
22	Move horizontally from left 90° to the right 90°	Centre	Move right and tilt by 30° towards the left	303
23	Move vertically from upward 90° to downward 90°	Centre	Move up and downwards by 30°	293
24	Move vertically from upward 90° to downward 90°	Centre	Move down and upwards by 30°	328
25	Move vertically from upward 90° to downward 90°	Centre	Move left and tilt by 30° towards the right	291
26	Move vertically from upward 90° to downward 90°	Centre	Move right and tilt by 30° towards the left	290
				7648

The sensitivity in the video for face detection is fixed; the age is higher than 17 years old. All video shooting time is from 10:08 14 March 2018 to 10:51 14 March 2018, and the experimental testing time is 25 April 2018 at 15:08. The time difference is more than one month, and the specific gravity value is 0.21. Therefore, from Event No. 1 to Event No. 26, sensitivity and timeline are fixed. We need to consider the influence of accuracy, specific gravity and angle on the privacy evaluations.

From Figure 4.7 to Figure 4.12, it shows the privacy level of the events at different angles and locations. By studying the differences of privacy of the faces in different directions in the same position or in different positions in the same direction, the comparisons were made and then analysed by comparing the data and then adjusting the weight ratio.

Figure 4.7 presents a comparison of horizontal and vertical face movements of Event No. 1 and Event No. 10 when the face is centred on the video frames. In Event No. 1, the left side was unstable with an extensive range of fluctuation. In Event No. 10, when the

face rose, its privacy was higher than the privacy when the face was at low positions. We had noted from the graph that when the face moved to the detectable angles, the privacy values of both events maintain at a high level. It rises to above 0.65, up to 0.73.

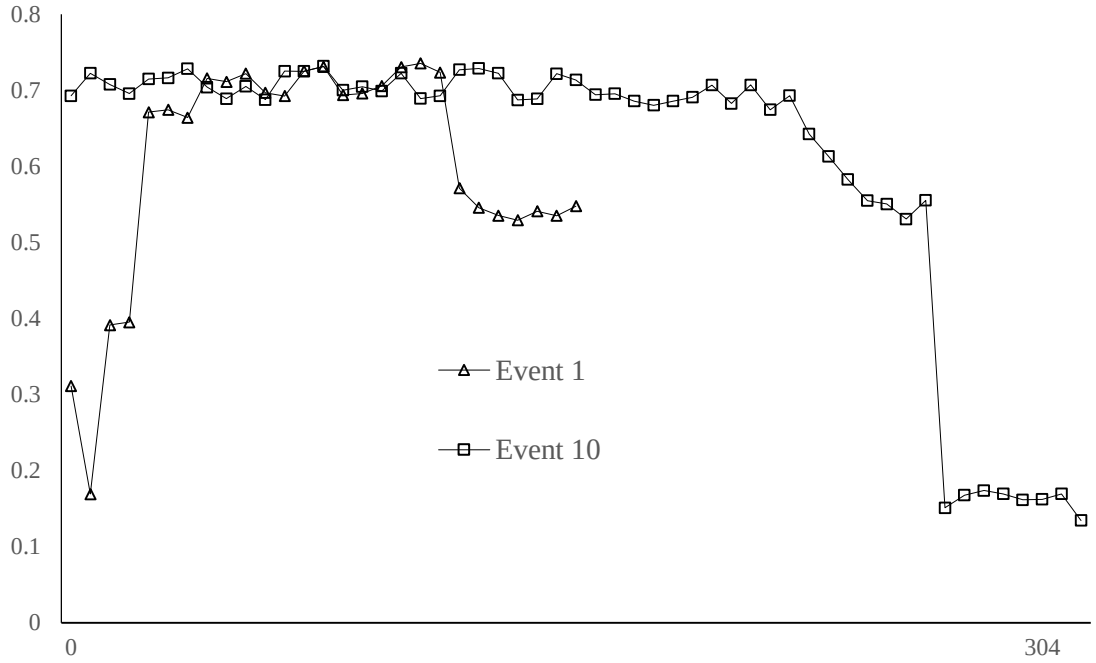


Figure 4.7 The comparison of the horizontal and vertical face movements when the face centred on the images

Figure 4.8 shows the collection of horizontal and vertical face movements of Event No. 2, Event No. 3, Event No. 11 and Event No. 12 when the face sites on the top and bottom of the images. It is noteworthy that the curve has fallen off from 0.64 to 0.67 when the face is being moved within the detectable range. The diagram shows a marked decline at the level of privacy when approaching to the end of those facial movements compared with that at the beginning of each movement.

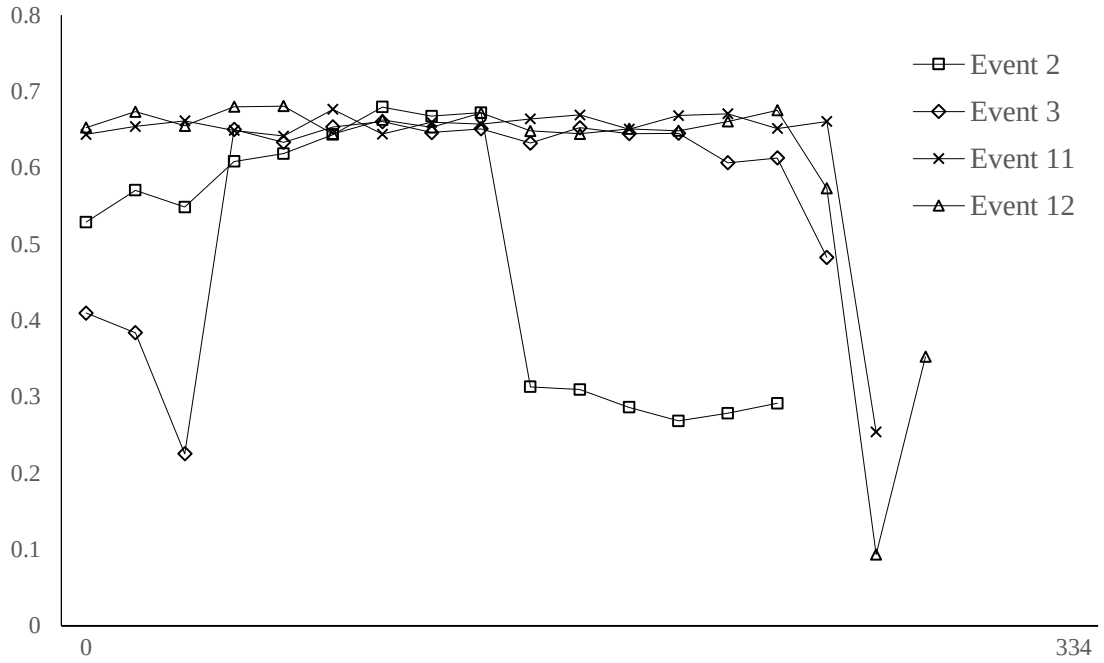


Figure 4.8 The collection of horizontal and vertical face movements when the face sites on the top and bottom of the images

Figure 4.9 displays the collection of horizontal and vertical face movements of Event 4, Event 6, Event 8, Event 13, Event 15 and Event 17 when the face sites on the right third of the images. According to the points shown in Figure 4.9, when the face is on the right third of the picture, the face is tilted to the left or tilted upwards, which is lower than the privacy level on the right side of the face. By comparing with Events 6, 8, 15 and 17, Events 4 and 13 have a higher privacy level. The highest privacy level for Events 4 and 13 is between 0.63 and 0.68, while the highest privacy level for Events 6, 8, 15 and 17 is between 0.6 and 0.63.

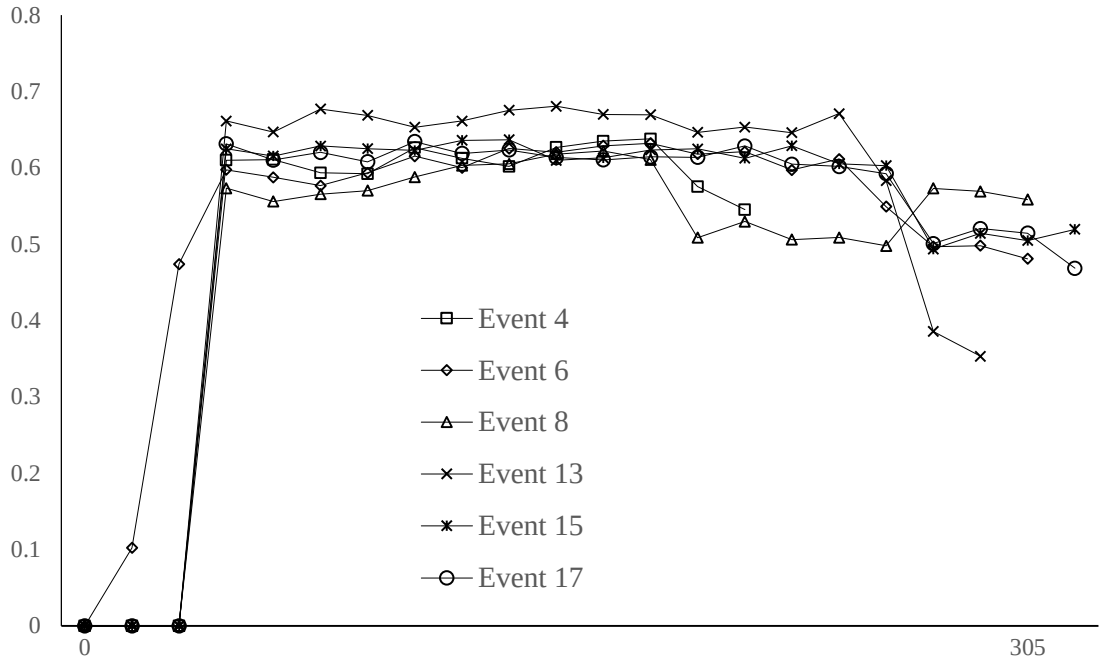


Figure 4.9 The collection of horizontal and vertical face movements when the face sites on the right third of the images.

Figure 4.10 presents the collection of horizontal and vertical face movements of Events 5, 7, 9, 14, 16 and 18 when the face sites on the left third of the images. We see from the statistics when the face is on the left, it is almost opposite to the curve shown in Figure 4.9. The privacy level of the right side and bowed face is slightly lower. By comparing with Event 5 and 14, Events 7, 9, 16 and 18 have a higher privacy level. The highest privacy level for Events 5 and 14 is between 0.64 and 0.68, while the highest privacy level for Events 7, 9, 16 and 18 is between 0.61 and 0.64.

