Currency Security and Forensics: A Survey

J. Chambers, W. Yan, A. Garhwal, M. Kankanhalli,

e-mail: wyan@aut.ac.nz

Abstract—By its definition, the word ‘currency’ refers to an agreed medium for exchange, a nation’s currency is the formal medium enforced by the elected governing entity. Throughout history, issuers have faced one common threat: counterfeiting. Despite technological advancements, overcoming counterfeit production remains a distant future. Scientific determination of authenticity requires a deep understanding of the raw materials and manufacturing processes involved. This survey serves as a synthesis of the current literature to understand the technology and the mechanics involved in currency manufacture and security, whilst identifying gaps in the current literature. Ultimately, a robust currency is desired.

Keywords—currency forensics, currency security, banknote recognition, substrate analysis, ink analysis, counterfeit currency

I. INTRODUCTION

Throughout recorded history, as our society has evolved, we have relied on the ability to exchange goods and services with one another. The earliest known medium of exchange was the barter system, although this system still exists, ‘bartering’ has largely been superseded by formal mediums such as coins, banknotes, and more recently, electronic currency.

Traditionally, formal mediums of exchange, or ‘currency’ represents an agreed medium both enforced and controlled by the state, today consisting of uniform items holding value. The value held in currency exists purely by the faith entrusted in authenticity, a common challenge currency issuers have faced is securing the design against counterfeits.

In many nations, government owned central banks officially known as “reserve banks” manage the nation’s entire monetary policy. Amongst numerous other tasks, they are entrusted as the sole banknote and coin issuing authorities, assuming full responsibility for security and design, ultimately controlling the level in circulation at any point in time.

Today currency consists of a combination of coins, banknotes and electronic data, still counterfeiting remains a threat, made possible by continuous technological advances in reprographic equipment available to the general public. The stability of society arguably rests to some degrees, on the confidence we place on our currency, and this confidence level is directly related to security.

The challenges facing currency forensics are many, the effort required to detect counterfeit banknotes is directly correlated to the skill level of those producing the counterfeits, which shows no sign of stopping. Clearly, detection is not a trivial task, to forensically determine authenticity, one must possess a deep understanding of all features.

Reserve or central banks are relatively new, traditionally privately owned banks issued their own form of currency. After centuries of unpredictability and incompatibility between currencies and widespread counterfeit operations, central banks were formed to centralize currency issue and policy management. Such entities are given appropriate legal authority, this differs depending on the country in question.

A counterfeiters' primary objective is to produce passable reproductions, by mastering known security features. Security features are classified into one of three categories: 1) immediately detectable through human senses, 2) hidden from normal view of our senses, detectable using basic tools, such as a magnifying glass or Ultra Violet (UV) light, 3) intrinsic characteristics resulting from the manufacturing process and the interaction of raw materials.

Physical currency is subject to wear and tear, further complicating inspection this degradation is not uniform. For instance, ink may wear more rapidly on some areas on paper currency than on others, and notes in warmer climates are known to wear more rapidly than those in cooler climates. Counterfeiters have been seen to take advantage of this by purposely dirtying specific areas of banknotes, making distribution inconspicuous and detection more troublesome.

To minimize and control the circulation of counterfeit banknotes, Automatic Teller Machines (ATM) and central banknote sorting machines incorporate banknote recognition software. A combination of image processing, machine learning, and pattern recognition, this software is trained to check specific security features using learned threshold values. Threshold values serve as templates of known good values, a banknote which does not meet the specified threshold value is deemed to either be counterfeit or worn out, then removed from circulation.

Typically, banknote recognition software is programmed to check print quality, in the observed literature (http://www.rhondasoftware.com/software-solutions/computer-vision/100-usd-banknotes-recognition), quality is defined as fidelity of the captured image to an original or known good value. Although this approach considers the highly important print quality, it is interesting that the majority of features remain to be authenticated through manual inspection only. Counterfeiters are likely to near perform the art of certain security features, but are unlikely to perform all features. Reproduction of security features, difficult to replicate Intaglio print press and Offset Lithographic printing methods, and composed of closely guarded secret ink and substrate recipes.

A growing trend is towards the research and development of technologies such as embedding Radio Frequency Identification (RFID) devices adding further security into existing banknotes, and the paradigm shift towards an electronic currency. Similar to traditional mediums, electronic currency comes in many variations from that which is issued and backed by the state or issuing authority, mobile payment systems, and complete virtual currency existing within cyberspace communities.

The exact meaning of electronic money is somewhat abstract and subjective, electronic money consists of any electronic value which is exchangeable just like physical currency, such as banknotes and coins, but it is not consistent or uniform. This inconsistent are at times incompatible array of stored value and electronic payment systems are complicated to regulate.

The electronic currency paradigm currently lacks governance, and is apparent from the wide array of largely incompatible models in use today such as the e-Coin. Electronic currency, may be considered an electronic counterpart to the coin or banknote, as users are assured anonymity, currencies are issued using one-way hashing. This is in contrast to debit and credit cards, where transactions are reversible. This is currently an active area of research with real world implementations in use today. The strength of irreversible transactions fundamentally relies on the strength of the hashing method used, clearly the electronic paradigm presents a totally new set of governance and security concerns.

Counterfeit detection has traditionally been a task for law enforcement agencies [1,2,3], experts are trained through years of hands on experience similar to that of Questioned Document Examiners

(QDEs) (http://en.wikipedia.org/wiki/Questioned_document_examination). Scientific societies encourage research toward understanding the nature of documents. QDE is a specialized niché area within forensic science defining methods for analysis of such intrinsic document characteristics as handwriting, signature, printing, paper, and ink analysis.

A. Ideal Security Features

The following list summarizes the optimal security features currently securing banknotes against forgery, optimal in this case indicates that aspects are robust to fatigue and forgery.

1) *Substrate*

a) Complex substrate recipe
b) Windowed security thread
c) Security fibres
d) Watermark
e) See through windows

2) *Ink*

a) Complex ink recipe
b) Colour-shifting ink
c) Ultra violet ink

3) *Printing*

a) Serial number
b) Design complexity
c) Intaglio printing
d) Offset Lithographic Printing

B. *Attacks and Vulnerabilities of Currency*

There are three principal attacks on currency, namely: *duplication*, *imitation*, *mutilation*. The following describes the attacks in detail and how they relate to the security features listed in Section I-A.

1) *Duplication*

a) *Photographing*. By taking high resolution, high quality photographs of banknotes high quality replica banknotes can be reproduced through traditional darkroom photographic enlargement techniques. These are difficult to detect at first glance as colours are true to life, however the substrate has considerably different tactile qualities.

b) *Photocopying*. Photocopy is one of the major nuisances causing a fluctuation of counterfeit currency world-wide during the 1908s and 1990s. Photocopying is one of the more naïve approaches tempting only the casual counterfeiter, typically using standard office quality paper and inks are easily detected due to repeating serial numbers and uncharacteristic feel and colours tend to be dull compared to the genuine article.

c) *Scanning*. It is more troublesome than photocopying as counterfeiters can process images using Photoshop editing software (http://www.adobe.com/products/photoshop.html?promoid=JOLIW).

This allows for precision modification specifically of serial numbers making duplicates potentially difficult to detect depending on the print, ink and substrate fidelity.

2) *Imitation*

a) *Desktop publishing*. Tempting the casual or low funded counterfeiter, today's equipment is capable of producing high quality documents representing documents passable at the first glance. Although equipment is capable of producing high quality documents, the current ability cannot match the Intaglio and Offset Lithographic methods, ink tends not to be bold and fades much quicker. Under microscopic inspection, microtext and Guilloché patterns are not rendered with the required quality.

b) *Commercial publishing*. A higher precision is achieved on the intricate microtext and Guilloché patterns. Likewise the vibrancy and true to life fidelity of colours resulting from higher quality commercial grade, inks tend to allow for superior print and image fidelity over that of desktop publishing. Similarly, the substrate used is usually of higher quality even remarkably similar in, thickness, Grams per Square Meter (GSM) and fibre texture. Here the embedded security components such as watermarks, security fibres, and security threads are often overlooked as there is not such control over the substrate.

c) *Intaglio offset lithographic production*. Usually reserved for legitimate banknote manufacturers, or highly funded criminal organizations. By using identical methods to those that are required for creating legitimate banknotes, makes identification extremely troublesome. At this level, great care is usually taken to use both substrates and inks similar in composition to the genuine article. This is where uncharacteristic anomalies of the printing process observed on known legitimate print press machines should be used to determine authenticity. In addition, the embedded security components such as security fibres, threads and watermarks deviate when compared to the original.

3) *Mutilation*

a) *Ink removal*. There are various techniques of removing ink from using light amounts of acid and bleach, through to concentrated laser removal techniques. The purpose of removing ink is to covertly modify a note of a lower value to present as a higher value note whilst keeping the underlying authentic substrate.

b) *Precision cutting and joining with clear adhesive*. Banknotes can be cut into precise vertical strips to produce subsequent banknotes after several strips. Initially difficult to detect, under close inspections, image edges tend to be slightly disjointed deviating from the original image depending on the precision and amount of banknotes used.

II. CURRENCY SECURITY AND FORENSICS

To successfully distribute counterfeit currency, the end product must be inconspicuous achieved by thwarting security components. The level of success is determined by how close the product compares to the genuine article.

Forensic analysis therefore, must observe and measure predetermined intrinsic characteristics of known security components, specifically analyzing whether each security component deviates from known good values. Table I defines the three levels of security components that may be found in banknotes. Typically a threshold value defining known good values of image and colour fidelity is

used in security applications such as ATMs and banknote sorting machines to determine authenticity and fatigue.

The first level security is directed towards the human senses, typically sight and touch, but also sound, it is noteworthy that the majority of security components are found in this level. The second level security is approximately hidden from view of our senses without using basic equipment, such as a UV lamp or magnifying glass. The third level characteristics are reserved for QDEs or forensic examiners, such measures often are inherent characteristics resulting from the raw materials and printing processes used. The level at which a security component falls within determines the first point and thus complexity involved in determination, the level of confidence required may require further investigation depending on the quality of the note in question.

Table I. Level 1, 2, and 3 security feature classification in banknote design

Level 1	**Level 2**	**Level 3**
Substrate Fidelity	Microtext	Magnetic Ink
Print Fidelity	UV Glowing Ink	Screen Traps
Colour Fidelity		Manufacture Anomalies
Acoustic Fidelity		Materials Interaction
Serial Number		Complicated Patterns
Holograms		Complicated Design
Watermark		Fluorescence Eminence
Security Thread		Texture Analysis
Security Fiber		
Planchets		
Tactile Fidelity		
Color-shifting Ink		
Clear Window		
Matching Sides		
Latent Image		

A. Features

Printing, the application of colour, consists of three main components: *pigment*, *solvent*, and *drier*. Looking at the individual components, pigment controls the colour; solvent combines the pigment with the drying agent, which then binds pigment to the substrate. The two primary banknote printing methods, Intaglio press and Offset Lithography differ by the solvents' chemical composition used [4].

