Digital Currency Forensics

JARRETT CHAMBERS

A thesis submitted to the graduate faculty of design and creative technologies
Auckland University of Technology
in partial fulfillment of the requirements for the degree
of
Master of Forensic Information Technology

2012

School of Computing and Mathematical Sciences

Abstract

The banknote manufacturing industry is shrouded in secrecy, the fundamental mechanics of security components are closely guarded trade secrets. Currency forensics is the application of systematic methods to determine authenticity of questioned currency. However, forensic analysis is a difficult task requiring specially trained examiners, the most important challenge is systematically and methodologically repeating the analysis process to reduce human error and time. In this thesis, an empirical approach for automated currency forensics is formulated and a prototype is developed. A two-part feature vector is defined comprised of colour features and texture features. Finally the note in question is classified by a Feedforward Neural Network (FNN) and a measurement of similarity between template and suspect note is output. Colorspace performance have been compared namely the: RGB, HSI, and Lab colorspaces. It is found that the combined average between the RGB channels known as the Intensity channel provides the highest discriminability, and is selected as the candidate colorspace.

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. Forensic science is the application of scientific methods to answer questions of a legal nature. Throughout history, issuers have faced one common threat, the threat of counterfeit. Despite technological advancements, overcoming counterfeit production remains a distant reality. Scientific determination of authenticity

requires a deep understanding of the raw materials, and manufacturing processes involved. This thesis 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, a robust currency is one which withstands security breaches, and is durable surpassing the lifetime of the current currency.

It has been identified that the current currency forensic investigation process is a manual ad-hoc process requiring specialist sought after questioned document examiners (QDEs), clearly this process is subject to human error. In a forensic setting, the analysis process must be systematic, methodological and repeatable. The digital currency forensics system addresses the issue of currency analysis by implementing a specific repeatable process through an automated examination using a combination of image processing, and classification techniques. This is achieved by implementing machine learning and pattern recognition.

Keywords: currency security, currency forensics, banknote recognition, banknote authentication, banknote classification

Contents

List of Tables

List of Figures

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: _____ Date: 09 November 2012

Acknowledgements

I would like to thank my parents and extended family for their incredible love and support throughout my entire academic life. The entire school of the AUT University has been extraordinary helpful in bringing this work to completion. I would like to thank in particular all teachers, supervisors and administration. Dr WeiQi Yan as a supervisor has both introduced me to the areas of image processing, artificial intelligence, its use in security and has inspired me to continue on through to Doctoral studies. I would also like to thank Dr Brian Cusack, Ms Ann Wu and Suzette Orquejo for their support an guidance throughout the Master of Forensic Information Technology program. Finally I would like to say thanks to my MFIT peers for their great help in the past two years.

Jarrett Chambers

Auckland

November 2012

Chapter 1

Introduction

1.1 BACKGROUND

Since the beginning of civilisation, societies have relied substantially on the ability to trade with one another, the ability to trade with one another is fundamental to the existence of our society as we know it. This ability to trade with one another is often a key enabling factor to an individual societies' strength to both survive and progress.

Trade has evolved from the elementary system of bartering to the complex combination of banknotes, coins, and electronic currency in use today. Interestingly what was once a system of trade facilitated by items of real intrinsic comparable value, has now evolved to a system where the primary medium for exchange holds no intrinsic value, yet value is exchanged.

Historically, coins were the preferred medium for exchange, due to their composition, consisting primarily of valuable precious metals, the trading parties involved would gain what could be seen as 'true value'. The use of precious metals as a common medium for exchange suffers from the fundamental problem of limit on supply (Bender, 2006; Kersten, 2009), whereas paper and electronic currency is

in abundance.

In an attempt to mitigate the shortage of precious metals, issuing authorities such as governing entities and banks issued promissory notes redeemable for actual precious metals stored in bank vaults. It was discovered with the issuance of promissory notes that the stocks held in vaults were seldom withdrawn in full, stocks held in vaults could be loaned out at interest generating a profit (Tarnoff, 2011). Promissory notes were easier to carry around than precious metals and therefore became the primary medium for exchange.

Promissory notes were troublesome, each issuing authority used a unique design, as issuing authorities consisted of banks a multitude of notes were in circulation at any moment. Fundamentally paper held no intrinsic value and it could be reproduced fraudulently without too much effort (Tarnoff, 2011), and widespread counterfeiting was a major problem.

The value held within promissory notes was not concrete, the reputation of the issuing bank for keeping their promise directly influenced the actual trading power held in each note. For an issuing authority to keep their promise, their stocks of precious metals must match the amount redeemable in circulation, widespread counterfeiting led to an inability to redeem promissory notes. Therefore the level of counterfeit notes in circulation of a specific issuing authority at any moment influenced their reputation and thus trading power.

1.2 MOTIVATION

Throughout history, currency issuers have faced one common threat, the threat of counterfeiting. Despite the introduction of electronic currency, banknotes remain in abundance. The amount of counterfeit currency in circulation at any moment threatens the confidence in the currency. Confidence influences the inherent value

and stability of the currency. Banknotes hold higher value than coins making them more susceptible to counterfeiting, and a higher economical risk. It is observed throughout history opponent societies have used counterfeit currency production of their enemies' currency as a weapon (Burger, 2009; Bender, 2006) in an attempt to weaken their opponents, reducing their financial bargaining power.

Today our currency system is composed of a complicated mix of coins, banknotes and electronic currency variants. Coins consist of a composition of raw materials, none of which are particularly valuable, functionally they are the same as banknotes. However coins hold lower denominations and are therefore a lower financial risk and target for counterfeiting. Paper currency holds higher denominations, and with the abundance of desktop publishing equipment available to the public this makes it a much higher risk for counterfeit reproduction.

Interestingly, although counterfeiting has been heavily reduced, even in today's environment counterfeiting of banknotes remains an issue and appears to be on the rise. Banknotes employ a wide array of security features, the design, composition of raw materials, combined with difficult to replicate printing methods such as Intaglio and offset lithographic methods add inherent security. The composition of raw materials is unique to a series of currency, whilst maintaining uniformity within the currency series to keep each unit as indistinguishable from the next as possible.

The printing methods employed require specialised equipment and are extremely difficult to replicate, even by master printers (Kersten, 2009). There are three print phases: offset lithography, Intaglio and letterpress, each printing method layers a different part of the design onto the banknote surface. Offset lithography is used to print the main background design typically consisting of the primary scene, patterns and variations in colour. A subsequent security feature applied by offset lithography, is precise alignment of the designs of the obverse and reverse for a seamless flow from front to back.

Immense pressure from two printing plates or rollers, creates a characteristic 3D effect resulting from minute bumps and grooves, and is extremely difficult to replicate. Although it is said the 3D effect wears out over time (Solymar, Stubendek, Radvanyi, & Karacs, 2011; García-Lamont, Cervantes, & López, 2012), it is assumed by issuing authorities that worn out banknotes will be destroyed, and new banknotes issued in their place. Apart from the minute bumps and grooves produced by Intaglio, the overlay scene or foreground and denomination value are applied to the surface. Finally, letterpress, a serial number uniquely identifying the individual note is literally pressed onto the banknote surface, typically this appears on the banknotes obverse both horizontally and vertically towards opposing edges.