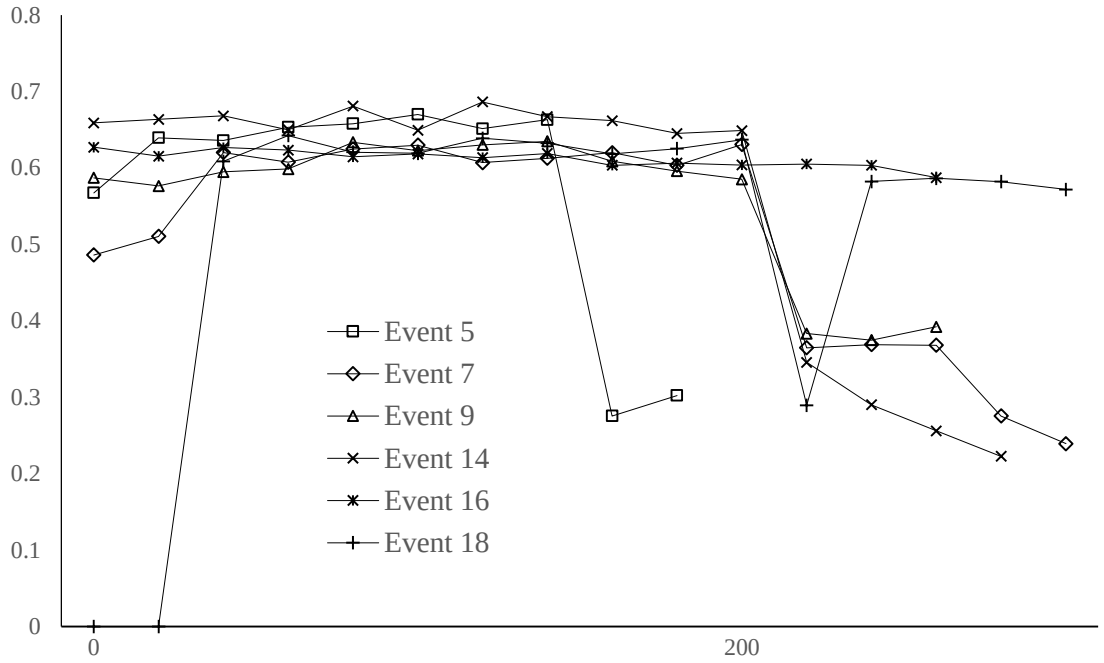


Figure 4.10 The collection of horizontal and vertical face movements when the face sites on the left third of the images

Figure 4.11 displayed the collection of Events 19, 20, 25 and 26 when the face was at the centre of the images. As the face was moving horizontally from left to right, the camera followed up and tilted down by 30° in Event 19, and the camera moved down and tilted up by 30° in Event 20. As the face was moving vertically from upward to downward, the camera was being moved left and tilted right by 30° in Event 25, and the camera moved right and tilted left by 30° in Event 26. When the face was shifting horizontally, the camera tilted up and down, and the image shows a lower privacy level curve on the left and right sides. Similarly, when the face was rising vertically, the camera tilted to the left and right, and their curves slide down at the upper and lower ends. The graph shows that it does not have much influence on the privacy level curve when the face looks horizontally, the camera tilted up and down; when the face rotated vertically, the camera tilted left and right compared with when the camera was at the frontal position. Besides, their highest value is between 0.61 and 0.69.

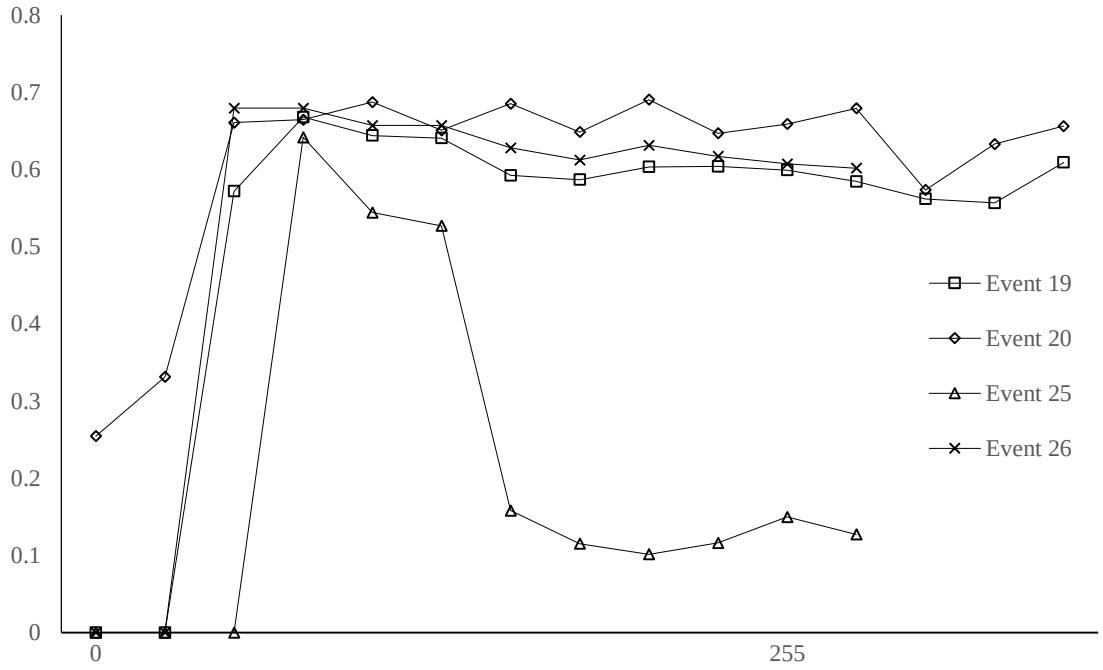


Figure 4.11 The collection of events 19, 20, 25 and 26
when the face was centred on the images

Figure 4.12 shows the collection of Events 21, 22, 23 and 24 when the face was at the centre of the images. As the face turned horizontally from left to right, the camera moved left and tilted right by 30° in Event 21, and the camera moved right and tilted left by 30° in Event 22. As the face moved vertically from upward to downward, the camera looked up and tilted down by 30° in Event 23, and the camera rotated down and tilted up by 30° in Event 24. When the face turned horizontally, the camera tilted to the left, showing that the privacy level on the left was always high. Even though the angle of the left side of the face is smaller than that of the right face; the high value of its privacy level was always on the left. Similarly, when the face moved horizontally and the camera tilted to the right, the higher privacy level was always on the right. When the face turned horizontally and the camera tilted downward, its privacy level is the highest. When the camera leaned upward, the privacy level is the highest one when the head was lowered. Their highest priority level is between 0.69 and 0.73.

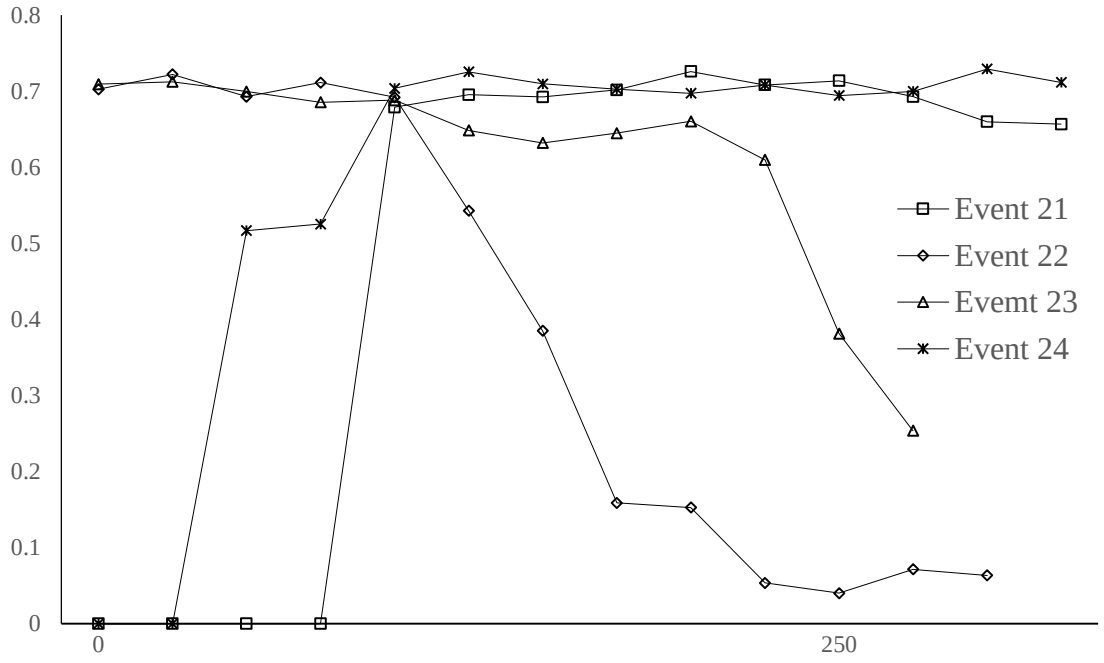


Figure 4.12 The privacy evaluations of the collection consisting of Events 21, 22, 23 and 24 when the face was centred on the images

Figure 4.13 is the privacy level curve of the car. According to the chart, the privacy level of the vehicle is more apparent when the vehicle is moving. When the angle is over 45°, the privacy of the vehicle does not exist. The privacy level of the license plate is between 0.58 to 0.61.

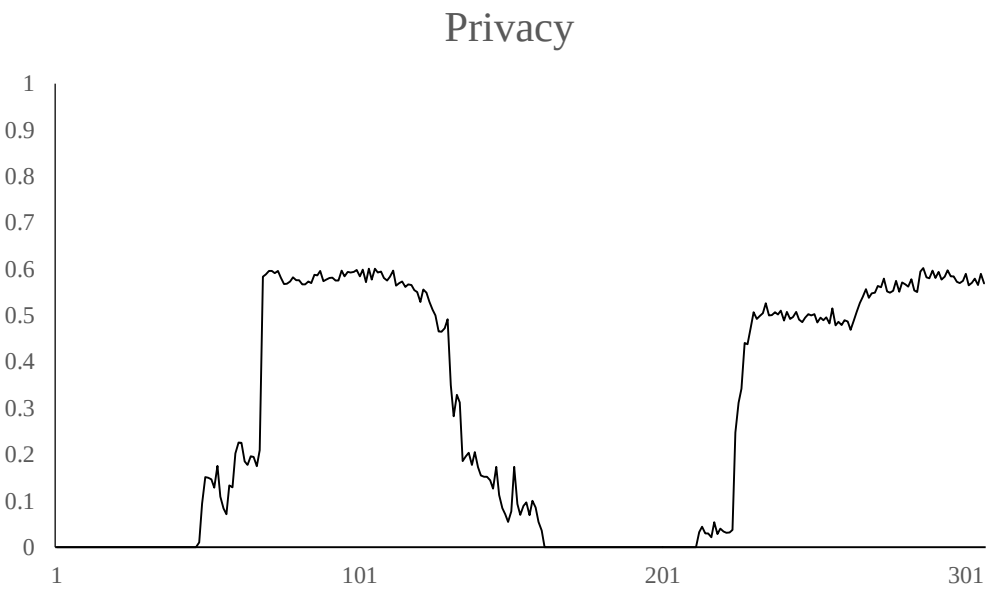


Figure 4.13 The result of privacy level in car plate detection

Figure 4.14 Privacy of a car and an adult.

Adult: 0.6137. Car plate number: 0.6112

Table 4.4 Privacy proportion of the adult on Figure 4.14

Adult	Privacy	Weight	Score
Accuracy	0.975	0.3443	0.3356925
Ratio	0.3	0.0755	0.02265
Angle	0.3736	0.1721	0.06429656
Sensitivity	0.5	0.3633	0.18165
Timeliness	0.21	0.0448	0.009408
Privacy level	0.61369706		

Table 4.5 Privacy proportion of the car plant number of Fig 4.14

Adult	Privacy	Weight	Score
Accuracy	0.9493	0.3443	0.32684399
Ratio	0.8	0.0755	0.0604
Angle	0.6132	0.1721	0.10553172
Sensitivity	0.3	0.3633	0.10899
Timeliness	0.21	0.0448	0.009408
Privacy level	0.61117371		

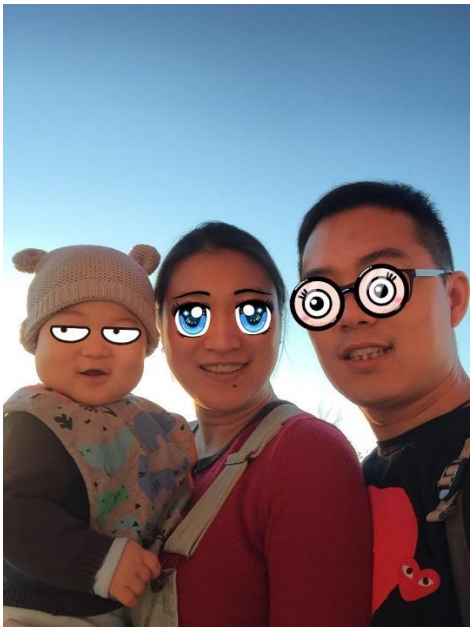


Figure 4.15 Privacy of family image. Child: 0.849; Adult No.1 at the middle: 0.7102; Adult No.2 at right side: 0.596

Table 4.6 Privacy proportion of the child on Figure 4.15

Child	Privacy	Weight	Score
Accuracy	0.975	0.3443	0.3356925
Ratio	0.5	0.0755	0.03775
Angle	0.5844	0.1721	0.10057524

Sensitivity	1	0.3633	0.3633
Timeliness	0.26	0.0448	0.011648
Privacy level	0.84896574		

Table 4.7 Privacy proportion of the adult No.1 on Figure 4.15

Adult No.1 Female	Privacy	Weight	Score
Accuracy	0.975	0.3443	0.3356925
Ratio	0.8	0.0755	0.0604
Angle	0.7021	0.1721	0.12083141
Sensitivity	0.5	0.3633	0.18165
Timeliness	0.26	0.0448	0.011648
Privacy level	0.71022191		

Table 4.8 Privacy proportion of the adult No.2 on Figure 4.14

Adult No.2 Male	Privacy	Weight	Score
Accuracy	0.975	0.3443	0.3356925
Ratio	0.5	0.0755	0.03775
Angle	0.1907	0.1721	0.03281947
Sensitivity	0.5	0.3633	0.18165
Timeliness	0.26	0.0448	0.011648
Privacy level	0.59955997		

We analysed and evaluated the pictures through the experimental results. The sample result of privacy level. The sample results for 20 pictures are shown in Figure 4.16.