Intaglio press printing ink dries by evaporation, drying takes considerably longer than Offset Lithography. As the time is longer, the ink has more time to spread creating which is known as the feathering effect, where the edges appear to run. Offset Lithographic ink is oil based, drying is achieved by heating the substrate, chemical polymerization occurs giving a sharper line on edges, and a brighter overall result than Intaglio press printing. Forensic examination is achieved by discriminating print methods, scanning at a high resolution and zooming into the edges or by microscope to look for typical characteristics, clearly this method is subject to human error.

The ink ingredients typically differ from one currency to the next, ink needs to be both durable and difficult to copy. This requires top secret unique blends of raw materials, subsequently, each combination emits different levels of radiation. The US Secret Service over the last century has been building an ink library for forensic purposes [5], this library supports analysis by providing a reference point allowing for both discrimination of ink compositions, and estimation of age.

Spectrography requires a device used to separate incoming light waves reflected from matter into a frequency spectrum, light waves reflected from the ink can be characterized and analyzed. This opens up a whole new domain for the forensic analysis of banknotes, testing characteristics outside of what we can see through the Human Visual System (HVS).

Uniqueness can be programmed for security purposes, where currencies emit unique levels in the infrared and UV spectrum [6, 7], this has been investigated in a forensic setting using a spectrography microscope [8] for investigation of layer three security features.

Mössbauer spectroscopy is a nondestructive alternative method to determining the atomic composition of pigments [9]. It is found, the black ink on US banknotes is more stable than green, black has very stable structure that is high in iron whilst green is more erratic. Similarly a two photon microscope is used, an excitement method used to view photons emitted [10]. Their findings show that fluorescence aspects of genuine banknotes differ quite considerably in wavelength and amount of photons emitted than fake paper. Analysis is considered for inkjet inks by using Raman spectroscopy and laser desorption mass spectrometry techniques [11]. Colour inkjet ink discrimination is found to be more reliable than for inkjet documents printed by black only, this is due to manufacturers using different raw materials for colour inks but common black carbon in their black inks.

Raman spectroscopy failed to determine the difference between fake and genuine Euros inks as shown in [108] because similar colour spectra obtained for the fake and genuine euro banknote but one thing of Raman Spectra still utilised for fake banknote i.e. different areas of fake Euro banknotes for the same colour show similar spectra.

A promising non-destructive novel approach to automated determination of ink age is provided by using a Region Of Interest (ROI) [12]. The ROI is sampled across similar documents to determine loss in hue of both the RGB and HSV colour spaces, results are promising. Although not strictly focussed on banknote research, their method is applicable as banknotes use the same design within a series of currency. Fluorescent ink, invisible under normal conditions, viewable only under UV light, serves the second layer of security features. Tests confirm fluorescence only covers specific areas of the banknotes, other features such as microprinting and watermarks are difficult for machines to detect [13,14,15].

Fluorescent ink is not difficult for counterfeiters with sufficient motivation and finance, as seen in operation Bernhard WWII, over time and numerous experiments it has been shown that UV characteristics can be tweaked to create notes with similar levels.

An effect known as ‘colour-shifting’ made possible by using ‘colour-shifting ink’, ink literally changes colour as the viewing angle shifts. Used in Optical Variable Devices (OVDs) (http://www.csiropedia.csiro.au/display/CSIROpedia/Optically+Variable+Devices) such as holograms and Kinegrams [1], many currency issuers employ this technique. The Euro currency displays a colour-shift on the denomination numerals, bottom right hand side of the reverse. Recently Securency Australia has developed a new technology that uses this idea to mimic nature called Aurora (http://www.legalforce.com/aurora-79111433.html). Colour-shift ink is difficult to recreate, precise levels of shift are required for authentic currency. If a note is noticed to shift through the colour spectrum at an incorrect rate, it will be suspected as counterfeit.

Known to be used on US banknotes from the early 1960s, magnetic inks, originally intended for machine readable cheques consisting of dark pigmentation, limiting usage to colours like dark green, stone red, sienna brown and purple violet restricting design. The specific amount of magnetism

required is unique within a currency and denomination, methods for automated banknote detection and validation by detecting the level of emitted electromagnetism have been developed [15,16]. One fundamental drawback is that the level of magnetism is reduced by wear and tear, notes of the highly exchanged denominations, typically those of lower values will have a higher false error rate than those at the higher value end.

Thermochromic inks are temperature sensitive, designed to momentarily change colour when the substrate reaches a specific temperature range [6]. There is no research showing application of thermochromic inks on paper currency, primarily use has been limited to bank cheques and identity cards.

As the sophistication of security inks increase, the methods used to authenticate them must follow. Converting to grayscale allows for edge detection supporting discrimination of image fidelity. However as the array of colours used in printing paper currency increases, especially on polymer, removing colour from the analysis process potentially misses a wealth of information.

Images are converted to grayscale [17, 18, 19], new values are generated for each pixel, compressing the amount of data to be analyzed reducing complexity. New pixel values are generated from grayscale values using a linear transform function.

Conversion of the RGB channels to one single intensity channel, known as intensity thresholding above noise level [20], the remaining binary image is referred to as the mask. The RGB channel to grayscale is converted [21, 22]. These methods suffer from the fundamental problem that colours with similar luminance, differing in hue, such as white and yellow cannot be differentiated when converting to grayscale. This results in a loss of potentially meaningful data especially for currencies with colours are similar.

Obtaining grayscale histogram using the previous methods also omits necessary information regarding the dirty factor of banknotes [23, 24]. The HSV colour space is a truer measure of colour in printed documents than RGB when converting to grayscale, as it separates the intensity (luminance), and colour information chromacity [25,26]. The YIQ colour space is used, the Y or ‘luminance’ channel is used for analysis of colour characteristics through histogram comparison [27].

Pixel averaging does have its caveats [28], whilst removing noise, we may also lose some of the intrinsic print defects [29, 30, 31]. Print defects in currency are important during investigation when discriminating between individual printer. Each individual printer systematically prints with slight defects contributing to the definition of unique print signatures, even applicable to commercial grade print machinery such as Offset Lithographic and Intaglio press printers. Print signatures can potentially be used to uniquely identify individual printer, therefore pixel averaging must be implemented sparingly.

Printer and substrate ballistics, the study of how substrate surface, materials, and printing methods interacts [32]. Each print method has unique characteristics, analysis is used to discriminate between printing processes such as inkjet and laser. Intaglio print press and Offset Lithographic machines within the same class produce intrinsic anomalies linking individual machines to counterfeit notes.

Very few computer users have accessed to specialized printing equipment, such as Offset Lithography and Intaglio print press machines. Although inkjet printers have resolution capabilities that rival laser, inkjet are more sensitive to substrate quality, resulting in wider variation when

comparing the same characters at the microscopic level. Two types of ink exist for inkjet, those that are composed from pigments, and those from dye. Pigment inks tend to be more robust than dye. Under a microscope both should in theory show round pixels, in practice the shape tends to be uniform [4]. Between inkjet printers there are distinct variations in the nature of the same element printed, this is particularly noticeable in the random scatter of satellite droplets and hazy edges. Satellite scatter and edge roughness are calculated for printer signatures and profiles when narrowing the printer make and model producing questioned currency.

A geometric displacement is observed between Intaglio print press and Offset Lithographic print elements of authenticated € 10 notes [33]. Using a measure called, Maximally Stable Extremal Region (MSER), at point (*x*, *y*), measuring the displacement is possible by using specific pixels at Points of Interest (POI) as reference points. This raises the question whether the method can be used to forensically verify banknotes, clearly discriminating by the displacement alone is insufficient as there is a noticeable variation amongst authenticated genuine notes.

A print signature is extracted from the outer boundary of a text glyph, referred to as Model Based Signature Profile (MBSP) [34]. Individual documents are given a signature value calculated from the statistical anomalies produced in the printing process by equation (1):

$$p_i = \frac{\sum_j j w_j e_{ij}}{\sum_j w_j \mid e_{ij} \mid} \tag{1}$$

where e_{ij} is the strength of an edge corresponding to the digital derivative of the profile image for column j and w_j is a windowing function. Test results provide sufficient discrimination with probability values for false validation less than 2.3×10^{-8} and 10^{-9} for the letter ‘a’ and ‘s’ respectively. Clearly this is an extremely low probability, protection against false validation is imperative. The lager the false validation probability rate is, the higher the potential rate of counterfeits will slip through undetected.

MBSP and Shape Warp Coding (SWC) are combined for analysis of the interaction between substrate and printing process [35]. Inkjet, laser printed documents produce random flecks of stray toner on the substrate surface. Signatures can be calculated from the systematic characteristics of such anomalies, allowing investigators to potentially pinpoint a laser printer by make and model.

Printer signatures are calculated using the geometric distortion characteristics of printed documents [36, 37, 38]. Geometric distortion introduced by Electrophotography (EP) printers is mainly due to variations in the Organic Photoconductive (OPC) drum and polygon mirror, resulting in displacement between original and printed output. The dot centre of a satellite droplet of ink or fleck of toner is calculated, rotation compensation, geometric signature extraction, then correlation-measure of the halftone dots of the input to the printer [36]. A 2D distortion displacement vector is then calculated for each halftone dot.

Differing edges, satellite ink droplets, measuring the homogeneity and uniformity of ink or toner on printed substrate can be used as identifiers [39]. To measure this, they employ three specific measures:

1) *Perimeter based edge roughness*. A measure which calculates the roughness of a character to compare the perimeter difference of a banalized and smoothed image.

2) *Distance map based edge roughness*. A measure of the relation of edge pixels through distance mapping.

3) *Gray value distribution on printed area*. The differences obtained are in the uniformity of ink or toner coverage within printed regions, by using a thresholding technique uniformity can be determined.

Table II. A list of the representative work in the currency security features section

Characteristics	**Methods**	**The Work**
Colour	1. Ink library	[5]
	2. Thermo chromic inks	[6]
	3. Programming black inks to be visible in IR	[7]
	4. Discrimination of black printing inks based on composition	[8]
	5. Raman spectroscopy, LDMS and MALDI-MS [11]	[11]
	6. RGB to gray scale conversion	[17,18,19,21,13]
	7. RGB channels to one single intensity channel	[20]
	8. Gray level Histogram thresholding	[23]
	9. Luminance histogram from Y in the YIQ colour space	[27]
	10. Saturation weighted hue variance measurement using the HSV colour space	[25]
	11. Colour segmentation using the HSV colour space	[26]
	12. Authentication color feature based approach for determining ink age in printed documents	[12]
Fluorescence fidelity	13. UV pattern segmentation, signature	[14, 13]
	14. Mössbauer X-Ray fluorescence measurement	[9]
	15. Intrinsic fluorescence lifetime measurement	[10]
Image fidelity	16. Binarization, edge detection	[21]
	17. Axis symmetrical MASKS	[22]
	18. Statistical characteristics estimation from neighbour pixels	[24]
Serial number	19. Binarization (Otsu's Method), edge detection (Hough transform)	[17]
Print fidelity	20. Model based approach on text glyph profiles	[34]
	21. Interaction of substrate on printer signature [35]	[35]
	22. Geometric distortions based on printed halftone dots [36]	[36]
	23. Geometric distortions based on line width [37]	[37]
	24. Print signature based on fixed parts of document [38]	[38]
	25. Print method discrimination, texture and edge based features	[39]
	26. Print geometric distortions based on a per character basis	[40]
	27. Print offset measurements	[29,31]
	28. 3D signature of substrate surface *v.s.* print quality	[44]
	29. Tie points to measure displacement between offset and Intaglio	[33]
Security thread	30. Pulsed eddy current	[16]

Such evidence is a crucial step to any investigation regarding questioned currency, or any questioned document for that matter. Ruling out known methods of print by unique intrinsic satellite droplets and edge characteristics provides investigators with sound methods and resulting evidence subject to peer review.