The unique composition of raw materials used to develop security inks and security substrates is highly classified (García-Lamont et al., 2012). During operation Bernhard at the Sachsenhausen concentration camp near Berlin WWII, a major operation took place to counterfeit the British currency and use it as a weapon. Here the composition of raw materials was discovered for successfully reproducing counterfeit British pounds worth billions (Burger, 2009). It was discovered the raw materials used for the substrate was from a reed found in Asia, a laborious process took place where it was discovered the unique climate in which the substrate grows alters the end result, however these banknotes went undetected even by the bank of England at the time.

An abundance of unique security components are added to banknote design to serve as further barriers against counterfeit attempts shown in table Table 1.1. Each security component is detected either by: level 1 immediate human senses, level 2 minor manipulation, or level 3 major forensic analysis.

Traditionally, counterfeiters required impeccable artistic skill to reproduce passable fraudulent banknotes. Today it is possible to reproduce passable copies using publicly available desktop and commercial reprographic equipment, this has made

Table 1.1: Level 1, 2, and 3 security feature classification in banknote design.

Level 1	**Level 2**	**Level 3**
Substrate Fidelity	Micro-text	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 Fibre		
Planchets		
Tactile Fidelity		
Colour-shifting Ink		
Clear Window		
Matching Sides		
Latent Image		

it possible for the general public to produce copies. The continual technological advancements available to both the security printing industry, and the public has fuelled an on-going arms race.

Currency forensics is the application of systematic methods to determine authenticity of questioned currency. Questioned currency is one which is suspected to have been produced fraudulently. To determine the authenticity of questioned currency, banknotes are individually inspected for fidelity of specific characteristic features shown in table Table 1.1.

Ultimately the final decision is made by performing a side-by-side comparison between a known good template and the suspect note, when a note is found to fall below satisfactory requirements it is not authentic. Clearly, making a final decision is subjective, the complexity involved in investigating each component directly relates to the quality of the banknote being examined.

As much of the necessary information required to determine authenticity of banknotes remains secret, forensic analysis often requires specialist trained individuals. Clearly, analysis is therefore reliant on the availability of highly sought after individuals. Such analysis is an ad-hoc process and subject to human error, to our knowledge there is no existing systematic formulated approach to ensure consistency. Similarly, to our knowledge there is no research to suggest the availability of an automated system to determine authenticity.

It is a fundamental requirement that forensic analysis be performed systematically to produce consistent results, if this fundamental requirement is not met, any such evidence may be questionable. Hence, it is imperative for legal proceedings that developed forensic analysis processes produce consistent, accurate, and verifiable results.

Therefore, the primary motivation for this study is to explore the security of banknotes, and formulate forensic analysis methods from a purely computational

perspective for counterfeit banknote identification. As the security printing industry is very secretive, the fundamental mechanics enhancing security remain largely as closely guarded trade secrets. By developing a system to computationally analyse questioned currency the human error component can be minimised or reduced. Subsequently, computational analysis of banknotes leans towards a more systematic approach, whereby the analysis approach remains the same from one investigation to the next. By automating the analysis process, results are not only consistent across investigations, they are verifiable through understanding of the algorithms used.

In this thesis, banknotes are taken into consideration, the contribution provided by this thesis, is an empirical approach to automation of the currency forensics analysis process. A method for verifying the level of authenticity of banknotes is formulated based on the image and colour fidelity of questioned banknotes. Banknotes are primarily a visual medium, typically characterised by their visual appearance consisting of intricate patterns, scenes, and combinations of colour. Subsequently, as such methods result in a unique end result, the image and colour fidelity of captured banknotes is suitable as the primary basis for analysis.

Any image can be characterised by two characteristics: colour fidelity specifies how similar two images are in colour, and texture fidelity characterises an image by the distribution of observed colour throughout the image. Texture and colour features when used individually may only partially describe an image, but when combined creates suitable characteristics to computationally describe an image or a scene (García-Lamont et al., 2012).

A model is formulated to computationally describe and compare captured banknote images, computationally, colour at each picture element (pixel) is represented by three components red, green and blue (RGB). Using grey-world algorithm each pixel is averaged to a single grey-level value describing the colour intensity, thus

reducing data complexity whilst maintaining suitable information to differentiate colour. The important information for analysis of colour is the frequency of specific values, banknotes of a specific denomination result in a histogram with similar shape and distribution. A grey-level histogram is computed where six shape descriptors are calculated to describe the shape.

Texture is primarily descriptive of how often pixels of specific colour values appear next to pixels of other pixel colours in the picture or scene. In this case, a matrix is formulated to record frequencies of colour in appearance to pixels of other colours, various descriptors can be calculated to describe the tonal differences and contrast in the image. In this model the entropy value and GLCM (grey-level co-occurrence matrix) is used.

A two-part feature vector firstly comprised of grey-level histogram shape descriptors: central moment, mean, skew, variance, standard deviation and kurtosis. The second part comprises the texture descriptors: entropy level and GLCM (grey-level co-occurrence matrix) features: contrast, correlation, energy and homogeneity. The feature vector is classified by a Feedforward Neural Network (FNN), finally a side-by-side comparison is made accompanied by a similarity measurement.

1.3 THESIS STRUCTURE

The thesis is organised as follows: section 2 describes current research related to the area of currency forensics. The contribution provided by this thesis of an empirical approach for currency forensics, is introduced in section 3. Section 4 describes the results of the research and development for the digital currency forensics system supported by results obtained from experimental analysis testing hypotheses. Section 5 evaluates the effectiveness of methods used during this project and reflects

on the results obtained through experimental phases. Final section 6 concludes the paper by summarising findings and providing an indication for intended future research directions.

Chapter 2

Literature review

Supporting literature exists focusing on banknote recognition software intended for a variety of applications, such as assisting the visually impaired (Grijalva, Rodriguez, Larco, & Orozco, 2010), banknote sorting and Automatic Teller Machine (ATM) machine software (Gou, Li, Li, & Yi, 2011), and banknote fatigue detection (Daraee & Mozaffari, 2010). A trend observed is that an image is acquired, it is pre-processed then classified and finally the result is output. Various methods are employed at each stage, the correct combination to use is subjective to the currency in question. The same workflow is employed by the digital currency forensics system to classify the note.

Image acquisition and image pre-processing techniques are employed, either the entire note or distinct Regions of Interest (ROI) are acquired and compared independently. The serial number uniquely identifies an individual banknote, in some cases the location of manufacture can be pinpointed (Bender, 2006). Therefore this adds a layer of security and can be computed (L. Li, Yu-tang, Yu, & Liang, 2010). If a note is found to have an incorrect or duplicate serial number it is not authentic.

Image acquisition techniques are explored, the aggregation of RGB colour with ultra-violet information (Chae, Kim, & Pan, 2009). Under ultra-violet light, a dif-

ferent visual appearance is observed, specific areas of the note glow displaying otherwise hidden information, this places extra complexity on the casual counterfeiter.

The fluorescence lifetime is investigated (Chia & Levene, 2009), it is found using a two-photon laser excitation and Time-Correlated Single Photon Counting (TCSPC) method, significant differences in the duration of fluorescence are observed when comparing genuine and counterfeit notes. This approach is an alternative to the image processing and classification model used by this thesis, yet due to the requirement for specialised equipment may not be a practical solution.