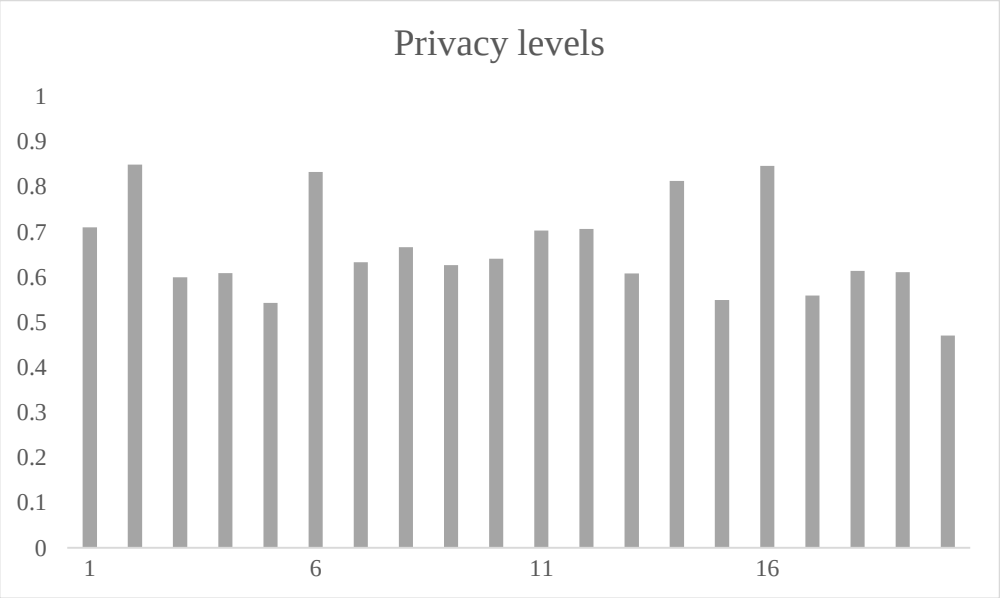


Figure 4.16 The sample result of privacy levels

4.3 Differential Privacy

Differential privacy protection is a mechanism of preprocessing and disturbance processing of raw input data. Table 4.9 presents a sample of the original input data for the image privacy scoring mechanism. A record of the PhotoId column is generated when a new image added. The confidence rate of factor accuracy is the output from OpenFace and OpenALPR. The factor ratio is the score of the bounding box of the recognised face or license plate in the position of the picture. The factor angle is the measured radians of the pitch, yaw, and roll. There are two types and their respective values in the factor sensitivity. The last factor is the time when the image was taken.

As shown in the Table 4.10, the score of each factor in [0,1] range is calculated according to 3.2. The privacy score is calculated based on the proportion of each criterium of section 4.1.

Table 4.9 The sample of the original input data for the mechanism of the image privacy scoring

PhotoId	Accuracy	Ratio	Angle	Sensitivity	Time
46247510	0.975	338,575,255,255,960,1280	0.111,-0.018,-0.104	age, 22	2018 05 03 17 21 00
72187488	0.975	314,305,380,380,1080,1440	0.493,0.089,-0.09	age, 1	2018 05 03 17 21 00
90545463	0.975	628,497,316,316,960,1280	0.036,0.565,-0.209	age, 26	2018 05 03 17 21 00
29309420	0.975	465,479,74,74,1200,1600	0.388,-0.257,-0.098	age, 32	2015 04 22 23 44 00
98920781	0.94	928,1020,100,74,1200,1600	-0.249,0.079,-0.13	plate, 1	2015 04 22 23 44 00
19372789	0.975	108,620,209,209,960,1280	0.009,-0.346,0.074	age, 2	2018 05 03 17 21 00
35936488	0.925	227,305,185,185,480,640	0.263,0.054,0.09	age, 44	2009 03 24 23 21 30
71801014	0.975	162,399,180,180,480,640	-0.169,-0.287,-0.072	age, 34	2009 03 24 23 21 30
21913272	0.975	108,191,191,191,480,640	-0.107,-0.225,-0.224	age, 58	2009 03 24 23 21 30
57819887	0.975	130,281,200,200,480,640	-0.36,0.019,-0.07	age, 71	2009 03 24 23 21 30
78637089	0.975	213,422,190,190,480,640	-0.101,0.066,-0.028	age, 34	2009 03 24 23 21 30
89254383	0.975	191,254,190,190,480,640	-0.056,0.048,-0.107	age, 45	2009 03 24 25 25 42
96801967	0.975	59,116,222,222,480,640	-0.346, -0.062,-0.042	age, 66	2009 03 24 25 25 42
54206959	0.975	470,305,63,63,1280,960	0.388,0.005,-0.102	age, 11	2017 03 30 12 04 59
15194062	0.975	156,212,206,206,960,1280	0.653,-0.305,-0.05	age, 29	2017 03 30 07 41 58
56128267	0.975	367,233,147,147,960,1280	0.218,0.084,0.092	age, 3	2017 03 30 07 41 58
46005818	0.9498	920,840,196,84,1440,1080	-0.026,0.284,-0.092	plate, 1	2018 05 04 08 04 36
29533275	0.975	200,54,79,79,1024,768	0.328,-0.246,0.212	age, 78	2018 01 15 12 16 27
94163372	0.9493	502,375,144,47,1024,768	-0.367,0.062,0.13	plate, 1	2018 01 15 12 16 27
64876248	0.7667	237,196,40,23,400,268	-0.371,0.249,-0.043	plate, 1	2018 03 07 16 11 06

Table 4.10 The sample output data for the mechanism of the image privacy scoring

PhotoId	Accuracy	Ratio	Angle	Sensitivity	Timeliness	Privacy level
46247510	0.975	0.8	0.7021	0.5	0.26	0.7102
72187488	0.975	0.5	0.5844	1	0.26	0.849
90545463	0.975	0.5	0.1907	0.5	0.26	0.5996
29309420	0.975	0.5	0.2590	0.5	0.21	0.6091
98920781	0.94	0.3	0.4532	0.3	0.21	0.5427
19372789	0.975	0.5	0.5044	1	0.21	0.833
35936488	0.925	0.5	0.4977	0.5	0.21	0.6329
71801014	0.975	0.5	0.5889	0.5	0.21	0.6659
21913272	0.975	0.5	0.3583	0.5	0.21	0.6262
57819887	0.975	0.8	0.3125	0.5	0.21	0.6409
78637089	0.975	0.5	0.8071	0.5	0.21	0.7034
89254383	0.975	0.8	0.6935	0.5	0.21	0.7065
96801967	0.975	0.3	0.3392	0.5	0.21	0.6078
54206959	0.975	0.8	0.2590	1	0.21	0.8134
15194062	0.975	0.3	0.0000	0.5	0.21	0.5494
56128267	0.975	0.5	0.5837	1	0.21	0.8466
46005818	0.9498	0.3	0.4684	0.3	0.44	0.559
29533275	0.975	0.3	0.3736	0.5	0.21	0.6137
94163372	0.9493	0.8	0.6132	0.3	0.21	0.6112
64876248	0.7667	0.5	0.2914	0.3	0.21	0.4703

Since the privacy scores of this picture directly reveal the privacy degree of the picture without complicated picture processing. It is easy to obtain high-privacy pictures

by looking at critical scoring parameters and privacy scoring. In order to protect the privacy of the picture and consider the future of the extensive application of third-party cooperation, the output data also need privacy protection. The three columns of PhotoId, Sensitivity and Privacy Level are processed by adding Laplace noise. As a consequence, the following output results are obtained so that we could safely release a differentially private dataset, as shown in the Table 4.11.

Table 4.11 The samples of the dataset for calculating differential privacy

PhotoId	Accuracy	Ratio	Angle	Sensitivity	Timeliness	Privacy level
47132021	0.98	0.8	0.70	0.73	0.26	0.75
54150618	0.98	0.5	0.58	0.63	0.26	0.69
57368274	0.98	0.5	0.19	0.57	0.26	0.66
57611865	0.98	0.5	0.26	0.54	0.21	0.64
56875242	0.94	0.3	0.45	0.53	0.21	0.63
56489712	0.98	0.5	0.50	0.54	0.21	0.64
56878427	0.93	0.5	0.50	0.55	0.21	0.65
57812955	0.98	0.5	0.59	0.56	0.21	0.66
58783390	0.98	0.5	0.36	0.56	0.21	0.66
59336811	0.98	0.8	0.31	0.56	0.21	0.66
59304732	0.98	0.5	0.81	0.56	0.21	0.66
58869955	0.98	0.8	0.69	0.57	0.21	0.66
58465475	0.98	0.3	0.34	0.57	0.21	0.67
58548522	0.98	0.8	0.26	0.58	0.21	0.68
59331804	0.98	0.3	0.00	0.59	0.21	0.68
60576221	0.98	0.5	0.58	0.58	0.21	0.68
61579789	0.95	0.3	0.47	0.56	0.44	0.67
61588514	0.98	0.3	0.37	0.53	0.21	0.65
61058589	0.95	0.8	0.61	0.49	0.21	0.62
64509993	0.77	0.5	0.29	0.40	0.21	0.57

Chapter 5
Analysis and Discussion

In this chapter, the discussion and resultant analysis with respect to outcomes of the experiments are demonstrated and presented. In this chapter, we will discuss the two parts of the statistical analysis from the results of previous chapters. The first part will highlight the results that support the primary goal of the thesis. More specifically, comparisons regarding the performance of various classifiers will be discussed in this chapter. The clear demonstration of outcomes from image privacy will be addressed. Finally, the significance will also be stated through analysing the outcomes.

5.1 Analysis of Expected Results and Actual Results

It is the survey result to test the responses on rating the privacy concerns of a lady's picture which is the adult No. 1 as shown in Figure 4.15. Most people care about preserving lady's privacy as Figure 5.1. According to the survey results, the average privacy is 0.6534. The result of our experiment is 0.7102. The difference between the two results is 0.0568. The result calculated by the system is 5.68 % higher than the result of the questionnaire survey and exceeds 0.68 %. Therefore, we will carry out the relevant weights of the female privacy scores again. Also, due to limitations of the questionnaire survey, when the expected result is significantly different from the result calculated by the actual system, we need to collect and debug the relevant data again and control the difference to 5 %.