Correlating contraband documents with exact individual printer by signature matching, is truly a step forward for forensics, concerning currency forensics and questioned document analysis. A specific printer can be identified and in some cases even the serial number of the specific printer, the fundamental question of where it was printed? In legal cases can be answered, further investigation is required to understand how the signatures change over time with respect to machinery wear and tear as geometric distortion is caused by physical internals of machinery, over time the machinery internals are subject to wear and tear potentially further distorting measurements observed.

Printer profiles are calculated for specific character set at differing levels of toner [40]. This method is dependent on the toner levels, degradation on the end print, and the particular time in question. The motivation is to determine whether manipulation of specific text values has occurred. Banknote serial numbers are likely to be modified as sequential or repeating serial numbers raise suspicion. This method is based on precise toner level measurement at any particular moment, new profiles have to be generated for differing toner levels. Such a method would be invaluable to define profiles with varying levels of toner.

The philosophy is to authenticate a banknote by detecting the characteristic minute bumps and grooves resulting from the Intaglio print press process. A novel algorithm is proposed for feature extraction based on incomplete shift invariant Wavelet Packet Transform (WPT) specifically for Intaglio [42].

One particular area that raises concern is the degradation of tactility, one of the key security features is the Intaglio print press tactile effect. It is found that the tactile effect degrades sharply, within a few weeks of circulation, special markings on the Hungarian notes to help the visually impaired identify notes are significantly reduced [43,44,45].

B. *Approaches, Methodologies, and Techniques*

1) *Security Components*

Paper is a fibrous matter, raw materials are combined in a large vat, mixed thoroughly adding binding agents, chemicals, and dyes resulting in a liquid-fibre pulp. The pulp is pressed through a rolling motion, flattening into thin precisely measured layers whilst squeezing out any remaining moisture, then finally setting in its final form. The substrate used for the manufacture of paper currency is known by the security printing industry as ‘security paper’. What sets security paper apart from regular paper is the secret, and unique recipe of raw materials, obscure physical dimensions, integrated security features such as watermarks, security threads, and security fibres.

Paper, at the microscopic level shows a fibrous texture of meshed plant fibres of varying lengths depending on the raw materials used. A standard paper is made predominantly from wood pulp, a security paper is made from plant material such as reeds, flax and cotton plants, the fibres are stronger, and visibly longer when viewed under a microscope [3].

Viewing a note under UV light, certain amounts of fluorescence become visible in specific areas creating a unique signature, this signature should be nearly identical across a currency. Through side by side comparison, one can identify forged security paper using this signature. Due to differing climates that raw materials grow and composition of soil UV characteristics can be greatly effected and thus the observed signatures contribute as evidence for questioned substrate.

Biaxially-oriented Polypropylene (BOPP) developed as a joint effort by the Reserve Bank of Australia (RBA), Commonwealth Scientific and Industrial Research Organization (CSIRO) and the University of Melbourne is the next generation of security substrate. Polymer currency looks and feels similar to paper currency. At its core is a thin clear plastic film covered by subsequent layers for added durability. The BOPP security substrate marketed by Securency (RBA and Inovia Films) is called guardian, is said to be more robust, and stay clean for longer than paper as it is non-fibrous and nonporous.

To the naked eye, the surface of BOPP appears and feels smooth to the touch. Under microscopic examination, the surface consists of a random scatter craters. Advocates for the use of BOPP security substrate claim a robustness surpassing the lifetime of traditional paper substrate, and security features not yet feasible with paper. In particular, the see through window feature Figure 1 which turns black when scanned or photocopied.

Fig.1. See through window on the New Zealand banknotes in the shape of a fern leaf, also on the corresponding side a see through window stating the denomination value having a unique raised tactile quality.

There is growing interest in the development of new security components for embedding through the manufacture and printing process. Research [46] shows, the scales of Lepidopetra and elytra of Coleoptera butterflies possess micro structures resulting in unique polarization effects. The scales create a unique complex texture with detail too minute for desktop publishing equipment to render and iridescence effect which could be applied to banknotes. However iridescent ink is available meaning basic passable counterfeit reproduction targeting layer one may be possible.

Paper surface texture can be fingerprinted similar to printer signatures, and identified using commodity scanners [47]. A surface is given a unique signature based on the natural imperfections occurring in the paper texture. The unique 3D qualities are calculated, it is extremely unlikely that two surfaces will present with identical 3D characteristics, however documents created from the same raw materials through the same manufacture process will show similarities. A one-way hash value can then be calculated and either stored in a database registered against the individual banknote serial number, or even printed on the document to provide added security.

Authenticating a document in this way is extremely robust in theory, especially through values stored in a database. However, printing on substrate is subject to fatigue and is more appropriately suited to security documents which are not handled often such as diplomas, certificates, land titles. Banknotes are handled often, crumpled and smudged constantly throughout their lifespan, such a

signature would change over time as banknotes wear. Therefore, any initial hash value will be irrelevant for application in banknotes even if stored on a database.

The majority of security paper manufacturers prefer the lower cost of paper over polymer. Although BOPP is initially expensive in comparison, it appears to be gaining in popularity, adopting countries have reported a decrease in long-term costs due to increased longevity. One of the world's largest security paper manufacturers has adopted polymer offering a polymer paper hybrid alternative.

Polymer is not immune to counterfeiting, and appears counterfeiter sophistication is on the rise. Clearly, as the sophistication of the counterfeiters rises, forensic analysis of the texture of BOPP must be analyzed similar to that of security paper, forensics could benefit from an understanding of BOPP surface signatures. This would build way for the development of recognition algorithms to authenticate the BOPP substrate using features other than image and colour fidelity.

Paper results from compression of many plant fibres. A common property of substrates is that there will always be some levels of transparency. Held up to a light source, the opposing side will blend through, manufacturers exploit this to their advantage embedding latent security components between layers. This also applies to polymer substrate, latent images or components are hidden from normal view.

Coloured fibres known as security fibres are woven into the layers scattered randomly throughout, whilst holding up a note to a light source individual fibres become visible, under UV light threads glow. Counterfeit notes began to turn up with imitation threads or fibres embedded, and even drawn on, these imitations are easily discovered by forensic analysis, however they are not obvious to the general public.

The security strip or thread is similar to the security fibre, generally a single thread is embedded between the layers of the note, typically a metallic thread sometimes incorporating micro-text on the strip, seen on the Bangladeshi Takka notes [48]. Windowed threads are a novel variation, more difficult to forge as threads are woven in and out of the note surface, typically in 10 mm stretches. Viewed normally it looks like a series of discontinuous metallic strips, held up to a light source the strip is revealed as a continuous thread. Typically counterfeit attempts are obvious. A commonly used method is to print or draw discontinuous thin lines in a metallic ink.

Planchets are minute disks measuring roughly one millimetre in diameter, are embedded throughout the banknote. When held up to a light source, the disks become visible similar to the watermark, security fibre, and windowed thread. Planchets take a number of forms from colourless disks which react to UV light only, or coloured disks which show through in normal light, for added security, planchets can incorporate micro-printing and micro-text.

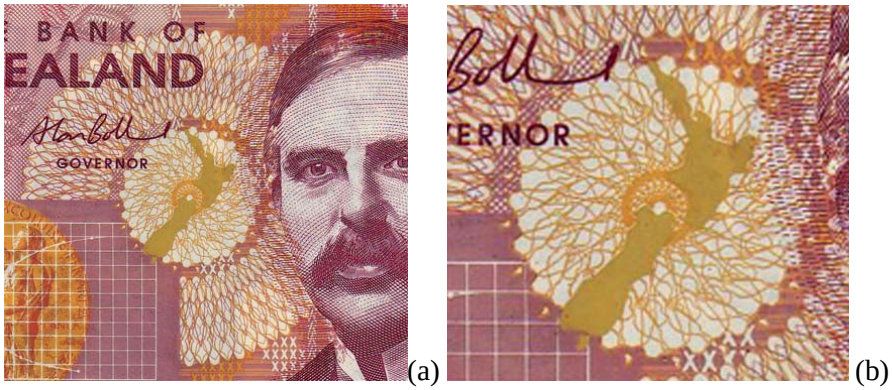
Moiré patterns come in many variations, such effects are created by an optical illusion, and are not there at all. These are hidden measures that only become apparent upon unauthorized reproduction, such measures are also aptly termed screen traps.

The effect is caused by the digitization of a genuine note, followed by an attempt to print from the digitized file. Benjamin Franklin, a printer by trade, was a pro-supporter of paper currency over precious metals, he intentionally misspelled the word 'Pennsylvania' to catch forgers who corrected the spelling. His next development showed more sophistication, an actual leaf was embedded in the printing process, resulting in unique intricate veins of the leaf, extremely difficult to replicate by

etching copper plates by hand which was the only method available at the time [2], this complexity of design has remained paper currencies' greatest security defence through to the present day.

Security patterns are intricate geometrical repeating designs at such a fine detail that traditionally made counterfeiting banknotes by hand extremely difficult, interestingly it still remains at the forefront of security exploiting the fact that current desktop publishing technologies available to the public are not capable of rendering images to the required intricate level of detail achieved by Intaglio and Offset Lithography [49] (http://www.indigoimage.com/count/print.html).

The Guilloché, a security pattern used originally on medieval armor and pottery, was first applied to paper currency by the National Bank of the Netherlands (AD 1814). The Guilloché has evolved from a simple repeating symmetrical design, through to elaborate spirographical designs. Guilloché is seen in Figure 2.



(a) (b)

Fig.2. (a) Guilloché can be found on the New Zealand banknotes just to the left of the portrait. (b) As the Guilloché is zoomed, it degrades gracefully maintaining detail, desktop grade publishing currently does not render this fine level of detail.

A latent image results from the Intaglio print process, this is achievable only under enormous pressure, and a fine raised ink pattern is rendered variable in contrast to the foreground. This is achieved by printing lines perpendicular to each other representing a foreground and background which varies by the viewing angle. There are limitations, latent images are only viewable under a certain angle, due to wear and tear the Intaglio print press tactile relief degrades.

Although latent images are near impossible for counterfeiters to reproduce without special purpose Intaglio print press machines, which sale and ownership are closely monitored by the authorities [3]. They are not robust security measures for high frequency use. Austria, Germany, Switzerland among others used latent images before the introduction of the Euro, it appears that this will not become a standard considering the inevitable wear and tear.

Vignettes are decorative, ornate, and intricate designs traditionally used as chapter or section separators in books, traditionally well suited to currency enhancing security. Vignette examples can be seen in most currency, noteworthy examples are shown on the Australian 1992 series $5 dollar notes, Australian polymer notes incorporate a vignette inside of the clear window, this shows that security components can be combined creating more complex obstacles for counterfeiters, though their use alone is questionable.