Image processing techniques are employed to extract key characteristics, key characteristics are numerical measures computationally describing a banknote image. There are two primary categories of key characteristics used. Colour measurements describe the level of colour by creation of an intensity or grey-level histogram, shape descriptors are key colour characteristics. Texture describes the pattern of pixel colour and their relationship with one another (Verma, Singh, & Agarwal, 2011). It is found that using a vector space composed of both texture and colour features may improve classification accuracy (García-Lamont et al., 2012).

The feature vector is input into a classifier where it is essentially compared against known good values. In literature, many classification techniques are employed on a wide array of currencies, the classification method chosen is subjective to the currency in question and characteristics extracted. Many variants of the classical Artificial Neural Network (ANN) are proposed, using the Back Propagation (BP) learning model with Genetic Algorithm (GA) improves learning performance (Cao & Liu, 2010).

To determine banknote authenticity a measurement is calculated upon comparison of the suspect note and template image. The measurement is used as the determining factor of similarity, the distance measurement is used specifically on ROIs

(Daraee & Mozaffari, 2010) to determine the fatigue of banknotes. It is anticipated, synonymous to fatigue determination, discrepancies occurring during counterfeit production will provide dissimilarity measures which substantially deviate from known good templates.

Different from the existing work, in this thesis the research scope is currency security and forensics, here work is presented in currency feature selection and classifier selection. To the best of our knowledge, this is the first time the Feedforward Neural Network (FNN) classifier with the combined color and texture feature vector combination has been used to automate the process of comparing banknotes.

2.1 BANKNOTE RECOGNITION

A considerable amount of works exist focusing on the area of banknote recognition software intended for application in Automatic Teller Machines (ATMs), automatic banknote sorters, recognition software for the visually impaired (Liu, 2008; Parlouar, Dramas, Macé, & Jouffrais, 2009; Papastavrou, Hadjiachilleos, & Stylianou, 2010; Paisios, Rubinsteyn, Vyas, & Subramanian, 2011; Grijalva et al., 2010) and counterfeit detection.

2.1.1 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 analysing whether each security component deviates from known good values. Table Table 1.1 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.

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. 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.

2.1.2 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 (Russ, 2007; Marques, 2011; Gonzalez, Woods, & Eddins, 2009).

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 what 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 polymerisation 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 tell tale 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 (Neumann, Ramotowski, & Genessay, 2011), 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 waves reflected from matter into a frequency spectrum, light waves reflected from the ink can be characterised and analysed. This opens up a whole new realm 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, achieved by these unique blends where currencies emit unique levels in the infrared and UV spectrum (Kulčar, Friškovec, Hauptman, Vesel, & Gunde, 2010; Žiljak, Pap, & Žiljak, 2009), this has been investigated in a forensic setting using a spectrography microscope (Vila, Ferrer, & Garcia, 2007) for investigation of layer three security features.

Mössbauer spectroscopy is a nondestructive alternative method to determining the atomic composition of pigments (Rusanov, Chakarova, Winkler, & Trautwein, 2009). 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 is used to view photons emitted (Chia & Levene, 2009). The findings show, 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. 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.

A promising nondestructive novel approach to automated determination of ink age is provided by using a Region Of Interest (ROI) (Halder & Garain, 2010). 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 (Chae et al., 2009; Lee & Park, 2010; Z. Li, Zhou, & Chen, 2009). Fluorescent ink is not difficult for counterfeiters with sufficient motivation and finance, during 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 is altered. Used in Optical Variable Devices (OVDs) such as holograms and Kinegrams (Kersten, 2009), 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. 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. Magnetic ink is limited to use on 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 (Qian, Zuo, He, Tian, & Zhang, 2011; Z. Li et al., 2009). 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 (Kulčar et al., 2010). 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 forensically authenticate them must follow. Converting to grey scale 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 (L. Li et al., 2010; K. K. Debnath, Ahdikary, & Shahjahan, 2009; K. Debnath, Ahmed, Shahjahan, & Murase, 2010), new values are generated for each pixel, compressing the amount of data to be analysed 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 *I*, known as intensity thresholding above noise level $I = R + G + B$ (Geusebroek, Markus, & Balke, 2011), the remaining binary image is referred to as

the mask. The RGB channel to grey scale is converted by: $Grey = (R+G+B) \,/\, 3$ (Grijalva et al., 2010). Similarly $k = (0.56 \times R) + (0.33 \times B) + (0.11 \times G)$ was used (Jahangir & Chowdhury, 2007). 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 which blend through the spectrum through similar colours.

Obtaining grey level histogram using the previous methods also omits necessary information regarding the dirty factor of banknotes (He, Peng, & Li, 2008; Hassanpour & Farahabadi, 2009). 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 (Dasari & Bhagvati, 2007; Morshidi, Marhaban, & Jantan, 2008). The YIQ colour space is used, the Y or luminance channel is used for analysis of colour characteristics through histogram comparison (Yeh, Su, & Lee, 2011).

Pixel averaging does have its caveats (Pramoun & Amornraksa, 2009), whilst removing noise, some of the intrinsic print defects may also be removed (Verikas, Lundstram, Bacauskiene, & Gelzinis, 2011; Kumpulainen, Mettänen, Lauri, & Ihalainen, 2011; Shankar, Ravi, & Zhong, 2009). 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 identify specific individual printer, therefore pixel averaging must be implemented sparingly.

This leads us to printer and substrate ballistics, the study of how substrate surface, materials, and printing methods interact. Each print method has unique char-

acteristics, forensic analysis is used to rule out 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.

Few computer users have access to specialised printing equipment, as Offset Lithography, and Intaglio print pressing machines. Inkjet printers are the most commonly used printer on the market today, although they have resolution capabilities that rival laser, they are the most sensitive to substrate quality, resulting in a larger variation of output 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 slightly more robust than dye. Under a microscope both should in theory show round pixels, in practical tests the shape tends not to be so uniform (Russ, 2007; Marques, 2011; Gonzalez et al., 2009). From one inkjet printer to the next 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 is calculated, ultimately, allowing for calculation of printer signatures and profiles for 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 (Huber-Mörk, Heiss-Czedik, Mayer, Penz, & Vrabl, 2007). Using a measure called Maximally Stable Extremal Region (MSER), at point (x, y), measuring displacement is possible by using specific pixels at Points of Interest (POI) as reference points at grey level L, the configuration of R is contained in $R_L \in M_L$, grey level L–δ is calculated using $\mathrm{R}_{L\text{-}\delta} \in \mathrm{M}_{L\text{-}\delta}$. The growth rate G at a specific region and its associated threshold is calculated as

$$G(R_L) = \frac{A(R_{L+\delta}) - A(R_{L\text{-}\delta})}{A(R_L)} \tag{2.1}$$

where $A(\mathrm{R_L})$ is the area of region R at intensity level L, and stored as M_L. The

growth rate local minima is selected as an MSER, where the limit δ specifies the detection sensitivity. This raises the question whether this 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) (Pollard, Simske, & Adams, 2010). Individual documents are given a signature value calculated from the statistical anomalies produced in the printing process

$$p_{\mathrm{i}} = \frac{\sum_{j} j w_j e_{ij}}{\sum_{j} w_j |e_{ij}|} \tag{2.2}$$

where e_{ij} is the strength of an edge corresponding to the digital derivative of the profile image for column i, 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. Currently this research focusses on text glyphs, future work would provide robustness as an added layer of robustness to applications such as serial number authentication.