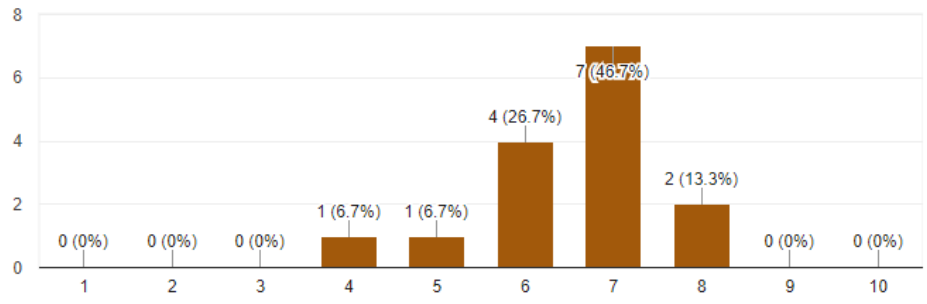


Figure 5.1 Privacy level for the lady in the image

It is the survey result to test the responses on rating the privacy concern of a child's picture which is shown in Figure 4.15. In Figure 5.2, the calculated average privacy is 0.8667. The experimental result is that the privacy is 0.849. The difference between the two results is 0.0177. The questionnaire is 1.77 % higher than the result calculated by using the algorithms. The difference between these two is within 5 %, which shows that the results calculated by the algorithms are relatively accurate.

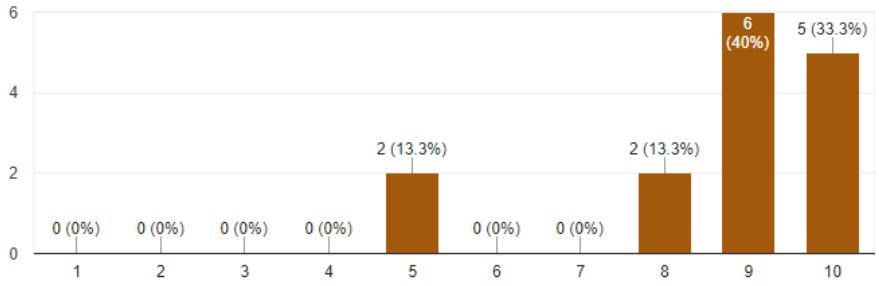


Figure 5.2 Privacy level for the baby in the image

Figure 4.15 shows the responses on rating the privacy concern of a gentleman's picture (adult No. 2). As shown in the Figure 5.3, the privacy for men is at an intermediate value. The average privacy calculated by the chart is 0.58. The result from the experimental calculation is 0.5996. The difference between the two values is 0.0196, and the difference remains within 5%. It shows that the results calculated by the system are relatively accurate in the process of men's privacy calculation.

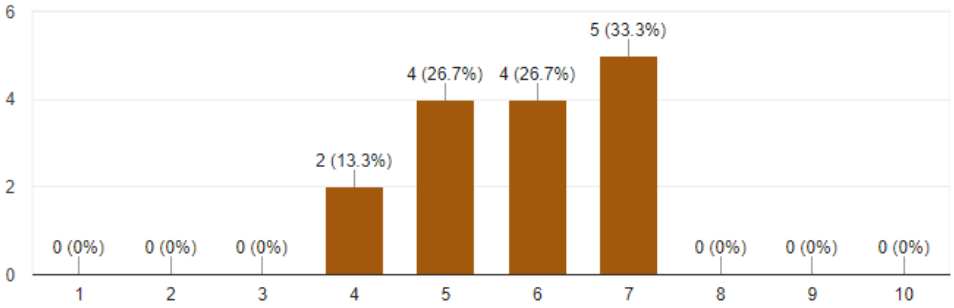


Figure 5.3 Privacy level for the gentleman in the image

Figure 5.4 is a comparison of the results shown the privacy scores for 20 test pictures. The comparison is between the expected results and the results calculated by the algorithms. This histogram can generally show that these two results are very close each other and the difference between them is very minor. The specific difference will be analysed by using ROC curves.

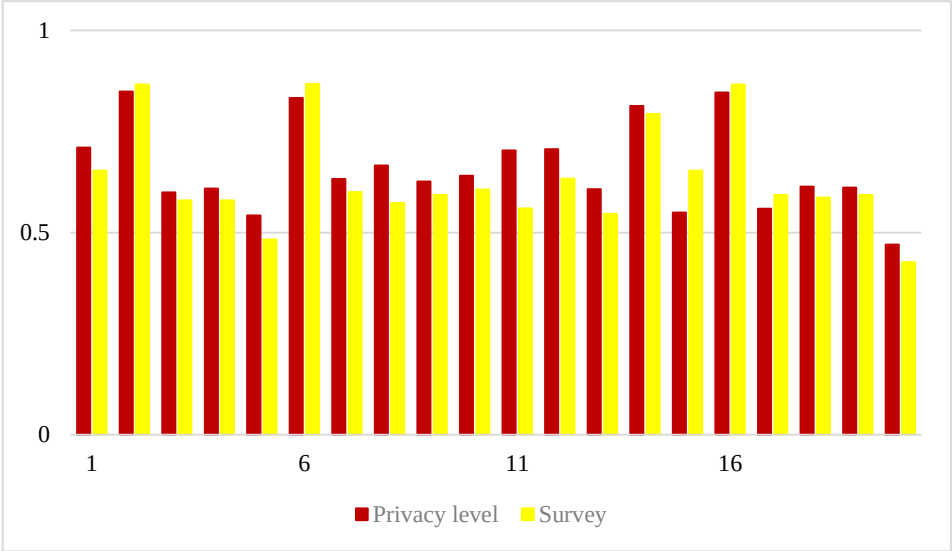


Figure 5.4 Privacy levels v.s. survey results

The data difference between the calculated results and the expected results was statistically analysed in Figure 5.5 and Figure 5.6. There was not significant difference in accuracy.

SUMMARY	*Count*	*Sum*	*Average*	*Variance*
Survy Score	20	12.5131	0.6257	0.0126
Privacy Level	20	13.1908	0.6595	0.0115
	2	1.3635	0.6818	0.0016
	2	1.7157	0.8579	0.0002
	2	1.1796	0.5898	0.0002
	2	1.1891	0.5946	0.0004
	2	1.0360	0.5180	0.0012
	2	1.6128	0.8064	0.0014
	2	1.2329	0.6165	0.0005
	2	1.2392	0.6196	0.0043
	2	1.2195	0.6098	0.0005
	2	1.2476	0.6238	0.0006
	2	1.2634	0.6317	0.0103
	2	1.3398	0.6699	0.0027
	2	1.1545	0.5773	0.0019
	2	1.6067	0.8034	0.0002
	2	1.1561	0.5781	0.0016
	2	1.6933	0.8467	0.0000
	2	1.1523	0.5762	0.0006
	2	1.2004	0.6002	0.0004
	2	1.2045	0.6023	0.0002
	2	0.8970	0.4485	0.0010

Figure 5.5 The results of variance analysis between survey score and privacy level

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Rows	0.0115	1.0000	0.0115	11.9646	0.0026	4.3807
Columns	0.4405	19.0000	0.0232	24.1597	0.0000	2.1683
Error	0.0182	19.0000	0.0010			
Total	0.4702	39.0000				

Figure 5.6 The results of variance analysis

The ROC curve has an excellent characteristic. It remains unchanged as the distribution of positive and negative samples in the test set changes. Class imbalance often occurs in real datasets. There are more negative samples than positive samples or vice versa, and the distribution of positive and negative samples in the test data may change with time. The area of the ROC curve is Area Under the Curve, referred to as AUC. AUC is used to measure the performance of machine learning algorithms for two classification problems. Since the ROC curve is generally above the ***y*=*x*** line, the range of values for AUC is generally between 0.5 and 1. The reason why AUC is used as the evaluation criterion is that the ROC curve often does not indicate which classifier has better effect, while as a value, the classifier with the larger AUC has the better effect. The greater the AUC values, the more the current classification algorithm is to rank positive samples ahead of negative ones.

Figure 5.7 is the ROC curve of the expected results and the actual calculated results from Figure 5.4. The ROC analysis shows that the AUC of the ROC of the calculated results is approximately 0.726, indicating that its accuracy is very high, nearly 73 %. The detected results are verified by the expected results, and the **P** value is greater than 0.05.

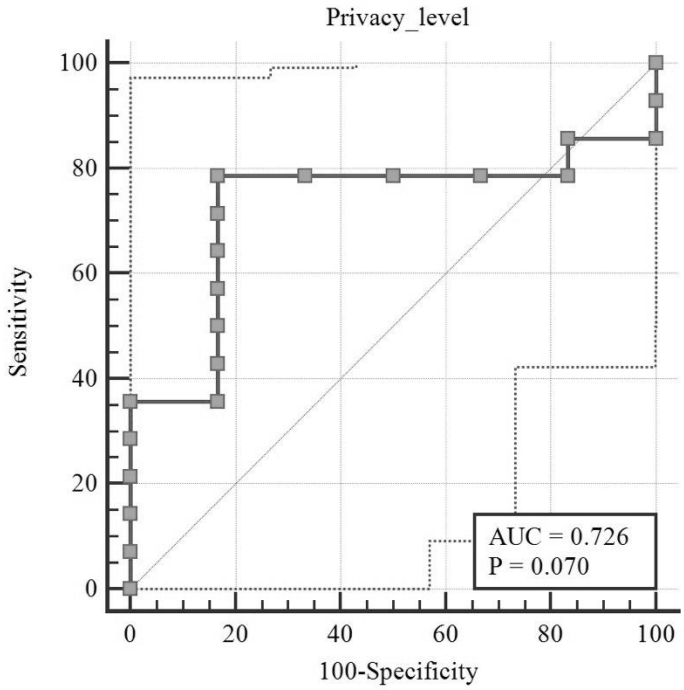


Figure 5.7 ROC metric to evaluate privacy level

The objective of this experiment was to test the results of the attacker's node identification attack on the published social network with different background. An attacker carries out node identification attack by querying the published network to obtain a candidate set that matches the target object. The larger the matching set, the smaller the identification probability, and vice versa.

Figure 5.8 is a comparative diagram of the PhotoId in the original data of Figure 4.10 and the PhotoId data in Figure 4.11 after the noise has been added. When coupled with the graphics information in Figure 5.8, the data of the PhotoId is injected with noise to ensure that there is no duplicate Id. It indicates that the perturbed data in turn hides the identifiable information. Therefore, when the noisy photo with PhotoID is made public, it is effective to avoid retrieving and raw data through identity information, which is the meaning of the calculation of differential privacy.

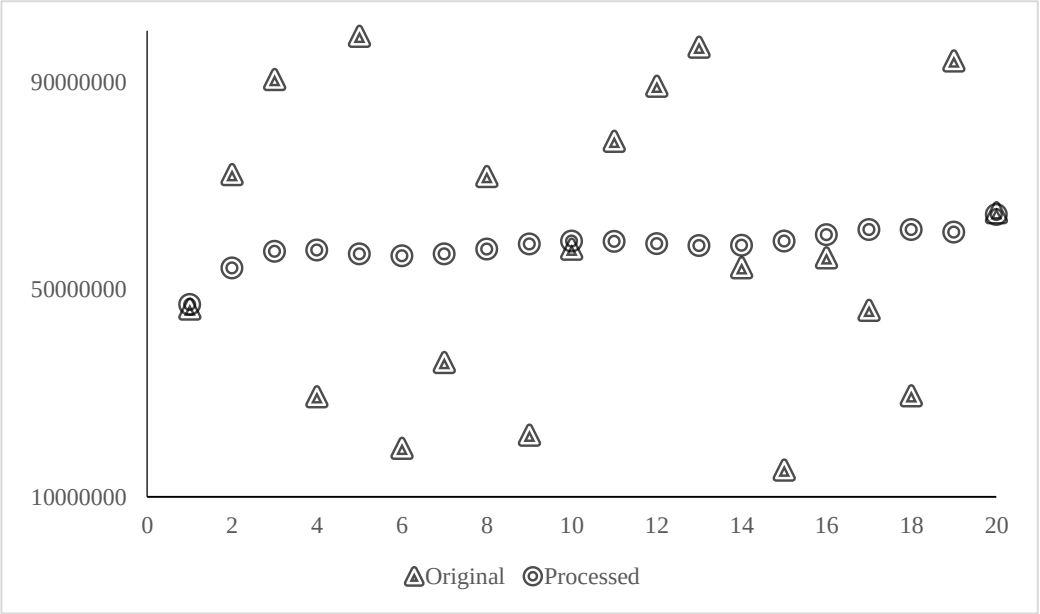


Figure 5.8 The original PhotoId vs the published one

Figure 5.9 shows the comparison of the protected privacy level with the original data from Figure 4.10 and Figure 4.11. The diagram depicts that the released dataset is in a more regular interval. When the results of the experiment are released by injecting noise, the viewer does not find the corresponding experimenter in the picture through the results. The analysis of this graph can clearly show that this differential privacy can avoid the disclosure of privacy.