Certain scanners, copiers, and desktop publishing software will fail to reproduce documents where anti-copy marks are detected, known as screen traps. The idea is to thwart attack by image

recognition, when an image is captured, a series of checks for known forbidden images take place. If the software or device recognizes a forbidden security image, it will refuse to continue theoretically rendering unauthorized reproduction impossible. Whilst this is a sound idea, there are limitations, software or devices must have such measures embedded or the screen trap is ineffective.

The EURion constellation [50] found on Euro notes, consists of five circles in exact distance apart, size, proportion and colour. If a copier, scanner, or software that is designed to protect against documents displaying the EURion recognizes this pattern, it will stop and present the user with an according error message. Tests show that the constellation must be of exact measurements and colour properties, if the constellation varies by even the most minute variation, copying is possible [29, 50].

Screen traps may also consist of hidden information which upon copying alters the printed output, such as printing the word copy repeatedly across a page rendering it void [51]. Similar to the Moiré effect, this is a more robust measure relying on the common optical effects occurring in nature than on specific functions to be presented in software [51].

Certain laser printers have been found to systematically print yellow dots, making the device identifiable [52]. These yellow dots are hidden codes that allow for the determination of the make and model [53]. A similar method is presented for steganographic techniques in bicolour printed documents, by pseudo-randomly distributing tiny black dots [54], preliminary tests show that this method, in contrast to similar methods, can be applied to any bicolour document consisting of images, not only alphanumeric documents.

Security strength can be calculated to determine how effective a screen trap will be when implemented with thermal injet, dry electrophotographic and liquid electrophotographic printing [55, 56, 57]. The colour-tile, standard barcode, and 2D are investigated, colour-tiles prove to be an effective method for measuring colour fidelity. Such findings allow for discrimination of recent documents where ink has not been exposed to light for long duration of time, monotone methods such as standard and 2D barcodes therefore appear to be more robust.

Watermarks are specific areas of paper deliberately made thinner providing a higher level of transparency than the rest of the paper so that light passes through easier. Watermarks are embedded in one of two ways: the dandy roll method and the cylinder mould method. As pulp emerges from the vat, it is almost completely water, the water is pressed out compressing the fibres by placing a kind of wire stencil pressed against the pulp before it dries the impression remains.

This impression is what imprints the watermark, numerous attempts have been made to recreate watermarks. Even though the process of creating watermarks is practically as old as paper, forgery attempts have been highly unsuccessful. However, Art Williams, the master US counterfeiter, embedded a centre substrate layer with a hand drawn watermark between, when held up to a light source, a semi-passable imitation watermark appeared [1].

Improving the traditional watermark is a method called the Optical Variable Watermark (OVW), micro apertures are embedded directly in polymer substrate as a series of pulse width modulated pixels. The structure is divided into two channels, the individual pieces of artwork are interlaced with each row so that each second row is of a subsequent image.

When multiple layers are used, each layer embeds a secret payload using phase modulation. Super-positioning multiple layers, each having a specific carrier structure using the right combination is known as the ‘key’. When the key is positioned, the hidden information below is revealed in its plain

unencrypted form [58, 59]. This seems feasible for single, one-off, security documents such as diplomas and certificates, however where one key authenticates individual document, key management for banknotes would be cumbersome.

A novel approach has been developed where images are watermarked with a payload of data processed by Direct Spread Spectrum (DSS), then embedded data by using Peak Position Modulation (PPM) [60]. Most watermarking techniques embed data in one colour component, or independently in each colour component [61].

Minute text or micro-text is printed in inconspicuous areas, such text is often only visible through a magnifying glass, or microscope. Typical desktop publishing is unable to render text at such intricate detail similar to the Guilloché. Counterfeit attempts are detected when the text appears as a line, higher quality desktop equipment may be capable of rendering it, but as we magnify the area, edges begin to blur.

A serial number shown in Figure 3 uniquely identifies an individual banknote, and is stored in a database. Repetition of the same serial number will never occur on authentic currency, many counterfeit attempts have been detected by observing repeating serial numbers. The exact method for creating serial numbers differs from one country to the next.

Fig. 3. A unique identifier, the serial number is usually found repeated vertically on the left hand side and horizontally on the right hand side of both the front and back.

Clearly the serial number is a simple yet effective security measure. The serial number allows issuing authorities to monitor the circulation of currency. Typically ATMs and banknote sorting machines check this through character recognition techniques, comparing values stored in the database. The age of ink can be determined through various methods such as the secret service ink database, potentially enabling automated detection of counterfeit also using legitimate reproduced or copied serial numbers discriminating the ink age against the reported serial number age.

2) *Authenticating Security Components*

Additional security regarding paper currency is implemented through external authentication devices implemented in ATMs and automatic banknote sorting machines. Using banknote recognition software both minimizes, controls the flow of counterfeit and worn out banknotes for destruction. A brief discussion of such software follows whilst outlining three core functions image processing, feature extraction and classification.

After the image of a banknote has been captured, it must be pre-processed to have specific characteristics of interest singled out. First, the edges of the banknote image must be recognized and captured. Typically pre-processing an image of a banknote consists of a binarization stage, an edge detection stage and distortion correction.

A modified Canny edge detection is used [62] for removal of noise and background from captured images. The Canny algorithm marks a point as an edge if the amplitude is larger than its neighbours without checking that the differences are higher than expected. This results in the algorithm being sensitive to weak edges such as where the colours are similar or where there is blurring in the picture.

Traditional line fitting is insufficient for banknote recognition, as images contain false edge points [17]. Hough transform is used to detect edges of the paper, removing distortion borrowing from Optical Character Recognition (OCR) techniques. The Hough transform method is well suited to the detection of banknotes which have been in circulation, this is because of its ability to detect lines where there are gaps in the captured image.

Thresholding is an important technique for image segmentation. Thresholding allows applications to identify and extract a target from a background of a distribution of grayscale levels or texture in image objects. The correct threshold value is determined using adaptive thresholding [21]. This method shows robustness to strong illumination changes, this means that the end system is able to be used under different kinds of environments. The threshold value is critical to obtain the right data in the onset before carrying on through to the next phases.

The next stage is the extraction of specific features for which to determine the authenticity, this is directly related to the selection of specific security components. Much of the observed literature focuses on the extraction of specific ROIs for consideration of banknote colour, print and image fidelity. A captured banknote image is often sectioned into small areas, each input into a separate template matching processes [63]. A threshold is used for each subsection, contributing to a threshold ratio or T-ratio.

One of the known powerful tools for texture description is Local Binary Pattern (LBP) of a pixel p, by Ojala et al as shown in equation (2) [107].

$$LBP(p) = \sum_{i=0}^{7} 2^i s(g_i - g_p) \tag{2}$$

where g_p is the gray value of the centre pixel p, g_i is the gray value of i^{th} pixel in clockwise order around the 8-neighbourhood of pixel p, $i = 0,1,..,7$, and $s(\cdot)$ is the threshold function explained by equation (3).

$$s(t) = \begin{cases} 1, t \geq 0 \\ 0, otherwise \end{cases} \tag{3}$$

Methods based on LBP and BP network are used for paper currency in [64, 65], in [64] whole paper currency image segmented into $M \times N$ blocks, each block is subject to a Local Binary Pattern (LBP) method. Each pixel within the block is calculated and assigned LBP value on the basis of the pixel value each block histogram is made, to reduce the dimensions of the histogram, LBP values are quantised using equation (4).

$$LBP(p) = (\sum_{i=0}^{7} 2^i s(g_i - g_p)) / Q \quad (4)$$

where $Q \neq 0$ is a scale factor of quantization reducing the number of patterns in the resulting histogram to 32, which results in a grayscale histogram of 256 bins normalized to give uniform amounts across banknotes. Limiting to a total 256 values representing possible colours from a much wider array of possible colours, again it possibly looses vital information. Some currencies use a wide range of colours, this is especially vital when the colours used are close to each other in both location on the colour spectrum and physical location.

In [21], digital image processing approach concepts like eigen-face and Principle Component Analysis (PCA) is utilised to identify the U.S. banknote denomination for visually impaired people using smartphones.

A PCA functions for image feature extraction and compression. PCA [66, 67] is well suited for extracting characteristics from banknotes, as banknotes are high quality documents, much classification data is captured. When implementing smart detection devices into ATM and banknote sorting machines, time is a critical factor, as the PCA is used to determine the necessary features, we can be assured that only the necessary elements are being checked for.

Following extraction, the Kohonen based Self-Organizing Map (SOM) model is used to cluster data extracted into homogenous regions, where SOMs are used as a pre-preparation phase, the SOM forms a map corresponding to the data distribution so that regions of the map can be interpreted as clusters in the data space [67].

Speeded Up Robust Features (SURF), inspired by Scale Invariant Feature Transform (SIFT) is used. Feature selection to find an image of a banknote in any orientation is then possible using location of interest points [68, 69]. A banknote image is able to be recognized in various environments, orientations and distances from the camera, tests show a 100% accuracy level. This would be an attractive option when considering development of surveillance devices detecting fraudulent currency for instance Closed Circuit Television (CCTV) footage located in a convenience store.

ROI approach is using Discrete Wavelet Transform (DWT) for scaling and shifting with Packet Wavelet Analysis (PWA), and Maximum Overlap Algorithm (MOA) [70]. This approach is found to be suitable for extraction of characteristics where defects such as wrinkles and holes caused by wear and tear are particularly troublesome. In developing countries, notes are circulated for longer before being disposed, thus counterfeit notes in these circumstances are more likely to remain in circulation. Not only is it imperative to account for wrinkles and holes [71], as a joint effect including dust and old age discolouring the notes over time and the randomness [70].

Character recognition using masking, geometric masks are applied to specific areas of interest, the amount of pixels obtained determines the character. Using single masks is insufficient, Axis Symmetric Masks (ASM) improves the accuracy by using multiple geometric shapes to extract more data about the area [22].

The final stage, feature classification uses various machine learning and pattern recognition techniques. Known good values or learned templates are used for side by side comparison, the threshold learned through training on those characteristics previously determined. This approach

allows for dynamic understanding of the medium, rather than setting strict values which would tend to be too restrictive.

Artificial Neural Networks (ANN) is used in much of the literature. Genetic Algorithm (GA) is combined with Back-Propagation (BP) [15, 72, 73, 74]. In each case, an increase performance was observed over using ANN alone. Ensemble Neural Network (ENN), a finite collection of NNs are trained to perform an identical task, input vectors are applied simultaneously in all ensembles. To ensure diversity among the individual ENN networks, Negative Correlation Learning (NCL) is applied, it is observed that notes containing more noise are classified correctly at a higher rate compared to single NN [18, 19]. A Counter Propagation Network (CPN) is used for note classification by [67], it is found that CPN gives greater accuracy for banknote classification over BP. By using a Bi-directional Associative Memory (BAM) technique, it was observed a 96.08% recognition rate with the remaining uncategorizable due to wear and tear [75].