MBSP and Shape Warp Coding (SWC) are combined for analysis of the interaction between substrate and printing process (Adams, Pollard, & Simske, 2011). It is concluded that forensic investigation scenarios where questions such as how, and who are possible, similar to 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 (Bulan, Mao, & Sharma, 2009; Y. Wu, Kong, You, & Guo, 2009; van Beusekom & Shafait, 2011). Geometric distortion introduced by Electrophotographic (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 (Bulan et al., 2009). 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 (Schulze, Schreyer, Stahl, & Breuel, 2008). 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 banalised and smoothed image.

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

3. **Grey 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.

Such evidence is a crucial step during 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 the investigator 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 forensic science, concerning currency foren-

sics 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 location 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 a specific character set at differing levels of toner (Kee & Farid, 2008). This method is dependent on the toner levels, degradation on the end print, and the particular time in question. The motivation here 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. A grayscale histogram is calculated to measure the texture of ink from

$$f(x,i) = (f(1,i), f(2,i), \ldots, f(m,i))^T \tag{2.3}$$

where the i^{th} row of the image (Xie, Qin, Liu, He, & Xu, 2009). The curve obtained is similar to a sine wave, texture of the ink is defined as

$$M_i = \frac{1}{m} \sum_{j=1}^{m} f(i,j) \tag{2.4}$$

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 (Glock, Gillich, Schaede, & Lohweg, 2009).

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 is significantly reduced (Solymar et al., 2011).

2.1.3 Approaches, methodologies, and techniques

2.1.3.1 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. Standard paper is made predominantly from wood pulp, 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 (Bender, 2006).

During WWII, the Nazi regime went to great lengths to uncover the secret substrate ingredients for the British pound, the key ingredient, a reed found only in south east Asia. However, after their initial products failed the UV lamp test, countless experiments later they discovered that the key material came from recycling

old fabric rags originally from the reed. This finding prompted distribution of rags from the same raw material to factories in Germany and its occupied states, the rags were collected and pulped. They then succeeded in creating counterfeits that were passable under the lamp test, far closer than they had ever been (Burger, 2009).

Viewing a note under UV light, certain amounts of fluorescence become visible in specific areas creating a unique signature, this signature should be near 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 Organisation (CSIRO) and the University of Melbourne, Australia. 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, shown in figure Figure 2.1, which turns black when scanned or photocopied.

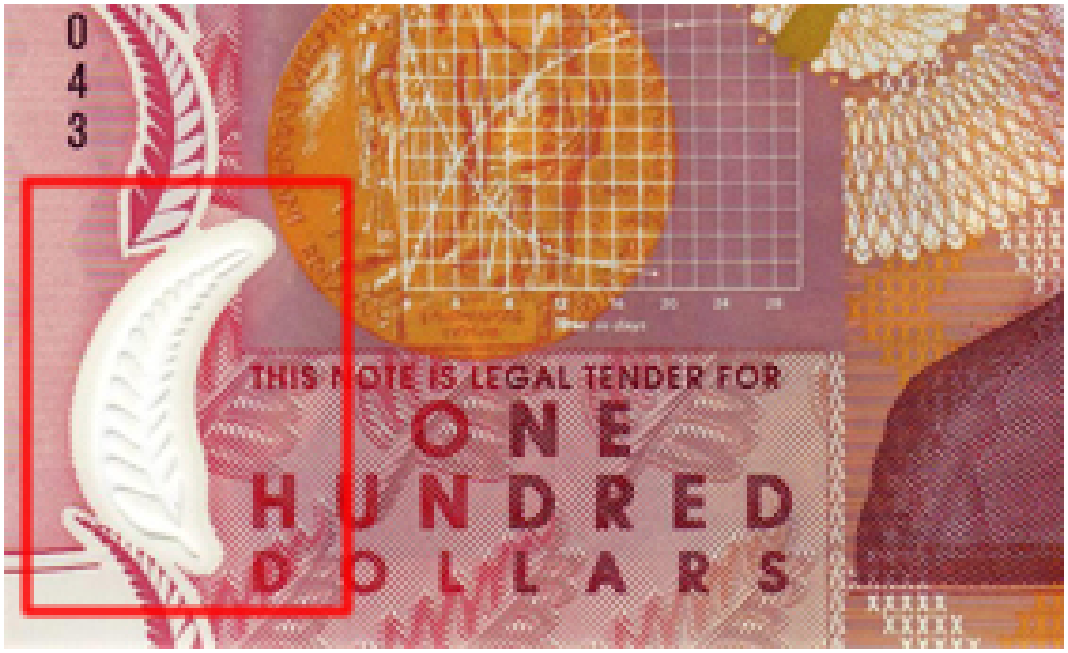


Figure 2.1: See through window on the New Zealand banknotes in the shape of a fern leaf, also on the corresponding side a see through window stating the denomination value having a unique raised tactile quality.

There is growing interest in the development of new security components for embedding through the manufacture and printing process. (Berthier, Boulenguez, & Bálint, 2007) shows, the scales of Lepidopetra and elytra of Coleoptera butterflies possess micro structures resulting in unique polarisation 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 (Clarkson et al., 2009). 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. Louisenthal, one of the worlds largest security paper manufacturers have adopted polymer offering a polymer-paper hybrid alternative.

The reserve banks of both Australia and New Zealand report that even polymer is not immune to counterfeiting, and appears counterfeiter sophistication is on the rise. Clearly, as the sophistication of the counterfeiters rise forensic analysis of the texture of BOPP must be analysed similar to that of security paper, forensic science 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 is produced by the compression of many plant fibres, a common property of substrates is that there will always a level 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 the 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 a note to a light source, random coloured fibres appear, 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 (Yoshida, Kamruzzaman, Jewel, & Sajal, 2007). 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 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 unauthorised reproduction, such measures are also aptly termed screen traps. The effect is caused by the digitisation of a genuine note, followed by an attempt to print from the digitised 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 (Tarnoff, 2011), 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 (Qi, Li, & Yang, 2009).

The Guilloché, a security pattern used originally on medieval armour 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 on the banknotes of the current series of the New Zealand currency shown in figure Figure 2.2.

(a)


(b)

Figure 2.2: The Guilloché. (a) Guilloché can be found on the New Zealand banknotes just to the left of the portrait, (b) As the Guilloché is magnified, 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, 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 monitored by the authorities (Bender, 2006). 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 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, also 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 recognises a forbidden security image, it will refuse to continue theoretically rendering unauthorised 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 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 recognises 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 (Nieves, Ruiz-Agundez, & Bringas, 2010; Verikas et al., 2011).

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 a counterfeit (Zhao, Gu, & Fang, 2008). 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 present in software (Zhao et al., 2008).