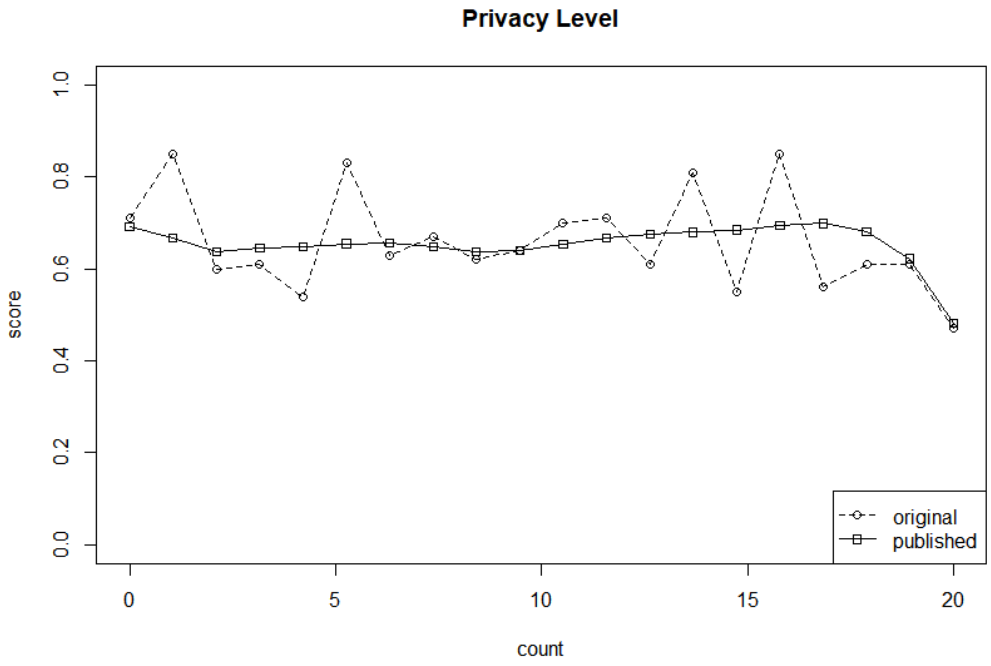


Figure 5.9 The original records of privacy level vs the published one

Likewise, the sensitivity has also been done in the same process as shown in the Figure 5.10. Figure 5.10 is a comparative analysis of sensitive data from Figure 4.10 and Figure 4.11. This diagram shows that the data, added the noises, does not coincide with the original data, which securely avoids the data breach caused by the index being recalculated after the data is published, thus the user's privacy information is protected.

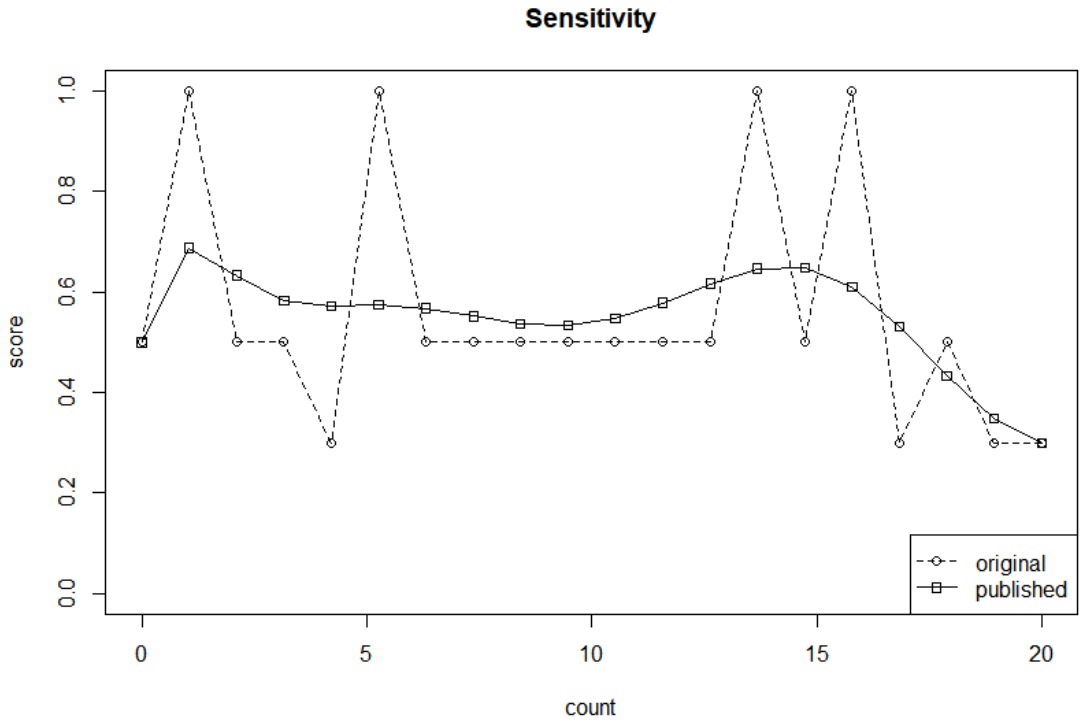


Figure 5.10 The original records of sensitivity vs the processed one

5.2 The Significance of the Experimental Results

With the rapid development of the social network, more and more experts from data mining, sociology, database and other fields have been attracted to conduct in-depth research and analysis on it. Social networks usually contain some sensitive personal attributes, relationships between individuals, graphic structures and other information. The privacy may be leaked or destroyed in the process of analysis and research. We expect that this research would allow users to maximise their privacy protection before publishing information on social networks and minimise their privacy leakage and damage to their interests.

Throughout the analysis of the questionnaires, we can make a clear comparison and analysis of the experimental results. Then through the ROC curve, we can understand the results of our experiments well, we can promptly change weights to ensure the accuracy of the privacy scores. The comparisons and analysis of these results before and after adding noises make the data having a more reliable results after analysis.

Through the experimental results of this paper, we can accurately analyse the privacy scores of each picture, so that the publisher can clearly know the degree of privacy of the pictures or videos they post. When the publishers release their own pictures, they could protect their own privacy. Similarly, we encrypt the corresponding data, or we can effectively prevent data breaches caused by data indexing and re-analysis. Publishers enjoy sharing information while also protecting their privacy information, which is the purpose of this research project.

Chapter 6

Conclusion and Future Work

In this thesis, in-depth articulation of the techniques was discussed which can be utilised to analyse the privacy scoring on media images. The main findings concerning the research questions are summarised; general conclusions based on the findings of the studies presented in this research are revealed. The similar approaches for each step have been implemented as the results of this thesis. In this chapter, we emphasise the strengths and limitations of the thesis. However, there are some considerations as well as suggestions for further research at a scholarly level, and conclusions are highly organised and integrated into the context. Meanwhile, the future work will be pointed out by the end of this thesis.

The mechanism for evaluating privacy of social images is implemented to let users be recognised what the privacy level is to affect user's published privacy information on the shared images by evaluating privacy risk. With the progress of data computing ability, the conflict between privacy and interpersonal relationship and human nature can be used to locate the individual by analysing the gender, age, education level, consumption behaviour, social activity, activity position, economic status and so on. Even a more severe situation is that privacy will always exist, the problem is that human daily and social life will be affected probabaly by the data, including both positive and negative.

For privacy protection, information security and surveillance abuse, in the context of massive data, these factors are intertwined. How to use computing technology to identify better illegal content and privacy content is the need for further development of technology to solve the breakthrough problem.

In this study, our differential privacy by injecting the data with Laplace noise to achieve the privacy protection of picture data release. The proposed method can ensure that privacy and security do not limit the attacker's background knowledge. It can resist various forms of privacy attacks and obtain acceptable publishing quality. There are still some problems with the method proposed in this dissertation for differential privacy, which needs to be further studied. On the one hand, our algorithm is still rudimentary. How to optimise the algorithm, reduce the error as well as improve the effectiveness of the published data remains to be further studied. On the other hand, though the proposed privacy protection method has realised the privacy protection to the weight, the attacker cannot infer the connection strength among the social individuals according to the published social network. However, this method only is taken of considerations of the anonymity of the weight itself. It does not think about the importance of the anonymity of the weights and the correlation between the weights. Subsequential research will conduct how to maintain the weight attribute in the published social network.

We work for this research project and hope that while people enjoy the convenience brought by social media, they can share their pictures and videos without revealing their privacy as much as possible. Because there is no absolute privacy in the world, and all

privacy will not be wholly protected from disclosure. This research hopes to protect people's privacy. In this thesis, there are many categories of privacy that are not considered. In future, the classification of privacy will be further subdivided to make the privacy scoring system more comprehensive and accurate.

References

Abdalaal, A., Nergiz, M. E., & Saygin, Y. (2013). Privacy-preserving publishing of opinion polls. Computers and Security, 37, (pp. 143–154).

Aggarwal, C. C., & Philip, S. Y. (2008). A general survey of privacy-preserving data mining models and algorithms. In Privacy-preserving data mining (pp. 11-52). Springer, Boston.

Ahern, S., Eckles, D., Good, N., King, S., Naaman, M., & Nair, R. (2007). Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, (pp. 357–366). ACM.

Alda, F., & Rubinstein, B. I. (2017). The Bernstein Mechanism: Function Release under Differential Privacy. In AAAI (pp. 1705-1711).

Aldeen, Y. A. A. S., Salleh, M., & Razzaque, M. A. (2015). A comprehensive review on privacy preserving data mining. SpringerPlus, 4(1), (pp. 694).

Almalki, N., Curtmola, R., Ding, X., Gehani, N., & Borcea, C. (2017). P2F2: Privacy-preserving face finder. In 37th IEEE Sarnoff Symposium, Sarnoff 2016 (pp. 214–219).

Ananthula, S., Abuzaghleh, O., Alla, N. B., Chaganti, S. B., Kaja, P. C., & Mogilineedi, D. (2015). Measuring privacy in online social networks. International Journal of Security, Privacy and Trust Management, 4(2), (pp. 1-9).

Archer, K., Wood, E., Nosko, A., De Pasquale, D., Molema, S., & Christofides, E. (2015). Disclosure and Privacy Settings on Social Networking Sites: Evaluating an Instructional Intervention Designed to Promote Informed Information Sharing. In Standards and Standardization: Concepts, Methodologies, Tools, and Applications (pp. 287-306). IGI Global.

Averell, L., & Heathcote, A. (2011). The form of the forgetting curve and the fate of memories. Journal of Mathematical Psychology, 55(1), (pp. 25-35).

Babaguchi, N., Koshimizu, T., Umata, I., & Toriyama, T. (2009). Psychological study for designing privacy protected video surveillance system: PriSurv. In Protecting

Privacy in Video Surveillance (pp. 147–164). Springer London.

Baby, S. (2013). AHP modeling for multicriteria decision-making and to optimise strategies for protecting coastal landscape resources. International Journal of Innovation, Management and Technology, 4(2), (pp. 218).

Baltrušaitis, T., Robinson, P., & Morency, L. P. (2013). Constrained local neural fields for robust facial landmark detection in the wild. In Proceedings of the IEEE International Conference on Computer Vision (pp. 354–361).

Baltrušaitis, T., Robinson, P., & Morency, L. P. (2016). Openface: an open source facial behavior analysis toolkit. In IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 1-10).

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. Information Polity, 10(1, 2), (pp. 65-78).

Benitez, K., & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. Journal of the American Medical Informatics Association, 17(2), (pp. 169–177).