Support Vector Machines (SVM) appears to be widely used throughout the literature and promise a wide variety of applications such as banknote classification [76, 77, 78, 79, 80, 81]. SVM is successfully implemented to recognize serial numbers on banknotes [82], and used for detection of stains to determine worn out banknotes [81]. Results show classification accuracy comparable to that of ANN, however it is determined that using multiple kernel SVM can increase accuracy and overall performance [27].

Learning Vector Quantization (LVQ), implemented by [66, 83], LVQ is relatively inefficient when compared to similar algorithms. As observed [66], though PCA was used before classification, to increase reliability, this method still requires a subsequent clustering phase model the complexity of the classified data, decreasing overall performance.

AdaBoost machine learning algorithm was applied on the *N* most discriminating features [20], the ratio between red and blue intensity channels is measured for those areas. It is found that using the colour channels over grayscale level characteristic intensity channels provides a significant improvement on classification performance when applied on identical training sets.

Hidden Markov Models (HMM) with Gaussian methods was used [84], a comparative analysis study of HMM, SVM and ANN is performed [84]. HMM outperformed both SVM and ANN, test results show HMM 93.92%, ANN 92.8% and SVM 88.52% [84]. HMM looks to be an attractive option due to the higher classification accuracy, furthermore as HMM can learn feature sets overtime we can tune strictly for what we need to check for using sound discriminative features.

Clearly, the security printing industry is making continual technological advances for which not only forensics needs to catch up, so too do the devices in the public domain which authenticate our banknotes. Specific qualities such as polymer security substrate characteristics, security fibre, security thread and watermark authentication have not yet been explored.

C. *Protocols, Tools and Systems*

Various tools and systems have been developed to authenticate banknotes through analysis of specific security components. Much of which is focussed on detecting incorrect or duplicate serial numbers, and assessing image fidelity. Although much research has been carried out concerning new document security techniques, issuers still rely largely on checking these legacy components.

Table III. A list of the representative work in the currency security components section

Security Layer	**Features**	**Techniques**	**The work**
Layer 1	Security patterns	1. Concaved iridescent texture 2. Bilinear coons patch 3. EURion constellation 4. Anti-copy mark morphology screen coding HVS	[46] [49] [50] [51]
Layer 2	Information hiding Anti-copy mark	5. Optical watermarking 6. Semi-covert watermarking/information hiding using dots on bi-colour documents 7. 2D colour barcode security payload density measurement 8. (yellow dots) representing serial number of printer	[58,59] [54] [55, 56, 57] [52, 53]
Layer 3	Microtext Substrate	9. Character recognition 10. Fingerprinting paper texture	[48] [47]

The serial number uniquely identifies a specific banknote, in some currencies the make and model of machinery can be pinpointed. The Euro currency includes a prefix denoting the country of issue. Intaglio print press machinery manufacture sale is strictly monitored by authorities, such as Interpol and the US Secret Service, thus serial numbers allow forensic examiners to pinpoint the printer locality of authentic notes. A low cost microcontroller device is developed [85], this shows that devices dedicated for a specific authentication task can be independently developed and used where required. Clearly serial number recognition is an extremely important and useful tool for both banknote security and currency forensics applications.

A combined hardware and software approach is provided by [109] for distinguishing between the original and fake Euros banknotes, by capturing the image of banknote with a near infrared camera. This approach also provides us the denomination of the Euro.

Physical currency, such as banknotes will remain in high demand at least for the near future, however over recent decades, there has been a paradigm shift towards the use of electronic currency. Electronic currency adds a whole new dimension for currency security and forensics, encompassing many forms from debit cards, Electronic Cash (e-Cash), right through to virtual money.

Here a synthesis towards a unified understanding of the variations observed in the literature is conducted with an emphasis on both implications for currency security and forensics. It is interesting to observe a lack of governance over the wide array of somewhat obscure variations [86, 87, 88], which may be precisely why there is an increasing array of models which are not compatible with one another.

Architectures known as mobile Cash (m-Cash) allow users to securely withdraw physical cash from ATM machines, using capable phones equipped with compatible RFID tags, and participating ATMs which have RFID readers. This encompasses an architecture incorporating a set of secure protocols for which the user may choose to only withdraw paper money through the phone replacing the traditional Personal Identification Number (PIN) [89, 90].

Similarly mobile payment architectures are used where payments can be made directly from person to person, business to business, or person to business and vice versa [91]. There are a range of options

where the phone is either linked through a Subscriber Identity Module (SIM) card, to personal bank account, or to a temporary deposit account similar to a prepay system where the prepay credit is able to be exchanged for goods and services.

The level of access in the mobile payment model determines the level of risk involved. If the SIM card is linked to a users' personal bank account, the user is vulnerable to potentially higher losses than to temporary deposit accounts. The risks involved must be supported by sufficient security measures, a secure protocol is developed for person to person transactions through wireless networks using mobile devices [92], the primary concerns here regard the security of the public networks and the protocols facilitating the communication over these networks facilitated through encryption communication protocols.

Electronic cash or (e-Cash) system is closely related to physical paper currency, interestingly and contrary to what one might think, e-Cash can provide anonymity. An e-Cash scheme lets a user withdraw money from a bank and spend it anonymously, this is achieved through cryptography and one-way hashing functions. An endorsed e-Cash scheme is proposed [93], a user may offer cash for payments offering more than one instance of the same item of e-Cash. However the merchant may only accept and complete the transaction once a third-party endorses the e-Cash instance, such as an issuing entity or third party trusted authority eliminating the double spending problem.

Architectures for e-Cash have been shown whereby virtual currency is transferred and managed on a server. The currency lives within a holding location until the transaction is confirmed by the endorsement procedure, and then finally completed [94]. Once the transaction is confirmed through the endorsement procedure, the currency or funds are then transferred into the recipients account.

A blind signature gives users complete anonymity making use of cryptographic protocols, an e-Cash transaction architecture is proposed employing the RSA public key cryptography system [95, 96]. The transaction is hidden from third parties, however in preserving this anonymity, certain security is lost, such as potential information supporting the audit money laundering. A method is proposed where trust relationships exist as rings of trusted banks, only trusted third parties specifically banks within the same ring may be aware of the users transactions [97], anonymity is restricted within the realm of trusted third parties.

Well known websites and online communities such as iTunes, Facebook.com, and World Of Warcraft (WOW) offer schemes where physical currency can be used to buy virtual currency. This virtual currency exists within the realm that it was bought for, online games for instance allow users to trade and auction artifacts with one-another inside the virtual world, such as weapons in the case of WOW, buy applications and music with iTunes. One-way virtual currency and two-way have been compared recently, it was concluded that many operators are not obliged to provide two-way exchange and typically do not. It appears this is primarily as it will cause a loss in profit and incompatibility with physical currency, concluding that two-way exchanges benefit both operators and users in the long run [98].

A solution to this problem aptly termed Common Money (CONEY) has recently been proposed where virtual money is managed within local sovereignties [99]. Each region defines and maintains local virtual currency compatible and exchangeable with physical currency. The architecture shows that local currencies can be integrated so that local virtual currency and local physical currency are synonymous with one another. Personal accounts are linked providing mechanisms for transfer from virtual to physical inside ones' own borders managed by these local servers.

There are many concerns regarding electronic currency from both a security and a forensic perspective, traditional concerns such as cryptographic protocols to facilitate data transport is primary. The lack of governance in the electronic realm leaves many doors open for money launderers to exploit. Hiding an electronic trail obfuscating transaction details is clearly made possible by abusing the use of blind signatures and the many obscure incompatible entities providing virtual currency facilities.

A recent emerging field of research is that of hybrid electronic-physical currency, to date the focus has been on the integration of Radio Frequency Identification (RFID) devices with paper currency. Research shows that RFID devices for application to banknotes. This gives banknotes the ability to communicate signatures with authentication and merchant devices.

Specifically, RFID tags embedded with encoded spectral signatures in printable thin flexible substrate circuit have been proposed as a subsequent security component for banknotes [100]. The use of RFID for both tracking of notes by law enforcement and authentication by merchants has been demonstrated, to enhance security memory cells is added, whilst adopting challenge responses protocol to avoid possible eavesdroppers stealing an access-key [101].

A paper currency management system is proposed to facilitate the distribution of uniform size wads of banknotes. An Ultra High Frequency (UHF) dipole tag based antenna with a short stub and meander lines [102]. RFID management systems can be applied in the management of supply chain. Facilitating management of banknote distribution to local bank branches, cuts down the human error involved in recording track and trace details of in transit wads.

Table IV. A list of the representative work in the authentication security components section

Tasks	**Methods**	**The work**
Feature extraction	1. Canny edge detection	[62]
	2. Hough transform edge detection	[17]
	3. Adaptive thresholding, PCA	[21,66]
	4. SOM and PCA for extraction	[67]
	5. Dynamic template matching, adaptive strictness	[63]
	6. Block-LBP algorithm, characteristic extraction	[64]
	7. Back propagation neural network for orientation recognition	[65]
	8. Banknote deterioration energy dust and wrinkle factor Evaluation	[71]
Classification	9. LVQ for classification	[66]
	10. CPN for classification	[67]
	11. SURF for feature extraction	[68,69]
	12. Discrete wavelet transform, packet wavelet analysis, maximum overlap algorithm	[70]
	13. Genetic algorithm is combined with back-propagation	[72,15,73,74]
	14. Ensemble neural network	[18,19]
	15. Counter propagation network	[67]
	16. Bi-directional associative memory	[75]
	17. Support Vector Machines	[76,77,78,79, 80,81,82]
	18. Multiple Kernel Support Vector Machines	[27]
	19. Learning Vector Quantization	[83,66]
	20. Adaboost	[20]
	21. Hidden Markov Model	[84]

III. Trends

One could be forgiven for assuming that it is not going to be too long before electronic currency replaces paper currency [103]. On the contrary, physically exchangeable currency is here to stay, at least for the near future. This is due to a number of factors: (1) a sense of anonymity is felt in the transaction; (2) much of the world does not have sufficient infrastructure to facilitate a completely electronic currency; (3) a common feeling of distrust towards the exchange of electronic funds considering numerous reported breaches in the media of late and; (4) a sense of nationalism felt through iconography of the locally unique artwork on currency [104].

The current trend in physical paper based currency shows the use of paper will continue for the near future, perhaps because the majority of substrate manufacturers prefer the lower cost associated. Polymer banknotes, although initially more expensive appear to be gaining in popularity, countries such as Australia, New Zealand, Romania, Singapore and Vietnam among others have fully replaced paper. All such countries have reported a decrease in both the long-term costs associated with their longevity and lower rates of detected counterfeits than their predecessor.

Louisenthal one of the world's largest specialist security paper substrate manufacturers have adopted polymer to create a new hybrid-paper substrate. This integration shows that the added benefits of polymer are not only being realized by countries whom have adopted polymer in full but those who produce security paper, providing a secondary option to their customers.

Banknote security and counterfeit detection research is a growing area, developing software for smart devices integrated into ATMs and central banknote sorting machines. Despite most devices focus on the legacy components of serial number and print fidelity. Implementing security detection devices at ATMs, to control the flow of counterfeit currency through to central points for disposal is now common place. Although the available literature predominantly tends towards paper currency, there is a clear need for polymer research. It has been identified that polymer has its own unique surface characteristics; authentication of polymer surface characteristics would influence future research and development towards machines recognizing specific characteristics intrinsic to polymer.