Certain laser printers have been found to systematically print yellow dots, making the device identifiable (Beekhof, Voloshynovskiy, Koval, Villan, & Topak,

2008). These yellow dots are hidden codes that allow for the determination of the make and model (van Beusekom, Schreyer, & Breuel, 2010). A similar method is presented for steganographic techniques in bicolour printed documents, by pseudo-randomly distributing tiny black dots (Kim & Mayer, 2007), 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 inkjet, Dry Electrophotographic, and Liquid Electrophotographic Printing (S. Simske et al., 2007; S. J. Simske, Aronoff, Sturgill, & Golodetz, 2008; S. Simske, Adams, Aronoff, & Sturgill, 2009). The colour tile, standard barcode, and 2D are investigated, colour-tiles prove to be an effective method for measuring a printers colour output fidelity. Such findings allow for discrimination of recent documents where ink has not been exposed to light for a long duration of time, monotone methods such 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, or 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 will remain.

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 (Kersten, 2009).

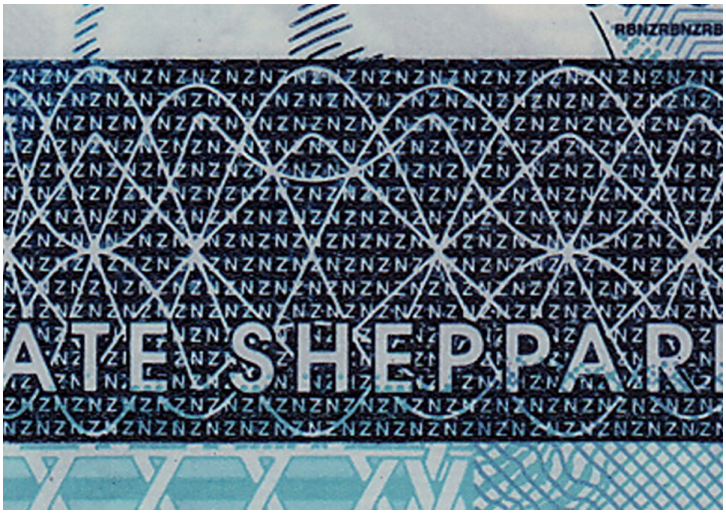
Building on the traditional watermark concept is a method called the Optical Variable Watermark (OVW), micro apertures are embedded directly in polymer substrate as a series of pulse width modulated pixels. The structure is divided into two channels: the individual pieces of artwork are interlaced with 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, consisting of a specific carrier structure, using the right combination of these layers is known as the 'key'. When the key is positioned, the hidden information below is revealed in its plain unencrypted form (Huang & Wu, 2007; Hrishikesh & Shefali, 2009). 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) (Nah, Kim, & Kim, 2009). Most watermarking techniques embed data in one colour component, or independently in each colour component (Trémeau & Muselet, 2009).

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 you magnify the area, edges begin to blur.

(a)



(b)

Figure 2.3: Micro-text, when micro text is magnified it should appear crisp and not blur as the magnification level increases. (a) the area on the RBNZ $10 banknote shown appears to consist of an arbitrary pattern; (b) when the magnification level is increased the letters NZ become clear and do not fade and were otherwise hidden from view.

Figure 2.4: A unique identifier, the serial number is usually found repeated vertically on the left hand side and horizontally on the right hand side of the obverse.

A serial number shown in figure Figure 2.4 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. New Zealand's current series of banknotes shown in figure Figure 2.4, indicates the year the banknote was printed and series number. Serial Number Range: AA07 000001 - AA07 001000 indicates the series manufactured within the Print Year: 2007, indicated by the prefix 'AA07' the remaining digits uniquely identify the individual note within that print year, the Euro

currency has the added complexity of specifying specific central bank of issue, as the Euro is issued from multiple points within the European union.

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. As discussed in Section 2.1.3.1, 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.

2.1.3.2 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 minimises, and controls the flow of counterfeit and worn out banknotes for destruction. A brief discussion of such software follows whilst outlining three core functions: 1) image processing, 2) feature extraction, 3) classification.

After the image of a banknote has been captured it must be preprocessed to have specific characteristics of interest singled out. First, the edges of the banknote image must be recognised and captured. Typically preprocessing an image of a banknote consists of: 1) a binarization stage, 2) an edge detection stage, 3) distortion correction.

A modified canny edge detection is used (Singh, Badoni, & Verma, 2011) 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 (L. Li et al., 2010). 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 grey levels, or texture in image objects. The correct threshold value is determined using adaptive thresholding (Grijalva et al., 2010). 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 (Nishimura, 2009). A threshold is used for each subsection, contributing to a threshold ratio or T-ratio.

Whole notes are separated into blocks using $M \times N$ (Grid Segmentation) (Guo, Zhao, & Cai, 2010; Q. Wu, Zhang, Ma, Wang, & Jin, 2009), each block is subject to a Logical Binary Pattern (LBP) method. Each pixel within the block is calculated

and assigned an LBP value where *p* is defined as:

$$LBP(p) = \sum_{i=0}^{7} 2^2{}_s(g_\mathrm{i} - g_\mathrm{p}) \tag{2.5}$$

Followed by:

$$LBP(p) = \frac{[\sum_{i=0}^{7} 2^2{}_s(g_\mathrm{i} - g_\mathrm{p})]}{Q} \tag{2.6}$$

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

A projection profile is calculated from eroded images $b\text{-}subscripte(x, y)$ of Q rows and R columns (Grijalva et al., 2010), the sum of all white pixels in each direction: vertical projection profile:

$$P_\mathrm{V}[y] = \sum_{x=1}^{R} b_e(x, y), y = 1, 2, \ldots, Q \tag{2.7}$$

Horizontal projection profile:

$$P_\mathrm{H}[y] = \sum_{y=1}^{Q} b_e(x, y), y = 1, 2, \ldots, R \tag{2.8}$$

where P_V refers to a vertical projection and P_H refers to a vertical profile. It is demonstrated that this is a flexible method for implementing into smart devices where the placement of the currency note is of an arbitrary rotation and design, as the template image can be tailored for recognition to suit requirements.

A Principal Component Analysis (PCA) function for image feature extraction and compression (Omatu, Yoshioka, & Kosaka, 2009; Sun & Li, 2008a). PCA

is well suited to application 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 PCA is used to determine the necessary features it can be assured that only the necessary elements are being checked for.

Following extraction, the Kohonen based Self Organising Map (SOM) model is used to cluster data extracted into homogenous regions, 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 (Sun & Li, 2008a).

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 (Hasanuzzaman, Yang, & Tian, 2011, 2012). A banknote image is able to be recognised 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 for the detection of fraudulent currency activity, for instance Closed Circuit Television (CCTV) footage located in a convenience store.

ROI approach is used (Daraee & Mozaffari, 2010), using Discrete Wavelet Transform (DWT) for scaling and shifting with Packet Wavelet Analysis (PWA), and Maximum Overlap Algorithm (MOA). 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 (Jin, Song, Tang, & Du, 2008), as a joint effect including dust and old age discolouring the notes over time and randomness (Daraee & Mozaffari,

2010).

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) improve the accuracy by using multiple geometric shapes to extract more data about the area (Jahangir & Chowdhury, 2007).

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 is learned through the initial training phase based 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) are used in much of the literature, Genetic Algorithm (GA) is combined with Back-Propagation (BP) (Jing, Shuang, Jin, & Wei, 2010; Z. Li et al., 2009; Cao & Liu, 2010; Zhou, Xie, & Liu, 2008). In each case, an increase performance was observed over using ANN alone. Ensemble Neural Network (ENN), a finite collection of Neural Networks 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 (K. K. Debnath et al., 2009; K. Debnath et al., 2010). A Counter Propagation Network (CPN) is used for note classification by (Sun & Li, 2008a), 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 un-categorisable due to wear and tear (Sajal, Kamruzzaman, & Jewel, 2008).