Bevilacqua, M., & Braglia, M. (2000). The analytic hierarchy process applied to maintenance strategy selection. Reliability Engineering & System Safety, 70(1), (pp. 71-83).

Beye, M., Jeckmans, A. J., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). Privacy in online social networks. In Computational Social Networks (pp. 87-113). Springer, London.

Bezzi, M. (2010). An information theoretic approach for privacy metrics. Transactions on Data Privacy, 3(3), (pp. 199–215).

Calvo, M. G., & Lang, P. J. (2005). Parafoveal semantic processing of emotional visual scenes. Journal of Experimental Psychology: Human Perception and Performance, 31(3), (pp. 502).

Campisi, P., Maiorana, E., & Neri, A. (2009). Privacy protection in social media networks a dream that can come true? 16th International Conference On Digital Signal Processing, (2006), (pp. 1–5).

Cheng, Y., Lu, J., & Yahagi, T. (2004). Car license plate recognition based on the

combination of principal components analysis and radial basis function networks. In 7th International Conference on Signal Processing. Proceedings. (Vol. 2, pp. 1455-1458). IEEE.

Clifton, C., Kantarcioğlu, M., Doan, A., Schadow, G., Vaidya, J., Elmagarmid, A., & Suciu, D. (2004). Privacy-preserving data integration and sharing. In the 9th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery (pp. 19). New York, New York, USA.

Commission, F. T. (2013). Facing facts: Best practices for common uses of facial recognition technologies. In Facial Recognition Technology: Best Practices, Future Uses and Privacy Concerns (pp. 1–27). Nova Science Publishers, Inc.

Davison, A. J. (2003). Real-time simultaneous localisation and mapping with a single camera. In IEEE International Conference on Computer Vision (pp. 1403). IEEE.

Delgado, J., & Llorente, S. (2016). Improving privacy in JPEG images. In IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-6). IEEE.

DeVries, W. T. (2003). Protecting Privacy in the Digital Age. Berkeley Technology Law Journal, 18(1), (pp. 283–311).

Domingo-Ferrer, J., & Soria-Comas, J. (2015). From t-closeness to differential privacy and vice versa in data anonymization. Knowledge-Based Systems, 74, (pp.151-158).

Duan, T. D., Du, T. H., Phuoc, T. V., & Hoang, N. V. (2005). Building an automatic vehicle license plate recognition system. In Proc. Int. Conf. Comput. Sci. RIVF (No. 1, pp. 59-63).

Dwork, C. (2006). Differential privacy. Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, (pp. 1–12).

Dwork, C. (2011). The promise of differential privacy: A tutorial on algorithmic techniques. In IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS) (pp. 1-2). IEEE.

Ebbinghaus, H. (1985). Remembering Ebbinghaus. Contemporary Psychology, 30(7), (pp. 519-523).

Emmons, C. J. (2016). Newton's Law of Cooling. Journal of Humanistic Mathematics, 6(1), (pp. 298-298).

Ergun, O. O. (2015). Privacy preserving face recognition in encrypted domain. In IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings (Vol. 2015–February, pp. 643–646).

Fanelli, G., Weise, T., Gall, J., & Gool, L. V. (2011). Real time head pose estimation from consumer depth cameras. In Joint Pattern Recognition Symposium (pp. 101-110). Springer, Berlin, Heidelberg.

Feriyanto, N., Saleh, C., Badri, H. M., Deros, B. M., & Pratama, Y. (2015). Implementation learning and forgetting curve to predict needs and decrease of labors performance after break. Jurnal Teknologi, 77(27), (pp. 135-140).

Fong, P. W., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for facebook-style social network systems. In European Symposium on Research in Computer Security (pp. 303-320). Springer, Berlin, Heidelberg.

Fouad, M. R., Elbassioni, K., & Bertino, E. (2014). A supermodularity-based differential privacy preserving algorithm for data anonymization. IEEE Transactions on Knowledge and Data Engineering, 26(7), (pp. 1591-1601).

Freudiger, J., Shokri, R., & Hubaux, J. P. (2011). Evaluating the privacy risk of location-based services. In International conference on financial cryptography and data security (pp. 31-46). Springer, Berlin, Heidelberg.

Geng, Q., & Viswanath, P. (2016). Optimal Noise Adding Mechanisms for Approximate Differential Privacy. IEEE Trans. Information Theory, 62(2), (pp. 952-969).

Goodfellow, I. J., Bulatov, Y., Ibarz, J., Arnoud, S., & Shet, V. (2013). Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks (pp. 1–13).

Grošelj, P., Stirn, L. Z., Ayrilmis, N., & Kuzman, M. K. (2015). Comparison of some aggregation techniques using group analytic hierarchy process. Expert Systems with Applications, 42(4), (pp. 2198-2204).

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic

society (pp. 71-80). ACM.

Gulzar, N., Abbasi, B., Wu, E., Ozbal, A., & Yan, W. Q. (2013). Surveillance privacy protection. In Intelligent Multimedia Surveillance (pp. 83-105). Springer, Berlin, Heidelberg.

Heiselet, B., Serre, T., Pontil, M., & Poggio, T. (2001). Component-based face detection. In Computer Vision and Pattern Recognition (Vol. 1, pp. I-I). IEEE.

Hong, J. I., Ng, J. D., Lederer, S., & Landay, J. A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques (pp. 91-100).

Houghton, D. J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. Journal of Technology in Human Services, 28(1-2), (pp. 74-94).

Hu, D., Chen, F., Wu, X., & Zhao, Z. (2017). A framework of privacy decision recommendation for image sharing in online social networks. In IEEE 1st International Conference on Data Science in Cyberspace (pp. 243–251).

Hu, Y. H. Y., Chen, L. C. L., Zhou, Y. Z. Y., & Zhang, H. Z. H. (2004). Estimating Face Pose by Facial Asymmetry and Geometry. In Automatic Face and Gesture Recognition (pp. 651–656).

Hui, L., Zhi, L., & Ahmad, W. (2018). Network (graph) data research in the coordinate system. Mathematical Foundations of Computing, 1(1), (pp. 1-10).

Hwang, Y. H. (2015). IOT security & privacy: threats and challenges. In Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security (pp. 1-1). ACM.

Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., & Ioannidis, S. (2015). Face/off: Preventing privacy leakage from photos in social networks. In the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 781–792).

Kahraman, F., Kurt, B., & Gökmen, M. (2003). License Plate Character Segmentation Based on the Gabor Transform and Vector Quantization. In A. Yazıcı & C. Şener (Eds.), ISCIS (pp. 381–388). Springer Berlin Heidelberg.

Kapadia, A., Henderson, T., Fielding, J. J., & Kotz, D. (2007). Virtual walls: Protecting digital privacy in pervasive environments. In International Conference on

Pervasive Computing (pp. 162-179). Springer, Berlin, Heidelberg.

Kazemi, V., & Sullivan, J. (2014). One millisecond face alignment with an ensemble of regression trees. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (pp. 1867–1874).

Kennedy, A., & Pynte, J. (2005). Parafoveal-on-foveal effects in normal reading. Vision Research, 45(2), (pp. 153–168).

Korobiichuk, I., Podchashinskiy, Y., Shapovalova, O., Shadura, V., Nowicki, M., & Szewczyk, R. (2016). Precision increase in automated digital image measurement systems of geometric values. In Advanced Mechatronics Solutions (pp. 335-340). Springer, Cham.

Lebanon, G., Scannapieco, M., Fouad, M. R., & Bertino, E. (2006). Beyond k-anonymity: A decision theoretic framework for assessing privacy risk. In International Conference on Privacy in Statistical Databases (pp. 217-232). Springer, Berlin, Heidelberg.

Lee, J., Wang, Y., & Kifer, D. (2015). Maximum likelihood postprocessing for differential privacy under consistency constraints. In the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 635-644). ACM.

Levi, G., & Hassner, T. (2015). Age and gender classification using convolutional neural networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 34-42).

Li, N., Qardaji, W., & Su, D. (2012). On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (pp. 32-33). ACM.

Li, Y., Vishwamitra, N., Hu, H., Knijnenburg, B. P., & Caine, K. (2017). Effectiveness and users' experience of face blurring as a privacy protection for sharing photos via online social networks. In Proceedings of the Human Factors and Ergonomics Society (pp. 803–807).

Liang, M., & Hu, X. (2015). Recurrent convolutional neural network for object recognition. In Proceedings of the IEEE Conference on Computer Vision and

Pattern Recognition (pp. 3367-3375).

Litt, E., & Hargittai, E. (2014). Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. Poetics, 42(1), (pp. 1–21).

Litt, E., Spottswood, E., Birnholtz, J., Hancock, J. T., Smith, M. E., & Reynolds, L. (2014). Awkward encounters of an other kind: collective self-presentation and face threat on facebook. In Proceedings of the 17th ACM conference on Computer Supported Cooperative Work & Social Computing (pp. 449-460). ACM.

Liu, G., Wang, L., Xu, S., Zhao, D., Yang, S., & Li, S. (2016). The adaptive privacy protection research based on video image. In Information Technology, Networking, Electronic and Automation Control Conference, IEEE (pp. 1074-1077). IEEE.

Liu, K., & Terzi, E. (2009). A framework for computing the privacy scores of users in online social networks. In IEEE International Conference on Data Mining, ICDM (pp. 288–297).

Lundy, L. (2007). 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. British educational research journal, 33(6), (pp. 927-942).

Mahbub, U., Sarkar, S., & Chellappa, R. (2018). Segment-based Methods for Facial Attribute Detection from Partial Faces. IEEE Transactions on Affective Computing, (1), (pp. 1-1).

Mashima, D., Serikova, A., Cheng, Y., & Chen, B. (2018). Towards quantitative evaluation of privacy protection schemes for electricity usage data sharing. ICT Express, 4(1), (pp. 35–41).

Mekovec, R., & Vrček, N. (2011). Factors that influence Internet users' privacy perception. In Information Technology Interfaces (ITI) (pp. 227-232). IEEE.

Meng, L., & Sun, Z. (2014). Face de-identification with perfect privacy protection. In Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1234-1239). IEEE.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit

and cost. Journal of the Association for Information Science and Technology, 66(4), (pp. 839-857).

Mohamadi, A. (2013) Civil liability arising from a breach of privacy by media Audio-Video, Journal of Applied Science and Agriculture, vol. 8, no. 4, (pp. 353-358).

Naghizade, E., Bailey, J., Kulik, L., & Tanin, E. (2017). Challenges of Differentially Private Release of Data Under an Open-world Assumption. In Proceedings of the 29th International Conference on Scientific and Statistical Database Management (p. 27). ACM.

Ngo Thanh, T., Nagahara, H., & Taniguchi, R. I. (2015). Shape and light directions from shading and polarization. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 2310-2318).

Nov, O., Naaman, M., & Ye, C. (2010). Analysis of participation in an online photo-sharing community: A multidimensional perspective. Journal of the American Society for Information Science and Technology, 61(3), (pp. 555–566).

Pallas, F., Ulbricht, M. R., Jaume-Palasí, L., & Höppner, U. (2014, April). Offlinetags: a novel privacy approach to online photo sharing. In CHI'14 Extended Abstracts on Human Factors in Computing Systems (pp. 2179-2184). ACM.

Pan, G., Lin, W., Wu, Z., & Yang, Y. (2002). Eye detection system based on SVM filter. In Electronic Imaging and Multimedia Technology III (Vol. 4925, pp. 326-332). International Society for Optics and Photonics.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, 82(4), (pp. 331-338).

Parisi, R., Di Claudio, E. D., Lucarelli, G., & Orlandi, G. (1998). Car plate recognition by neural networks and image processing. In IEEE International Symposium on Circuits and Systems (pp. 195-198). IEEE.

Pelánek, R. (2016). Applications of the Elo rating system in adaptive educational systems. Computers & Education, 98, (pp. 169-179).

Pensa, R. G., & Di Blasi, G. (2016). A semi-supervised approach to measuring user privacy in online social networks. In International Conference on Discovery Science (pp. 392-407). Springer, Cham.