Print signature or printer profile analysis is a promising move towards a secondary level of confidence for the forensic investigator, potentially allowing for document origination to be correlated with individual printers. It is shown in [34, 35, 36, 40, 78, 79, 105, 106], print anomalies can be detected and calculated to create a signature based on pixel distribution and satellite droplets. Similarly texture analysis of paper [41, 47] investigates various qualities of the texture and roughness of surfaces relating to documents and banknotes, similarly [42] investigates the texture of the ink pattern. Classifications of ink, paper and printing techniques are invaluable to both forensic investigation and security banknote recognition software.

Security features such as watermarks, security fibres, security threads, and security patterns appear to be some of the oldest yet most effective methods for thwarting counterfeit attempts. Crude attempts have been shown to at least thwart the first level of security defences, but appear to generally be detected through electronic analysis by the aforementioned ATMs and banknote sorting machines. To stay ahead of the curve, novel approaches are realizing real-world potential such as variations of the hologram specifically the Kinegram, moreover as cryptographic methods applied through RFID.

The paradigm shift towards use of electronic currency as a medium appears to be well on the way and definitely here to stay, similar to RFID electronic currency is made possible through cryptographic algorithms. Traditionally credit and debit cards have primarily been used. Over the last

decade, there has been an explosion in the variety of electronic currencies, such as virtual currencies for spending within online communities and mobile person to person, or person to business transactions. Much of this infrastructure remains widely incompatible with one another and lacking in governance. Proposals have been put forth suggesting the implementation of interoperable governed virtual currency systems.

To conclude this section, physical currency will be around for the near future, polymer banknotes offer advanced security features over paper substrate. Much of the research to date has focussed on developing devices to identify worn out and counterfeit notes ATM and central bank note sorting machines. The method of classification between worn out or counterfeit against an authentic note in good condition is the image fidelity. Research on texture analysis of paper and ink is showing signs of hope for pinpointing make and model of printer used.

Table V. A list of the representative work in the protocols, tools and system section

Paradigms	**Usages**	**The work**
Physical currency	1. Serial number micro-controller recognition device http://www.google.co.in/patents/US20110206265	[85]
Electronic currency	2. M-Cash, ATM withdrawal protocol http://www.gi-de.com/en/products_and_solutions/products/electronic_ payment/electronic-payment.jsp	[89,90]
	3. Mobile payment http://www.gi-de.com/en/products_and_solutions/solutions/mobile_money/mobile-money.jsp	[91]
	4. Endorsed e-Cash	[93, 95]
	5. RSA based e-Cash http://en.wikipedia.org/wiki/Ecash	[94]
	6. e-Cash with group signature	[96]
	7. Common money (CONEY)	[99]
RFID	8. RFID embedding	[100,101]
	9. RFID banknote bundle management http://www.fleur-de-coin.com/eurocoins/banknote-rfid	[102]

IV. Future Work

To date there is little research in the area of forensic science focusing strictly on currency when compared to other areas. Other areas of discipline were examined to build a foundation, we need understand the process of security printing, the ingredients and characteristics of substrates, inks and complexities of integrated security components.

Extensive research exists for applications of computer vision and machine learning in ATM or banknote sorting machines. Research in this area looks at the texture of the substrate surface, pixel distribution patterns, pigments in ink, fluorescence levels emitted from specific parts of the note and strict analysis of specific regions of interest such as watermarks and overall design.

Ultimately, a robust form of currency to both forgery and fatigue is desired, polymer the latest in banknote substrate. Even polymer is not immune to counterfeiting and appears that the level of sophistication is on the rise. As polymer is a new and emerging technology, it is absolutely critical that the field of forensics is equipped to identify forgery.

Analyzing how ink reacts to polymer may eventually enable for the determination of ink age on polymer substrates. Evidence to determine the date for the actual forgery, supposing the ink was

bought commercially, the raw material makeup of the ink should lead us to possibilities of determination of location to begin a trail to follow for investigation.

There are many aspects of physical currency yet to explore, the watermark, security threads, and fibres are some of the oldest, and simplest yet most effective techniques in securing documents. These methods are incredibly difficult to replicate, crude attempts have been seen, yet these are not checked in banknote authentication devices.

The governance of electronic currency systems is lacking and therefore needs to be reviewed. Proposals have been put forth suggesting models to integrate virtual currency and physical currency thus bridging the gap. Not only do systems need to be reviewed for integration models, the jurisdictional issues defining the rules and regulations within these systems collaborating with other systems need to be specified in consideration of this ubiquitous paradigm.

V. CONCLUSION

To conclude, this has been a survey of the current state of the art within the field of forensics dealing with currency security. A survey was necessary, as there is no known available research specifically dealing with counterfeit currency or electronic fraud from a forensic investigator. To fully appreciate this area, a look at where currency came from, and how it has evolved into what we have today. Currency has been around since ancient times and has taken many forms.

To detect flaws and analyze with any scientific merit, we need understand how currency is manufactured. We need also understand what it is made from, the raw materials, the unique components such as watermarks, security threads, and micro-text whilst considering how these interact with one another. Each of the numerous elements has their unique characteristics, these systematically become evident over the same series of currency.

Banknotes are produced from a painstakingly precise engineering process integrating beautiful artwork, and optical security components. The general public does not go out of their way to check for known security features, if it feels and looks good at first glance then it must be authentic. The previous point illustrates the first layer of the three layers of banknote security. Specifically the first layer is that which by the first glance and touch humans can identify. The second requires more in-depth investigation like with UV light, or magnifying glass. The third combines those features which require yet more in-depth investigation in a special purpose laboratory.

Traditionally, complexity of design was paper currency’s greatest defence, reproducing the artwork required a great deal of skill and talent. Today’s quality and complexity are still used as a major deterrence, intricate designs are still not possible on commonly available reprographic equipment. As technological advances continue to improve desktop publishing abilities, design may no longer be deterrence in itself and remain only for tradition sake.

Traditionally banknotes in question have been checked by specially trained Questioned Document Examiners (QDE), QDEs analyze such aspects as ink quality, print quality, substrate, and handwriting characteristics. The Secret Service was originally entrusted to fight the battle against counterfeiters of the US currency are still at the forefront of currency forensics.

Those who are successful at counterfeiting become that way through motivation and resources. It is interesting to see that not only do the security features of banknotes become more sophisticated, but

also do the skills and resources of counterfeiters. Automatic banknote sorting and authentication have been adopted by many banks worldwide embedded in ATMs and central banknote sorting machines.

Such devices check the colour quality and characteristics of the note, when the particular threshold has not been met, the note is deemed either counterfeit, or no longer fit for recirculation. Understandably, this is essential to protecting a country's economy. Counterfeiters may perfect perhaps one or more security components, however, it is only necessary to perfect as many as necessary pass them quickly and covertly. Therefore a more holistic approach is needed, although somewhat of a distant future, the idea is that authenticating all components known will build robustness into the currency system.

The banknote polymer substrate is gaining popularity, so much that the notable security paper manufacturer Louisenthal has adopted it offering a hybrid paper-polymer note. Yet research of polymer currency is almost nonexistent. Clearly, there is a need to develop methods for currency forensics moving towards specific automatic polymer banknote authentication devices, using the unique intrinsic characteristics of polymer.

Clearly electronic currency is the new medium for exchange, electronic currency due to its many varieties is somewhat difficult to define. Making it even more difficult to describe is the fact that the varieties are often incompatible with one another and even traditional currency, whilst lacking governance. Despite the convenience of electronic transactions, physical paper money as paper currency still provides benefits over electronic currency such as full anonymity of payment and a reducing more controlled form of currency.

REFERENCES

[1] J. Kersten, The Art of Making Money: The Story of a Master Counterfeiter. Penguin Group USA, 2010.

[2] B. Tarnoff, Moneymakers: The Wicked Lives and Surprising Adventures of Three Notorious Counterfeiters. The Penguin Press HC, USA, 2011.

[3] K. W. Bender, Moneymakers: The Secret World of Banknote Printing. Wiley-VCH, Weinheim, Germany, 2006.

[4] J. C. Russ, The Image Processing Handbook, fifth edit ed. Raleigh, USA: CRC Press, 2007.

[5] C. Neumann, R. Ramotowski, and T. Genessay, "Forensic examination of ink by high-performance thin layer chromatography - The United States Secret Service Digital Ink Library," Journal of Chromatography A, vol. 1218, no. 19, pp. 2793–2811, 2011.

[6] R. Kulˇcar, M. Friškovec, N. Hauptman, A. Vesel, and M. K. Gunde, "Colorimetric properties of reversible thermochromic printing inks," Dyes and Pigments, vol. 86, no. 3, pp. 271 – 277, 2010.

[7] V. Žiljak, K. Pap, and I. Žiljak, "CMYKIR security graphics separation in the infrared area," Infrared Physics and Technology, vol. 52, no. 2-3, pp. 62 – 69, 2009.

[8] A. Vila, N. Ferrer, and J. F. Garcia, "Chemical composition of contemporary black printing inks based on infrared spectroscopy: Basic information for the characterization and discrimination of artistic prints," in Analytica Chimica Acta, vol. 591, no. 1. Elsevier, 2007, pp. 97–105.

[9] V. Rusanov, K. Chakarova, H. Winkler, and A. X. Trautwein, “Mössbauer and X-ray fluorescence measurements of authentic and counterfeited banknote pigments,” Dyes and Pigments, vol. 81, no. 2, pp. 254–258, 2009.

[10] T. H. Chia and M. J. Levene, “Detection of counterfeit U.S. paper money using intrinsic fluorescence lifetime,” Optics Express, vol. 17, no. 24, pp. 22 054 – 22 061, 2009.

[11] L. Heudt, D. Debois, T. A. Zimmerman, L. KÈhler, F. Bano, F. Partouche, A.-S. Duwez, B. Gilbert, and E. D. Pauw, “Raman spectroscopy and laser desorption mass spectrometry for minimal destructive forensic analysis of black and color inkjet printed documents,” Forensic Science International, 2012. pp. 64-75.

[12] B. Halder and U. Garain, “Color Feature Based Approach for Determining Ink Age in Printed Documents,” in 20th International Conference on Pattern Recognition (ICPR’10), 2010, pp. 3212–3215.

[13] S.-H. Chae, J. K. Kim, and S. B. Pan, “A Study on the Korean Banknote Recognition Using RGB and UV Information,” in Communication and Networking, ser. Communications in Computer and Information Science, D. ´ Sl¸ezak, T.-h. Kim, A. C.-C. Chang, T. Vasilakos, M. Li, and K. Sakurai, Eds. Springer Berlin Heidelberg, 2009, vol. 56, pp. 477–484.

[14] K.H. Lee and T.H. Park, “Image segmentation of UV pattern for automatic paper-money inspection,” in 11th International Conference on Control Automation Robotics Vision (ICARCV’10), 2010, pp. 1175–1180.