Support Vector Machines (SVM) appear to be widely used throughout the lit-

erature and promise a wide variety of applications such as banknote classification (Ishigaki & Higuchi, 2008; Chang, Yu, & Yen, 2007; Gaubatz & Simske, 2009; Gaubatz, Simske, & Gibson, 2009; Ryu, Lee, Cho, & Lee, 2008; Sun & Li, 2008b). SVM is successfully implemented to recognise serial numbers on banknotes (Wenhong, Wenjuan, Xiyan, & Zhen, 2010), and used for detection of stains to determine worn out banknotes (Sun & Li, 2008b). Results show classification accuracy comparable to that of ANN, however it is determined that using multiple kernel support vector machines can increase accuracy and overall performance (Yeh et al., 2011).

Learning Vector Quantisation (LVQ), implemented by (Gou et al., 2011; Omatu et al., 2009), LVQ is relatively inefficient when compared to similar algorithms. As observed (Omatu et al., 2009) though PCA was used before classification, to increase reliability, this method still requires a subsequent clustering phase to model the complexity of the classified data, decreasing overall performance.

AdaBoost machine learning algorithm was applied on the N most discriminating features (Geusebroek et al., 2011), the ratio between red and blue intensity channels is measured for those areas. It is found that using the colour channels over grey 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 (Shan, Peng, Jiafeng, & Xianglong, 2009), a comparative analysis study of HMM, SVM and ANN is performed (Shan et al., 2009). HMM outperformed both SVM and ANN, test results show HMM %93.92, ANN %92.8, SVM %88.52. HMM looks to be an attractive option due to the higher classification accuracy, furthermore as HMM can learn feature sets overtime the system can be tuned strictly for what needs to be checked, using sound discriminative features.

Clearly, the security printing industry is making continual technological ad-

vances for which not only forensics needs to catch up, so 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.

One could be forgiven for assuming that it will not be long before electronic currency replaces paper currency (Hong, 2009). On the contrary, physically exchangeable currency is here to stay, at least for the foreseeable 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.

The current trend in physical paper based currency shows the use of paper will continue for the foreseeable 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, Vietnam, and Singapore 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 worlds 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 realised by those countries whom have adopted polymer in full but by those who produce security paper, by 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. Although most devices focus on the legacy components of serial number and print fidelity. Implementing security detection devices ATMs and banks, 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 recognising specific characteristics intrinsic to polymer.

Print signature and 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 (Adams et al., 2011; Bulan et al., 2009; Gaubatz & Simske, 2009; Gaubatz et al., 2009; Kee & Farid, 2008; Pollard et al., 2010), print anomalies can be detected and calculated to create a signature based on pixel distribution and satellite droplets. Similarly texture analysis of paper, (Xie et al., 2009; Clarkson et al., 2009) investigate various qualities of the texture and roughness of surfaces relating to documents and banknotes, similarly (Glock et al., 2009) investigates the texture of the ink pattern. Classification 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 realising 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 ATMs and central bank note sorting machines. The method of classification between that which is 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.

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, forensic science must understand the process of security printing, the ingredients and characteristics of substrates, inks and complexities of integrated security components.

Extensive research exists for computer vision and machine learning for application 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 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 forensic science is equipped to identify forgery.

Analysing 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.

2.2 CONCLUSION

To conclude, this has been a synthesis of the current state within the field of forensic science dealing with currency forensics. A survey was necessary, as there is no known available research specifically dealing with counterfeit currency or electronic fraud from a forensic investigator, or forensic scientist point of view. 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 analyse with any scientific merit, forensic science must understand how currency is manufactured. Forensic science must 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 have 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 of the three layers of banknote security. Specifically the first layer is that which by 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 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 a deterrence in its self and remain only for tradition sake.

Traditionally, banknotes in question have been checked by specially trained Questioned Document Examiners (QDE), QDEs analyse 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 and 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, so do the skills and resources of counterfeiters. Automatic banknote sorting and authentication has 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 re-circulation. Understandably, this is essential to protect any 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, though 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 benefits over electronic currency, such as full anonymity of payment and a

reducing more controlled form of currency.

Chapter 3

Methodology

3.1 INTRODUCTION

A comparatively infinitesimal amount of literature exists in support of forensic analysis of questioned currency, when compared to other areas of specialization requiring forensic investigation. There are continual technological advancements promising high levels of security, whilst allowing for stronger security, and more robust currency, these advancements also allow for unauthorised currency reproduction.

Since the epoch of formal currency systems, currency issuers have faced one common threat, the threat of counterfeit currency. This continual technological advancement of tools and techniques available to both the issuing authorities, and the general public have fuelled an incessant battle.

It is well known that the purpose of forensic investigation is to answer questions of a legal nature, this requires scientific investigation to understand the fundamental mechanics of questioned phenomenon. Much of the fundamental mechanics of currency systems is unknown, and shrouded by great mystery, and trade secret style secrecy.

This presents one fundamental problem, forensic science will remain in the wake of counterfeiter skills and manufacturer technologies. With the increasing array of currency variants, and the corresponding lack of forensically motivated literature there is much room to explore. Clearly there is much opportunity to develop currency forensic analysis methodologies and more robust currency.

Design of the thesis: It has been identified that the security of currency is constantly being compromised, the primary motivation for this thesis is to solve the problem and provide a solution, building the foundations for further research. It is envisaged that such a solution be in marketable prototype form with supporting blueprints, therefore a prototype will be designed and developed through research efforts.

Design science research was identified as the ideal research paradigm to follow; design science research supports the design, and development of an artefact to solve an identified problem, where there is no clear literature base, or methods available for solution. Incrementally, and iteratively a prototype will be developed to satisfy requirements identified during initial investigation, at each increment new requirements which will be fed back into the beginning of the next iteration.

Following the design science methodology, seen in figure 1, there are six high level phases which will be used to manage this research and development project. Following is an explanation of what will be done in each phase, accompanied by a timeframe estimate.

Problem Identification and Motivation: Initial investigations have identified that a problem exists, specifically the relentless battle between currency designers and criminals. This has motivated a thesis in developing secure currency and defining forensic investigative methods.