Pergament, D., Aghasaryan, A., Ganascia, J.-G., & Betgé- Brezetz, S. (2011). FORPS: Friends-oriented reputation privacy score. In Proceedings of the First International Workshop on Security and Privacy Preserving in e-Societies (pp. 19–25). ACM.

Picazo-Sanchez, P., Pardo, R., & Schneider, G. (2017, May). Secure Photo Sharing in Social Networks. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 79-92). Springer.

Polishetty, R., Roopaei, M., & Rad, P. (2016). A next-generation secure cloud-based deep learning license plate recognition for smart cities. In Machine Learning and Applications (ICMLA) (pp. 286-293). IEEE.

Prasser, F., & Kohlmayer, F. (2015). Putting statistical disclosure control into practice: The ARX data anonymization tool. In Medical Data Privacy Handbook (pp. 111–148). Springer International Publishing.

Pun, C. M., Yuan, X. C., & Chen, C. P. (2011). Geometric invariant digital image watermarking scheme based on feature points detector and histogram distribution. In Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 166-172). IEEE.

Qin, Z., Weng, J., Cui, Y., & Ren, K. (2018). Privacy-Preserving Image Processing in the Cloud. IEEE Cloud Computing, 5(2), (pp. 48-57).

Ra, M. R., Govindan, R., & Ortega, A. (2013). P3: Toward Privacy-Preserving Photo Sharing. In NSDI (Vol. 13, pp. 515-528).

Rajpoot, Q. M., & Jensen, C. D. (2014). Security and privacy in video surveillance: Requirements and challenges. In IFIP International Information Security Conference (pp. 169-184). Springer, Berlin, Heidelberg.

Rubinstein, B. I., & Aldà, F. (2017). Pain-Free Random Differential Privacy with Sensitivity Sampling. In International Conference on Machine Learning (pp. 2950-2959).

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. International journal of services sciences, 1(1), (pp. 83-98).

Saaty, T. L. (2013). Analytic hierarchy process. In Encyclopedia of operations research and management science (pp. 52-64). Springer, Boston, MA.

Saeed, A., Al-Hamadi, A., & Ghoneim, A. (2015). Head Pose Estimation on Top of Haar-Like Face Detection: A Study Using the Kinect Sensor. Sensors, 15(9), (pp. 20945–20966).

Saglam, A., & Baykan, N. A. (2017). Effects of color spaces and distance norms on graph-based image segmentation. In 3rd International Conference on Frontiers of Signal Processing (ICFSP) (pp. 130-135).

Salgado, L., Menendez, J. M., Rendon, E., & Garcia, N. (1999). Automatic car plate detection and recognition through intelligent vision engineering. In Security Technology (pp. 71-76).

Sarathy, R., & Muralidhar, K. (2011). Evaluating laplace noise addition to satisfy differential privacy for numeric data. Transactions on Data Privacy, 4(1), (pp. 1–17).

Schönborn, S., Egger, B., Morel-Forster, A., & Vetter, T. (2017). Markov Chain Monte Carlo for Automated Face Image Analysis. International Journal of Computer Vision, 123(2), (pp. 160–183).

Schnetler, R., Steyn, H., & Van Staden, P. J. (2015). Characteristics of matrix structures, and their effects on project success. South African Journal of Industrial Engineering, 26(1), (pp. 11-26).

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823).

Sen, J. (2014). Security and privacy issues in cloud computing. In Architectures and protocols for secure information technology infrastructures (pp. 1-45). IGI Global.

Sen-ching, S. C., Paruchuri, J. K., & Nguyen, T. P. (2008). Managing privacy data in pervasive camera networks. ICIP (pp. 1676-1679).

Shi, J., Zhang, S., & Qiu, L. (2013). Credit scoring by feature-weighted support vector machines. Journal of Zhejiang University SCIENCE C, 14(3), (pp. 197–204).

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1310-1321). ACM.

Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012). Big data privacy issues in public social media. In Digital Ecosystems Technologies (DEST) (pp. 1-6).

Sondhi, G., & Sloane, A. (2007). Digital photo sharing and emotions in a ubiquitous smart home. In IFIP International Federation for Information Processing (Vol. 241, pp. 185–200).

Squicciarini, A. C., Lin, D., Sundareswaran, S., & Wede, J. (2015). Privacy policy inference of user-uploaded images on content sharing sites. IEEE Transactions on Knowledge and Data Engineering, 27(1), (pp. 193–206).

Squicciarini, A., Caragea, C., & Balakavi, R. (2017). Toward Automated Online Photo Privacy. ACM Transactions on the Web, 11(1), (pp. 1–29).

Srivastava, A., & Geethakumari, G. (2013). Measuring privacy leaks in online social networks. In Advances in Computing, Communications and Informatics (ICACCI) (pp. 2095-2100). IEEE.

Steger, A., & Timofte, R. (2017). Failure detection for facial landmark detectors. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10117 LNCS, pp. 361–376). Springer Verlag.

Such, J. M., & Criado, N. (2016). Resolving multi-party privacy conflicts in social media. IEEE Transactions on Knowledge and Data Engineering, 28(7), (pp. 1851-1863).

Sun, H., Luo, H., & Sun, Y. (2016). Privacy-Preserving Recoverable Photo Sharing in Mobile Social Network. In Mobile Ad-Hoc and Sensor Networks (MSN) (pp. 152-159). IEEE.

Taddicken, M. (2013). 13 privacy, surveillance, and self-disclosure in the social web. Internet and Surveillance: the challenges of Web 2.0 and social media, 16, (pp. 255-272).

Tierney, M., Spiro, I., Bregler, C., & Subramanian, L. (2013). Cryptagram: photo privacy for online social media. In Proceedings of the first ACM Conference on Online Social Networks (pp. 75-88). ACM.

Tong, L., Dai, F., Zhang, Y., Li, J., & Zhang, D. (2011). Compressive sensing based video scrambling for privacy protection. In Visual Communications and Image

Processing (VCIP) (pp. 1-4).

Valstar, M., Martinez, B., Binefa, X., & Pantic, M. (2010). Facial point detection using boosted regression and graph models. In IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 2729-2736).

Villani, S. (2001). Impact of media on children and adolescents: a 10-year review of the research. Journal of the American Academy of Child & Adolescent Psychiatry, 40(4), (pp. 392-401).

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. Journal of Broadcasting & Electronic Media, 56(4), (pp. 451-470).

Wagner, I. (2015). Genomic privacy metrics: a systematic comparison. In Security and Privacy Workshops (SPW) (pp. 50-59).

Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013). Privacy nudges for social media: an exploratory Facebook study. In Proceedings of the 22nd International Conference on World Wide Web (pp. 763-770). ACM.

Wang, J., Bacic, B., Yan, W. (2018) An effective method for plate number recognition. Multimedia Tools and Applications 77 (2), 1679-1692.

Wang, J., Yan, W. (2016) BP-Neural Network for Plate Number Recognition International Journal of Digital Crime and Forensics (IJDCF) 8 (3), 34-45

Wen, Y., Zhang, K., Li, Z., & Qiao, Y. (2016). A discriminative feature learning approach for deep face recognition. In Lecture Notes in Computer Science (Vol. 9911 LNCS, pp. 499–515). Springer Verlag.

Weng, L., Amsaleg, L., Morton, A., & Marchand-Maillet, S. (2015). A privacy-preserving framework for large-scale content-based information retrieval. IEEE Transactions on Information Forensics and Security, 10(1), (pp. 152–167).

Wicker, S. B. (2013). A Right to Surveillance-Free Cellular Access? Cellular Convergence and the Death of Privacy, (pp. 156-174).

Winkler, T., & Rinner, B. (2010). A systematic approach towards user-centric privacy and security for smart camera networks. In Proceedings of the Fourth ACM/IEEE International Conference on Distributed Smart Cameras (pp. 133-141). ACM.

Xi, D., Podolak, I. T., & Lee, S. W. (2002). Facial component extraction and face

recognition with support vector machines. In 5th IEEE International Conference on Automatic Face Gesture Recognition (pp. 83–88).

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, (pp. 195–204).

Xing, J., & Heeger, D. J. (2000). Center-surround interactions in foveal and peripheral vision. Vision Research, 40(22), (pp. 3065–3072).

Yan, T., Lu, Y., & Zhang, N. (2015). Privacy disclosure from wearable devices. In Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing (pp. 13-18). ACM.

Yan, W., Wu, X., Liu, F. (2018) Progressive Scrambling for Social Media IJDCF 10 (2), 56-73

Yan, W., & F. Liu (2015) Event analogy-based privacy preservation in visual surveillance, Pacific-Rim Symposium on Image and Video Technology (pp.357-368)

Yan, W. (2017). Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics. 2nd edn. Springer International Publishing AG, Switzerland (pp. 41-63).

Yang, Y., Zhang, Z., Miklau, G., Winslett, M., & Xiao, X. (2012,). Differential privacy in data publication and analysis. In Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data (pp. 601-606). ACM.

Yang, H., Soboroff, I., Xiong, L., Clarke, C. L., & Garfinkel, S. L. (2016). Privacy-preserving ir 2016: Differential privacy, search, and social media. In Proceedings of the 39th International ACM SIGIR Conference on Research and Development in Information Retrieval (pp. 1247-1248). ACM.

Yang, S., Luo, P., Loy, C. C., & Tang, X. (2017). Faceness-Net: Face Detection through Deep Facial Part Responses. IEEE Transactions on Pattern Analysis & Machine Intelligence, (1), (pp. 1-1).

Yu, J., Zhang, B., Kuang, Z., Lin, D., & Fan, J. (2017). IPrivacy: Image Privacy Protection by Identifying Sensitive Objects via Deep Multi-Task Learning. IEEE Transactions on Information Forensics and Security, 12(5), (pp. 1005–1016).

Yu, X., Chinomi, K., Koshimizu, T., Nitta, N., Ito, Y., & Babaguchi, N. (2008). Privacy protecting visual processing for secure video surveillance. In Proceedings - International Conference on Image Processing, ICIP (pp. 1672–1675).

Zhang, W., Cheung, S. C. S., & Chen, M. (2005). Hiding privacy information in video surveillance system. ICIP (Vol. 3, pp. II-868). IEEE.

Zhang, Z., Luo, P., Loy, C. C., & Tang, X. (2014). Facial landmark detection by deep multi-task learning. In European Conference on Computer Vision (pp. 94-108). Springer, Cham.

Zhong, H., Squicciarini, A., Miller, D., & Caragea, C. (2017). A Group-Based personalized model for image privacy classification and labelling. In International Joint Conference on Artificial Intelligence (pp. 3952–3958)

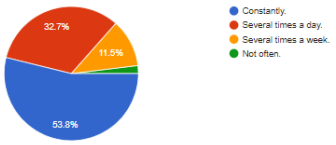
Zhou, B., & Pei, J. (2011). The *k*-anonymity and *l*-diversity approaches for privacy preservation in social networks against neighbourhood attacks. Knowledge and Information Systems, 28(1), (pp. 47-77).

Appendices

Appendix Ⅰ: Questionnaire of Privacy Concerns on Online Photo Sharing

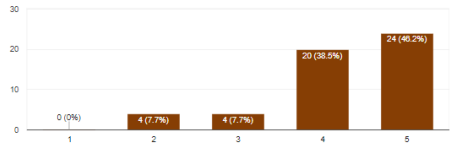
How often do you use social networking sites or apps?

52 responses



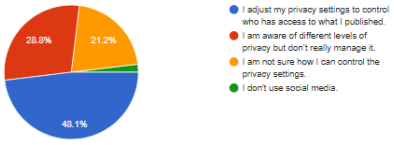
How concerned are you about how social networking use your information? (1 = not at all concerned - 5 extremely concerned)

52 responses



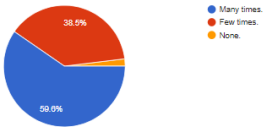
How do you control the privacy settings of your social media?