[15] Z. Li, X. Zhou, and Y. Chen, “Research for the intelligent RMB sorter based on ANN,” in 9th International Conference on Electronic Measurement and Instruments (ICEMI ’09), 2009, pp. 1–103.

[16] S. Qian, X. Zuo, Y. He, G. Tian, and H. Zhang, “Detection technology to identify money based on pulsed eddy current technique,” in 17th International Conference on Automation and Computing (ICAC’11), 2011, pp. 230–233.

[17] L. Li, Y. Yu-tang, X. Yu, and P. Liang, “Serial Number Extracting and Recognizing Applied in Paper Currency Sorting System Based on RBF Network,” in International Conference on Computational Intelligence and Software Engineering (CiSE’10), 2010, pp. 1–4.

[18] K. K. Debnath, J. K. Ahdikary, and M. Shahjahan, “A currency recognition system using negatively correlated neural network ensemble,” in 12th International Conference on Computers and Information Technology (ICCIT ’09), 2009, pp. 367–372.

[19] K. K. Debnath, S. U. Ahmed, and M. Shahjahan, “A paper currency recognition system using negatively correlated neural network ensemble,” in 12th International Conference on Computers and Information Technology (ICCIT ’09), vol. 5, no. 6, 2010, pp. 367 –372.

[20] J.-M. Geusebroek, P. Markus, and P. Balke, “Learning banknote fitness for sorting,” in International Conference on Pattern Analysis and Intelligent Robotics (ICPAIR’11), vol. 1, 2011, pp. 41–46.

[21] F. Grijalva, J. C. Rodriguez, J. Larco, and L. Orozco, “Smartphone recognition of the U.S. banknotes’ denomination, for visually impaired people,” in IEEE ANDESCON 2010, 2010, pp. 1–6.

[22] N. Jahangir and A. R. Chowdhury, “Bangladeshi banknote recognition by neural network with axis symmetrical masks,” in 10th international conference on Computer and information technology (ICCIT’07). IEEE, 2007, pp. 1–5.

[23] K. He, S. Peng, and S. Li, “A Classification Method for the Dirty Factor of Banknotes Based on Neural Network with Sine Basis Functions,” in International Conference on Intelligent Computation Technology and Automation (ICICTA’08), vol. 1, 2008, pp. 159–162.

[24] H. Hassanpour and P. M. Farahabadi, “Using Hidden Markov Models for paper currency recognition,” Expert Systems with Applications, vol. 36, no. 6, pp. 105– 111, 2009.

[25] H. Dasari and C. Bhagvati, “Identification of Non-Black Inks Using HSV Colour Space,” in Ninth International Conference on Document Analysis and Recognition (ICDAR’07), vol. 1. IEEE, 2007, pp. 486–490.

[26] M. A. Morshidi, M. H. Marhaban, and A. Jantan, “Color segmentation using multi layer neural network and the HSV colour space,” in International Conference on Computer and Communication Engineering. ICCCE 2008. Washington, DC, USA: IEEE Computer Society, 2008, pp. 1335–1339.

[27] C.Y. Yeh, W.P. Su, and S.J. Lee, “Employing multiple-kernel support vector machines for counterfeit banknote recognition,” in IEEE Applied Soft Computing, vol. 11, no. 1, 2011, pp. 1439–1447.

[28] T. Pramoun and T. Amornraksa, “Improved image watermarking using pixel averaging and unbiased retrieval,” in 9th International Symposium on Communications and Information Technology (ISCIT’09), Washington D. C. USA, 2009, pp. 247–249.

[29] A. Verikas, J. Lundstram, M. Bacauskiene, and A. Gelzinis, “Advances in computational intelligence-based print quality assessment and control in offset colour printing,” Expert Systems with Applications, vol. 38, no. 10, pp. 13 441–13 447, 2011.

[30] P. Kumpulainen, M. Mettänen, M. Lauri, and H. Ihalainen, “Relating halftone dot quality to paper surface topography,” Neural Computing & Applications, vol. 20, no. 6, pp. 803–813, 2011.

[31] N. G. Shankar, N. Ravi, and Z. W. Zhong, “A real-time print-defect detection system for web offset printing,” Measurement, vol. 42, no. 5, pp. 645–652, 2009.

[32] P.-J. Chiang, N. Khanna, A. Mikkilineni, M. V. O. Segovia, S. Suh, J. Allebach, G. Chiu, and E. Delp, “Printer and scanner forensics,” Signal Processing Magazine, vol. 26, no. 2, pp. 72–83, 2009.

[33] R. Huber-Mörk, D. Heiss-Czedik, K. Mayer, H. Penz, and A. Vrabl, “Print process separation using interest regions,” in Proceedings of the 12th international conference on Computer analysis of images and patterns (CAIP’07). Berlin, Heidelberg: Springer-Verlag, 2007, pp. 514–521.

[34] S. B. Pollard, S. J. Simske, and G. B. Adams, “Model Based Print Signature Profile Extraction for Forensic Analysis of Individual Text Glyphs,” in Workshop on Information Forensics and Security (WIFS’10), 2010.

[35] G. Adams, S. Pollard, and S. Simske, “A study of the interaction of paper substrates on printed forensic imaging,” in Proceedings of the 11th ACM symposium on Document engineering (DocEng ’11), New York, USA, 2011, pp. 263–266.

[36] O. Bulan, J. Mao, and G. Sharma, “Geometric distortion signatures for printer identification,” in Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP’09), Washington D. C. USA, 2009, pp. 1401–1404.

[37] Y. Wu, X. Kong, X. You, and Y. Guo, “Printer forensics based on page document’s geometric distortion,” in IEEE International Conference on Image Processing (ICIP’09), Washington D.C. USA, 2009, pp. 2909–2912.

[38] J. van Beusekom and F. Shafait, “Distortion Measurement for Automatic Document Verification,” in International Conference on Document Analysis and Recognition (ICDAR’11), 2011, pp. 289–293.

[39] C. Schulze, M. Schreyer, A. Stahl, and T. M. Breuel, “Evaluation of Gray level-Features for Printing Technique Classification in High-Throughput Document Management Systems,” in Proceedings of the 2nd international workshop on Computational Forensics(IWCF ’08). Berlin, Heidelberg: Springer-Verlag, 2008, pp. 35–46.

[40] E. Kee and H. Farid, “Printer profiling for forensics and ballistics,” in Proceedings of the 10th ACM Workshop on Multimedia and Security (Sec’08), New York, NY, USA, 2008, pp. 3–10.

[41] J. Xie, C. Qin, T. Liu, Y. He, and M. Xu, “A new method to identify the authenticity of banknotes based On the texture roughness,” in IEEE International Conference on Robotics and Biomimetics (ROBIO’09), 2009, pp. 1268–1271.

[42] S. Glock, E. Gillich, J. Schaede, and V. Lohweg, “Feature Extraction Algorithm for Banknote Textures Based on Incomplete Shift Invariant Wavelet Packet Transform,” in Proceedings of the 31st DAGM Symposium on Pattern Recognition. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 422–431.

[43] Z. Solymar, A. Stubendek, M. Radvanyi, and K. Karacs, “Banknote recognition for visually impaired,” in 20th European Conference on Circuit Theory and Design (ECCTD’11), 2011, pp. 841–844.

[44] P. Kumpulainen, M. Mettänen, M. Lauri, and H. Ihalainen, “Relating halftone dot quality to paper surface topography,” in Engineering Applications of Neural Networks, ser. Communications in Computer and Information Science, D. Palmer-Brown, C. Draganova, E. Pimenidis, and H. Mouratidis, Eds. Springer Berlin Heidelberg, 2009, vol. 43, pp. 178–189.

[45] A. Burger, The devil’s workshop: a memoir of the Nazi counterfeiting operation. Frontline Books, Barnsley, South Yorkshire, England, 2009.

[46] S. Berthier, J. Boulenguez, and Z. Bálint, “Multiscaled polarization effects in Suneve coronata (Lepidoptera) and other insects: application to anti-counterfeiting of banknotes,” Applied Physics A: Materials Science and Processing, vol. 86, no. 1, pp. 123–130, 2007.

[47] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, “Fingerprinting Blank Paper Using Commodity Scanners,” in 30th IEEE Symposium on Security and Privacy, 2009, pp. 301–314.

[48] K. Yoshida, M. Kamruzzaman, F. A. Jewel, and R. F. Sajal, “Design and implementation of a machine vision based but low cost stand alone system for real time counterfeit Bangladeshi bank notes detection,” in 10th international conference on Computer and information technology (ICCIT’07), 2007, pp. 1–5.

[49] W. Qi, X. Li, and B. Yang, “Bilinear Coons Patch and its Application in Security Pattern Design,” in Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP’09), 2009, pp. 881–884.

[50] J. Nieves, I. Ruiz-Agundez, and P. G. Bringas, “Recognizing Banknote Patterns for Protecting Economic Transactions,” in IEEE Workshop on Database and Expert Systems Applications (DEXA’10), 2010, pp. 247–249.

[51] L.-l. Zhao, Z.-c. Gu, and Z.-l. Fang, “A morphology screen coding anticounterfeiting method based on visual characteristics,” Optoelectronics Letters, vol. 4, pp. 371–374, 2008,

[52] F. P. Beekhof, S. Voloshynovskiy, O. Koval, R. Villan, and E. Topak, “Document forensics based on steganographic anti-counterfeiting markings and mobile architectures,” in Proceedings of the 1st

international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics'08), 2008, pp. 1–5.

[53] J. van Beusekom, M. Schreyer, and T. Breuel, "Automatic counterfeit protection system code classification," in Proceedings of SPIE Media Forensics and Security XII. SPIE, 2010, pp. 1–8.

[54] H. Y. Kim and J. Mayer, "Data Hiding for Binary Documents Robust to Print-Scan, Photocopy and Geometric Distortions," in XX Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI'07), 2007, pp. 105–112.

[55] S. Simske, S. Aronoff, M. Sturgill, F. Collins, G. Golodetz, and R. Israel, "Security printing deterrents: A comparison of TIJ, DEP and LEP printing," in International Conference on Digital Printing Technologies and Digital Fabrication, vol. 23, 2007, pp. 543–548.

[56] S. J. Simske, J. S. Aronoff, M. M. Sturgill, and G. Golodetz, "Security Printing Deterrents: A Comparison of Thermal Ink Jet, Dry Electrophotographic, and Liquid Electrophotographic Printing," Journal of Imaging Science and Technology, vol. 52, no. 5, pp. 050 201–050 207, 2008.

[57] S. Simske, G. Adams, J. Aronoff, and M. Sturgill, "New findings in security printing and imaging," in 25th International Conference on Digital Printing Technologies and Digital Fabrication 2009 (NIP25), vol. 25, 2009, pp. 158–160.

[58] S. Huang and J. K. Wu, "Optical watermarking for printed document authentication," IEEE Transactions on Information Forensics and Security, vol. 2, no. 2, pp. 164–173, 2007.

[59] C. Hrishikesh and S. Shefali, "Printed Document Watermarking Using Phase Modulation," in 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET'09), 2009, pp. 222–227.

[60] J. Nah, J. Kim, and J. Kim, "A New Image Watermarking Using Peak Position Modulation for ID Photos," in 11th IEEE International Symposium on Multimedia (ISM '09), 2009, pp. 595–599.