Definition of Objectives for a Solution: It has already been identified that the main objective is to understand and define the mechanics of currency, whilst

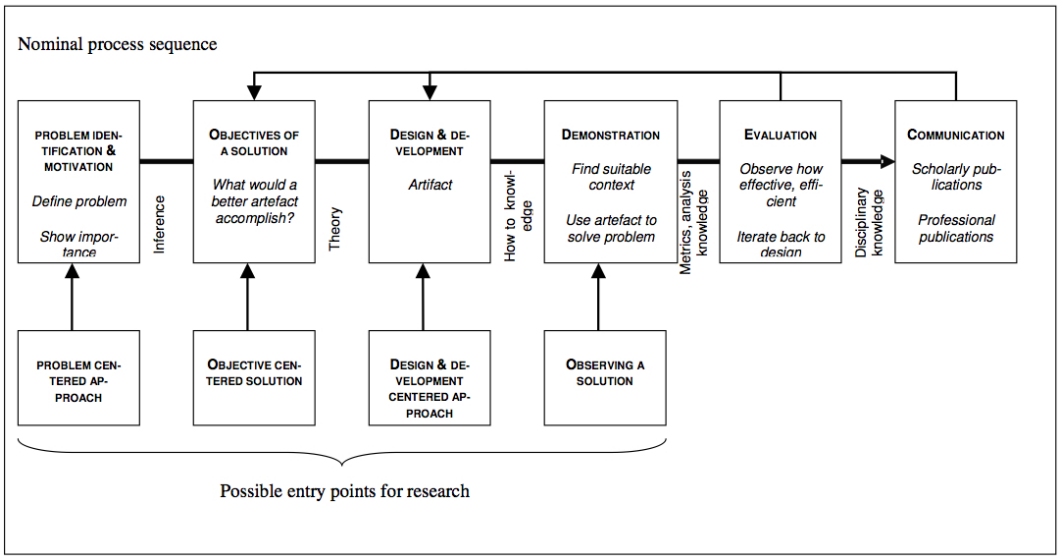


Figure 3.1: Design science research methodology process model (Peffers et al., 2006).

emphasising the weaknesses so that specific improvements can be made to address identified weaknesses. Objectives will continue to surface as this exploration takes place.

Design and Development: The envisaged artefact is not yet known, and cannot be known at this stage. However, the process will be to use the objectives defined in the previous two phases to influence the required output. Depending on the exact artefact requirements identified in previous phases, specific development methodologies may be employed at this stage.

Demonstration: Demonstration will address the key issues being solved at each iteration end, potential stakeholders will be invited to take part and provide feedback.

Evaluation: Evaluation, immediately following demonstration of outputs, a critical evaluation will take place to determine how well the output satisfies requirements. Based on the type of output at each iteration, specific metrics will be

defined for measuring the effectiveness to solve the following problems.

3.2 REVIEW OF SIMILAR STUDIES

3.2.1 Colour features

Colour has been used widely as a prominent feature by banknote designers for the differentiation between denominations; colour features are suitable for computation and analysis, as statistics can be derived for computational description of an image or a scene. A large majority of banknote recognition technology and research in literature applies the use of colour, it is observed that where currencies apply a dominant colour for differentiation, the dominant colour can be calculated and used as part of a feature vector and even as a single feature (García-Lamont et al., 2012).

3.2.2 Texture features

The texture of the Indian Rupee banknotes is considered a more robust descriptive characteristic than colour (Verma et al., 2011). The Mazda tool was employed to extract texture features, in total Mazda is capable of gathering 320 useful texture features; the fisher Linear Discriminant Analysis (LDA) was used for reducing the total number and complexity of actual features selected for end use. Feature reduction is performed by using the Linear Discriminant Analysis (LDA) method. The determination of key features is obtained from a given set D, the d best features on a $d \times D$ linear transformation matrix, A is performed. Following this, a determination of the between class scatter matrix, and within-class scatter matrix where the most discriminating feature is obtained, and used as the key characteristics.

A method was formulated for the recognition of the Mexican Peso banknotes, based on their colour and texture features (García-Lamont et al., 2012). It was

concluded, many countries globally use colour as a key defining feature for the differentiation of banknote denominations, and colour is a suitable computable characteristic. The average colour is taken at every pixel location and summed to obtain the dominant colour of the image:

$$\vec{C_s} = \sum_{i=1}^{N} \sum_{j=1}^{M} \vec{C}(i,j) \tag{3.1}$$

the dominant colour is used as the key defining colour. It was determined, using this characteristic alone gave a 93.34% accuracy rate on classification with a Linear Vector Quantisation (LVQ) classifier; when combined with texture characteristics using the Logical Binary Pattern (LBP) accuracy was increased to around 97.50%.

3.3 THE RESEARCH QUESTION AND HYPOTHESES

This is a multi-pronged thesis. Primarily, the objective is to define the key mechanics of banknotes from a security perspective, and to develop an authentication system to facilitate the forensic analysis of such security mechanics. Initially, a synthesis of the literature was conducted in the form of a literature survey. This survey was conducted over areas of interest specifically related to currency forensics, whilst identifying the major security components, their associated mechanics, and associated attacks. Subsequently, the survey provides an insight into current trends; whilst suggesting future directions to begin design and development of suitable algorithms, and a functional software prototype for demonstration purposes. Resulting from this survey, further questions were raised regarding the most suitable algorithm design to automate the analysis process.

The primary insight gained through conducting the aforementioned survey concludes: banknote recognition software is an active area of research, as are various

areas related to print, substrate, and ink analysis. However, it appears that research on automated systems focusing on counterfeit detection is a comparatively infinitesimal area. Consequently, automated counterfeit currency detection algorithms and system proposals can be separated into two broad categories: 1) those focusing on analysis of the banknote as a whole image; 2) those which focus on specific areas of interest known as Regions of Interest (ROI).

The former category refers to a clearly defined model – where banknote image processing techniques are used in varying ways to extract characteristics suitable for computational description of the banknote; whereas the latter category may refer to a unique analysis method applied to a specific ROI, such as known security marks. ROIs are prime candidates for dedicated analysis, as the algorithm is able to concentrate on authentication of known difficult to replicate areas; typically, traditional scientific methods of analysis, such as, detection of magnetism levels emitted from pre-defined areas on the banknote surface. The approach employed by this thesis, is to use the former method, firstly to classify a given banknote image, followed by matching the features extracted from the given image with known good values from template images in a database of legitimate banknote samples.

To ensure an optimal approach is used to design this solution, various questions are raised regarding computational definition of a banknote image; given a computer's inability to understand the contextual nature of images, we are left with the analysis of colour, and the texture of the banknote image (García-Lamont et al., 2012). It is observed from the literature; both colour, and texture features provide suitable key characteristic discriminability, to perform pattern recognition using machine learning techniques. The key question relates to determination of the right, or 'best-fit' characteristics to implement in the end solution.

As this solution must classify banknotes by their respective denomination before authentication, the key characteristics used must be of the most descriptive as

possible to enable the classifier to differentiate between any given data. The grey-world algorithm is used to reduce the complexity of image data from a colour RGB image shown in figure Figure 3.2, to a single colour intensity channel shown in figure Figure 3.4, thus, focus is solely on colour intensity characteristics. Initially, an image is captured in the RGB colour space, there is a total of three channels, suppose an image is captured at 640×312, this gives a total of 199,680 pixels; however, in actuality there is $640 \times 312 \times 3$ values shown in figure Figure 3.3 as all three colour channels are considered.

Hence, as an image is input to the system it is represented in the RBG colour space shown in figure Figure 3.2. Computationally, the image is represented by an array in the Cartesian coordinate system.

Figure 3.2: An acquired image is input to the system as a three channel RGB image, and is converted to a uniform size of 640×312.

As there are three channels, there is essentially three individual arrays, for illustrative purposes each channel has been shown as its respective colour shown in figure Figure 3.3. Computationally, the individual arrays are represented as intensity values within the respective channel, shown in figure Figure 3.3, thus each

channel stores different aspects of the images, the individual channels may provide information which may be lost when converting to single intensity channel.

Figure 3.3: The RGB image is separated into individual R, G, and B channels thus three individual 640×312 arrays, respectively.