52 responses



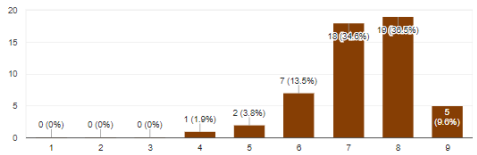
Have you regretted posting information like location, mode, relationship and group pictures about yourself?

52 responses



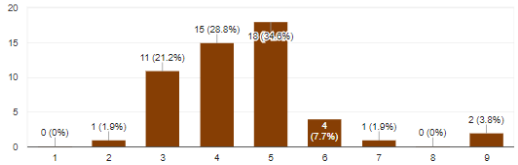
The factor accuracy is about whether an object can be accurately identified. What do you think the importance of the factor accuracy on revealing privacy?

52 responses



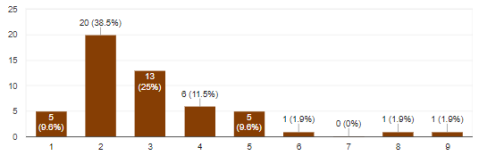
The factor angle means the detection angle. What do you think the importance of the factor angle?

52 responses



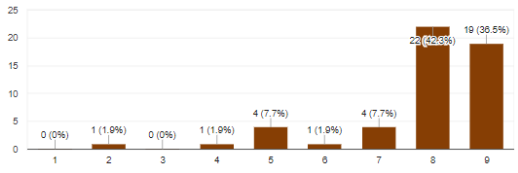
The factor ratio indicates the position and area ratio of an object. How do you score the importance of this factor which determines the level of privacy disclosure?

52 responses



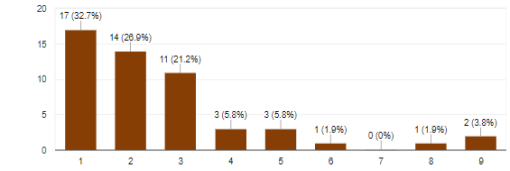
The factor sensitivity which represents whether the detected age is less than or equal to 17 or whether the car plate number is accurately recognized. What do you rate the importance of the factor sensitivity?

52 responses

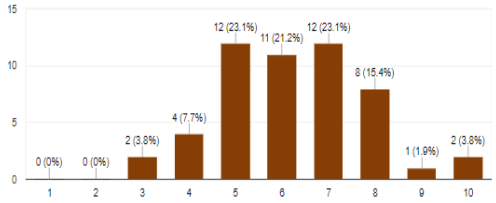


The length of time between the photo taken and publish will affect the level of privacy. What do you score the importance of factor timeliness?

52 responses

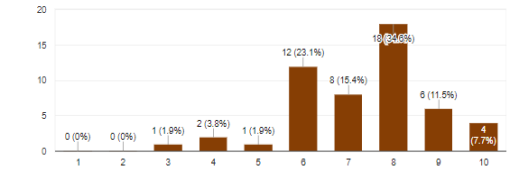


52 responses

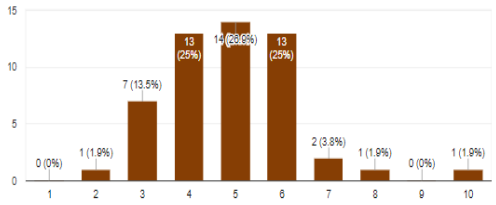


Please rate your concern on below social photos:

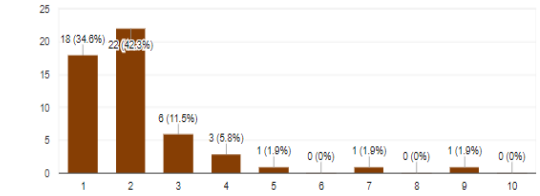
52 responses



52 responses

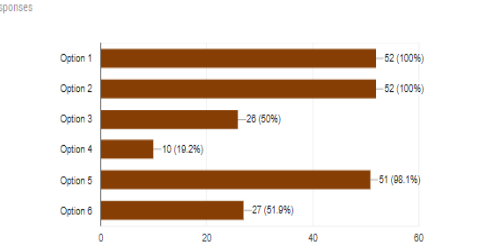


52 responses



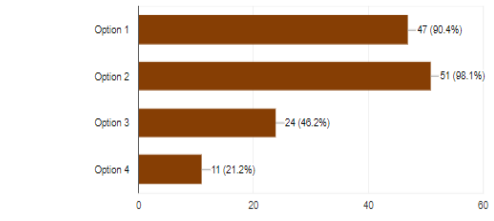
(Multiple choice) Which elements in the photo below do you think it's privacy?

52 responses



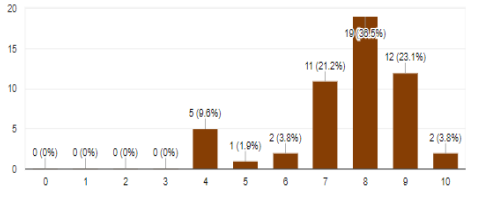
(Multiple choice) Which pictures below get your privacy concern about?

52 responses



On a scale 0 to 10, please rate your concern on the photo Below:

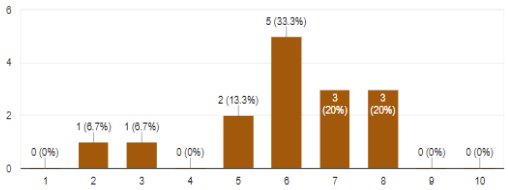
52 responses



Appendix II: Questionnaire of Evaluation of Image Privacy

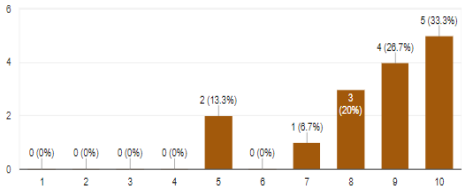
ID: 35936488

15 responses



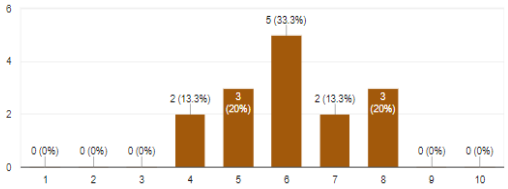
Boy

15 responses



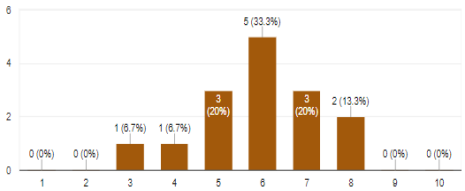
Adult

15 responses



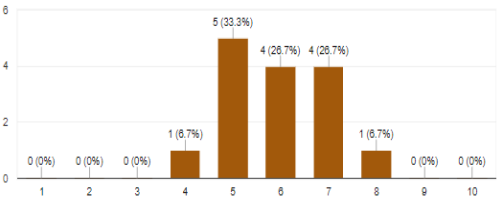
ID: 21913272

15 responses



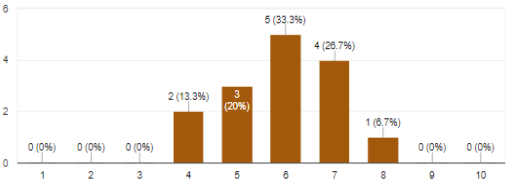
Car Plate

15 responses



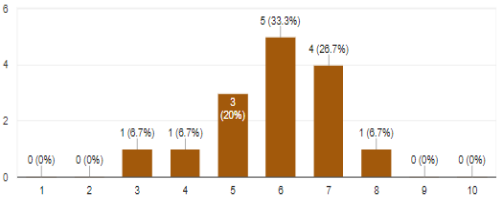
ID: 46005818

15 responses



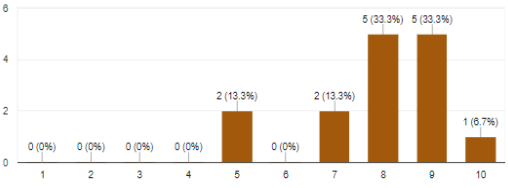
Senior

15 responses



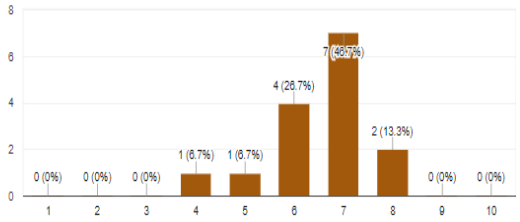
ID: 54206959

15 responses



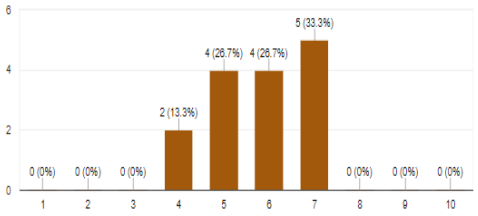
Lady

15 responses



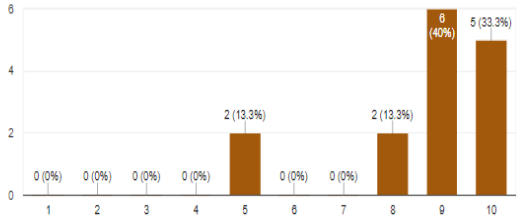
Gentleman

15 responses



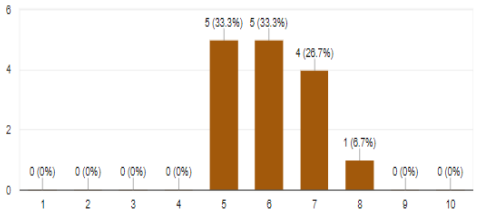
Baby

15 responses



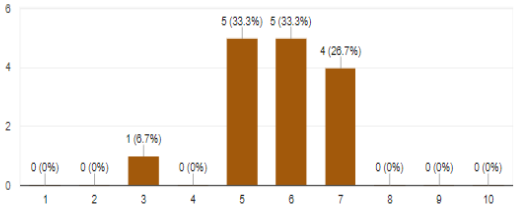
ID: 57819887

15 responses



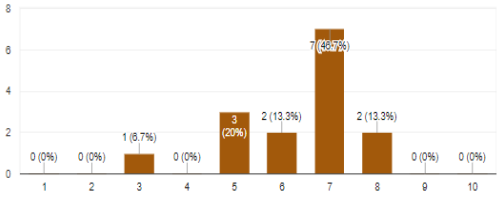
ID: 71801014

15 responses



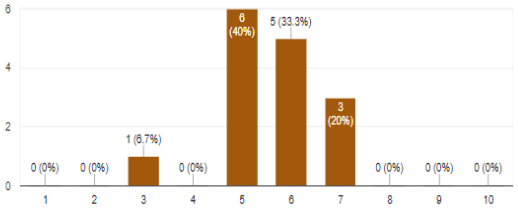
ID: 89254383

15 responses



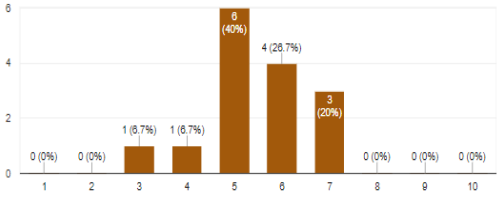
ID: 78637089

15 responses



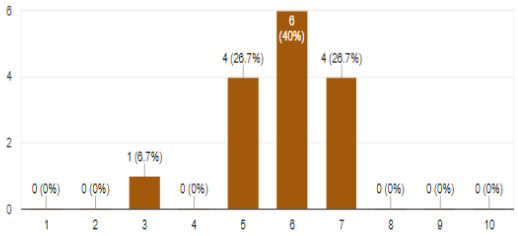
ID: 96801967

15 responses



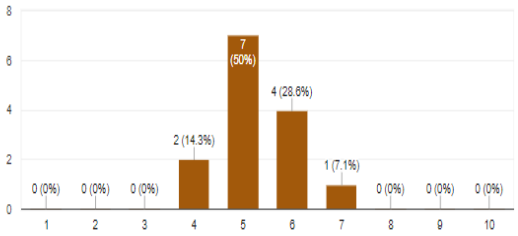
Gentleman

15 responses



Car Plate

14 responses



ID: 64876248

15 responses