[61] A. Trémeau and D. Muselet, "Recent Trends in Colour Image Watermarking," Journal of Imaging Science and Technology, vol. 53, no. 1, pp. 10 201 – 10 215, 2009.

[62] B. Singh, P. Badoni, and K. Verma, "Computer Vision based Currency Classification System," International Journal of Computer Applications, vol. 16, no. 4, pp. 34–38, 2011.

[63] K. Nishimura, "Banknote recognition based on continuous change in strictness of examination," in ICCAS-SICE. IEEE, 2009, pp. 5347–5350.

[64] J. Guo, Y. Zhao, and A. Cai, "A reliable method for paper currency recognition based on LBP," in 2nd IEEE International Conference on Network Infrastructure and Digital Content, Washington, DC, USA, 2010, pp. 359–363.

[65] Q. Wu, Y. Zhang, Z. Ma, Z. Wang, and B. Jin, "A Banknote Orientation Recognition Method with BP Network," in Proceedings of the 2009 WRI Global Congress on Intelligent Systems (GCIS '09), Washington, DC, USA, 2009, pp. 3–9.

[66] S. Omatu, M. Yoshioka, and Y. Kosaka, "Reliable Banknote Classification Using Neural Networks," in 3rd International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP '09), 2009, pp. 35–40.

[67] B. Sun and J. Li, "Recognition for the Banknotes Grade Based on CPN," in International Conference on Computer Science and Software Engineering, vol. 1, 2008, pp. 90–93.

[68] F. M. Hasanuzzaman, X. Yang, and Y. Tian, "Robust and effective component-based banknote recognition by SURF features," in 20th Annual Wireless and Optical Communications Conference (WOCC'11), 2011, pp. 1–6.

[69] F. M. Hasanuzzaman, X. Yang, and Y. Tian, "Robust and Effective Component-Based Banknote Recognition for the Blind," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, no. 99, pp. 1–10, 2012.

[70] F. Daraee and S. Mozaffari, "Eroded money notes recognition using wavelet transform," in 6th Iranian Machine Vision and Image Processing (MVIP'10), 2010, pp. 1 –5.

[71] Y. Jin, L. Song, X. Tang, and M. Du, "A hierarchical approach for banknote image processing using homogeneity and ffd model," IEEE Signal Processing Letters, vol. 15, pp. 425–428, 2008.

[72] L. Jing, L. Shuang, M.S. Jin, and W. Wei, "About RMB number identification with genetic evolution neural network," in International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE'10), vol. 1, Washington D.C. USA, 2010, pp. 286–288.

[73] B.Cao and J.Liu, "Currency recognition modelling research based on BP neural network improved by gene algorithm," in Proceedings of the Second International Conference on Computer Modelling and Simulation (ICCMS '10), Washington, DC, USA, 2010, pp. 246–250.

[74] W. Zhou, G. Xie, and B. Liu, "The application of mixed GA-BP algorithm on remote sensing image classification," in Geoinformatics 2008 and Joint Conference on GIS and Built Environment: Classification of Remote Sensing Images, L. Liu, X. Li, K. Liu, and X. Zhang, Eds., vol. 7147, no. 1. SPIE, 2008, doi 10.1117/12.813210.

[75] R. F. Sajal, M. Kamruzzaman, and F. A. Jewel, "A machine vision based automatic system for real time recognition and sorting of Bangladeshi bank notes," in 11th International Conference on Computer and Information Technology (ICCIT'08), 2008, pp. 533–535.

[76] T. Ishigaki and T. Higuchi, "Dynamic spectrum classification by divergence-based kernel machines and its application to the detection of worn-out banknotes," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'08). Washington, DC, USA: IEEE Computer Society, 2008, pp. 1873–1876.

[77] C. C. Chang, T. X. Yu, and H. Y. Yen, "Paper Currency Verification with Support Vector Machines," in Third International IEEE Conference on Signal-Image Technologies and Internet-Based System (SITIS '07), Washington, DC, USA, 2007, pp. 860 – 865.

[78] M. D. Gaubatz and S. J. Simske, "Printer-scanner identification via analysis of structured security deterrents," in First IEEE International Workshop on Information Forensics and Security (WIFS'09), 2009, pp.151-155.

[79] M. D. Gaubatz, S. J. Simske, and S. Gibson, "Distortion metrics for predicting authentication functionality of printed security deterrents," in 16th IEEE International Conference on Image Processing (ICIP'09), Washington, DC, USA, 2009, pp. 1489-1492.

[80] S.-J. Ryu, H.-Y. Lee, I.-W. Cho, and H.-K. Lee, "Document Forgery Detection with SVM Classifier and Image Quality Measures," in Proceedings of the 9th Pacific Rim Conference on Multimedia (PCM'08), Y.-M. R. Huang, C. Xu, K.-S. Cheng, J.-F. K. Yang, M. N. Swamy, S. Li, and J.-W. Ding, Eds., 2008, pp. 486-495.

[81] B. Sun and J. Li, "The Recognition of New and Old Banknotes Based on SVM," in Second International Symposium on Intelligent Information Technology Application (IITA '08), vol. 2, 2008, pp. 95–98.

[82] L. Wenhong, T. Wenjuan, C. Xiyan, and G. Zhen, “Application of support vector machine (SVM) on serial number identification of RMB,” in 8th World Congress on Intelligent Control and Automation (WCICA). Washington, DC, USA: IEEE Computer Society, 2010, pp. 6262–6266.

[83] H. Gou, X. Li, X. Li, and J. Yi, “A Reliable Classification Method for Paper Currency Based on LVQ Neural Network,” in Advances in Computer Science and Education Applications. Springer Berlin Heidelberg, 2011, vol. 202, pp. 243–247.

[84] G. Shan, L. Peng, L. Jiafeng, and T. Xianglong, “The design of HMM based banknote recognition system,” in IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS’09), vol. 4, 2009, pp. 106–110.

[85] Dayakshini and K. Sathisha, “Bank automation system for Indian currency- a novel approach,” in Recent Advances in Intelligent Computational Systems (RAICS’11), 2011, pp. 299–302.

[86] R. Dass and R. Muttukrishnan, “Security framework for addressing the issues of trust on mobile financial services,” in 7th International Conference on Next Generation Web Services Practices (NWeSP), 2011, pp. 99 –104.

[87] P. Tobbin, “Understanding mobile money ecosystem: Roles, structure and strategies,” in Tenth International Conference on Mobile Business (ICMB’11), 2011, pp. 185 –194.

[88] D.-X. Wang and J.-K. Teng, “Research and analysis of electronic cash payment system,” in International Conference on Educational and Information Technology (ICEIT’10), vol. 3, 2010, pp. V3–335 –V3–339.

[89] A. Arabo, “Secure cash withdrawal through mobile phone/device,” in International Conference on Computer and Communication Engineering (ICCCE 2008), vol. 1, 2008, pp. 818–822.

[90] D. Mirembe, J. Kizito, D. Tuheirwe, and H. Muyingi, “A model for electronic money transfer for low resourced environments: M-cash,” in Third International Conference on Broadband Communications, Information Technology Biomedical Applications, 2008, pp. 389 –393.

[91] D. Kumar, T. Gonsalves, A. Jhunjhunwala, and G. Raina, “Mobile payment architectures for india,” in National Conference on Communications (NCC’10), 2010, pp. 1 –5.

[92] Y. Zhu and J. Rice, “A lightweight architecture for secure two-party mobile payment,” in International Conference on Computational Science and Engineering (CSE ’09), vol. 2, 2009, pp. 326 –333.

[93] J. Camenisch, A. Lysyanskaya, and M. Meyerovich, “Endorsed e-Cash,” in IEEE Symposium on Security and Privacy (SP ’07), 2007, pp. 101–115.

[94] Y. Ling, Y. Xiang, and X. Wang, “RSA-based secure electronic cash payment system,” in IEEE International Conference on Industrial Engineering and Engineering Management, 2007, pp. 1898 – 1902.

[95] V. Das, “Protocol for anonymous e-cash for secure electronic commerce - initiation,” in Second International Conference on Future Information Technology and Management Engineering (FITME ’09), 2009, pp. 119 –123.

[96] J. Zhang, L. Ma, and Y. Wang, “Fair e-cash system without trustees for multiple banks,” in International Conference on Computational Intelligence and Security Workshops (CISW’07), 2007, pp. 585 –587.

[97] L. Wang, “A new multi-bank e-cash protocol with anonymity control,” in Fifth International Conference on Information Assurance and Security (IAS ’09), vol. 1, 2009, pp. 536 –539.

[98] H. Peng and L. Niu, “Two-way exchange of virtual currency: Future tendency and inherent risks,” in International Conference on Future Networks, 2009, pp. 220 –224.

[99] J. Guo and A. Chow, “Virtual money systems: A phenomenal analysis,” in 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and EServices, 2008, pp. 267 –272.

[100] S. Preradovic and N. Karmakar, “Design of fully printable chipless RFID tag on flexible substrate for secure banknote applications,” in 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication (ASID’09), 2009, pp. 206 –210.

[101] C.N. Yang, J.R. Chen, C.Y. Chiu, G.C. Wu, and C.C. Wu, “Enhancing privacy and security in RFID-enabled banknotes,” in IEEE International Symposium on Parallel and Distributed Processing with Applications, 2009, pp. 439 –444.

[102] T. Kim, U. Kim, G. Jung, and J. Choi, “Design of an UHF RFID tag antenna for paper money management system,” in Asia Pacific Microwave Conference (APMC’ 09), 2009, pp. 1056 –1059.

[103] Z. Hong, “The impact of e-money on the economy,” in WRI World Congress on Computer Science and Information Engineering, vol. 3, 2009, pp. 126 –130.

[104] J. Penrose, “Designing the nation. banknotes, banal nationalism and alternative conceptions of the state,” Political Geography, vol. 30, no. 8, 2011, pp. 429 – 440.

[105] D. H. Ahmed, H. J. Sung, and D.S. Kim, “Simulation of non-Newtonian ink transfer between two separating plates for gravure-offset printing,” in International Journal of Heat and Fluid Flow, vol. 32, no. 1, 2011, pp. 298–307.

[106] A. Roy, B.Halder, and U.Garain, “Authentication of currency notes through printing technique verification,” in Proceedings of the Seventh Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP ’10), New York, NY, USA, 2010, pp. 383–390.

[107] T. Ojala, M. Pietikäinen, and D. Harwood. “A comparative study of texture measures with classification based on feature distributions,” Pattern Recognition, vol. 29, no. 1, 1996, pp.51-59.

[108] A. Guedes, M.Algarra, A. C. Prieto, B. Valentim, V. Hortelano, S. Neto, R. Algarra and F. Noronha. “Raman Microspectroscopy of Genuine and Fake Euro Banknotes,” Spectroscopy Letters: An International Journal for Rapid Communication, 2013, pp. 569-576.

[109] A. Bruna , G. C. Guarnera and S. Battiato (2013). “Forgery Detection and Value Identification of Euro Banknotes.” Sensors 2013, vol. 2, pp. 2515-2529.