Each of the individual R, G, and B channels are represented computationally as arrays of equal dimensions, where each corresponding array element of the same coordinate defines the colour characteristics of its respective channel at the (x, y) location. The average at each (x, y) location is calculated, thus for each of the 640×312 elements, the average is taken as $I = \frac{(R+G+B)}{3}$, and the resulting average value is stored as a value between 0 and 255 at the corresponding (x, y) location in the newly created intensity image, shown in figure Figure 3.4.

Thus, each banknote intensity image stored in the template database is repre-

Figure 3.4: After conversion, a resulting intensity image is saved for all future analysis.

sented as one single uniformly sized matrix of 640×312 pixel values, this concludes the preprocessing phase. Each 640×312 array representing template and suspect notes from herein specify the fundamental storage of image data, from which all future processing will be performed.

A histogram is computed to define a signature of the captured image as shown in figure Figure 3.5, and figure Figure 3.6; each denomination should show a similar shape. Thus, shape, and statistical shape descriptors can be used to specify a threshold to evaluate similarity between template banknote array, and suspect banknote array. From the resulting histogram, statistical shape descriptors enable the system to computationally define and compare the shape; the histogram records the frequency occurrence of all pixel intensity values between 0 and 255, where 0 is completely black and 255 is completely white, all values between represent the grey-level representation of the respective averaged RGB value. Each denomination should present a histogram with similar shape characteristics, particularly in the peaks and troughs; this can be verified by initial pilot tests shown in fig-

ure Figure 3.5, and figure Figure 3.6, the reverse of all subsequent $100 RBNZ notes should provide similar shape, similarly, the histogram of the $10 RBNZ shape is shown.

Therefore, it can be said that the intensity histogram obtained from an image of the reverse side of all suspect RBNZ $100 banknotes should roughly match that shown in figure Figure 3.5, and, similarly, an image of the obverse side of all suspect RBNZ $10 RBNZ banknotes should match closely to that shown in figure Figure 3.6. Histogram statistical shape descriptors are therefore suitable candidates, and are calculated accordingly to define a colour feature vector. In this thesis the colour feature vector is comprised of six key shape descriptors, namely: (1) kurtosis, (2) central moment, (3) mean, (4) variance, (5) standard deviation, and (6) skew.

Kurtosis is a measure of the 'peakedness' of a probability distribution, another way to describe the kurtosis, is that it is a measure of how 'outlier-prone' the distribution is. Distributions are determined as outlier-prone when the calculation returns a value greater than 3, distributions which are not outlier-prone return a value less than 3. The matrix of an image is permeated to a vector, and then the kurtosis calculation is performed,

$$k = \frac{E(x-\mu)^4}{\sigma^4} \tag{3.2}$$

where μ is the mean of x, and σ is the standard deviation of x, and E is a function representing the expected value of the input vector.

The second characteristic used in the colour feature vector is the third or 'μ_3' central moment, the third central moment is a standardised moment used to define the skewness of the distribution. The central moment is calculated by

$$m_k = E(x-\mu)^k \tag{3.3}$$

where E is a function producing the expected value of x. Here, similar to kurtosis,

the third central moment is calculated over a permeated matrix of the original grey-scale image, as one single vector.

A well known statistic, the mean value μ, is used as the third part of the colour feature vector. The mean is a useful characteristic in the application of banknote recognition, where banknote denominations are characterised by specific dominant colours. Intuitively it could be expected that, in dominant colour defined banknotes, each colour specifies an intensity level in the intensity image; therefore, the mean value will describe the dominant colour, and allow for denomination discriminability accordingly. Then, the mean value μ, in this instance, is taken as the summation of the 'element-by-element' multiplication over the pixel counts, and, then, divided by the number of pixels in the image, as

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i = \frac{1}{n}(x_1 + \ldots + x_n) \tag{3.4}$$

where i is the grey-level value at pixel location i, n is the total number of pixels in the image.

Another well known statistic, variance, is a statistic which measures, and describes the spread of the observed distribution. Typically, the variance is used to measure the variability of data, by how far the observations deviate from the mean value. The variance is simply a calculation of all squared differences at each observation, where we have σ^2, using the elementary calculation for variance as

$$Var(X) = \sum_{i=1}^{n} p_i \cdot (x_i - \mu)^2 \tag{3.5}$$

where in this thesis the summation is obtained by an element-by-element subtraction of observed grey-level values, from the mean grey-level, squared, and similarly multiplied in an element-by-element fashion by the total number of pixels, then finally dividing by the total number of pixels, minus the value one.

Similarly, the standard deviation σ, is another well known statistic used to describe the shape of a probability distribution; the standard deviation measures the

variation, or dispersion from the average or mean value, shown in equation (3.4). The standard deviation is used to measure the variability of the data distribution, particularly how the observations deviate from the observed mean value. Therefore, in each sample obtained from captured banknote images, we would expect to observe similar standard deviation values within each specific denomination. The standard deviation is calculated as the square root of the variance in equation (3.5), and, thus, the standard deviation is obtained by

$$s_N = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2} \tag{3.6}$$

The calculated skewness measure of a distribution provides a description of variability of observed data about the mean μ, indicating the asymmetry of the distribution. Again, the skew is a well known statistical measure used in many applications; the calculation outputs either a negative, or a positive value. Here, a negative number indicates skewness tending to the left, positive skew values indicates skewness tends to the right. The direction of the skew indicates to which direction data in the observed sample contains a higher level of variability. The skewness of any distribution is calculated by

$$s = \frac{E(x-\mu)^3}{\sigma^3} \tag{3.7}$$

where, similar to the equations for mean, variance, standard deviation, and skewness, in this thesis matrix values are the fundamental units being operated on, as such an element-by-element calculation is performed, whereby at each pixel the calculation is performed to calculate skewness. It is expected, in any captured banknote image, the skew would also be similar from one banknote of the same denomination to another, thus providing capabilities for discriminability between captured banknote image classification.

Texture is taken into consideration, texture relates to tonal characteristics of colour, thus, providing the ability to describe the nature of transition from one

colour to another within an image. The entropy value of a grey-scale image determines the randomness, and the nature or distribution of pixel intensity values throughout an image. The first measure of texture used in the texture feature vector is the measure of entropy, entropy is calculated from a converted grey-scale image as

$$E = -\sum_{i=1}(p_i \cdot \log_2^{p_i}) \tag{3.8}$$

where p_i is the histogram counts returned from the pre condition, where a grey-level histogram must be compiled, in this thesis the grey-level histogram is using a total of 256 bins representing grey-levels between 0 and 255.

Next, a Grey-Level Co-occurrence Matrix (GLCM) is computed, in this thesis a GLCM is a matrix of values representing the frequency of intensity values between 0 and 255, whilst indicating how often an intensity value i occurs adjacent to intensity value j in the matrix. If one considers the grey-level RBNZ $100 note shown in figure Figure 3.7, in this example, the grey-level banknote image is magnified; when the image is magnified, we observe what is called pixelation. Now if we consider each pixel in the image, we can see that there is a single intensity value at each pixel, each pixel value may have a grey-level value recorded between 0 and 255. Then, as we move to each pixels i, adjacent pixel j, in a N, level circular neighbourhood, we can describe how intensity changes throughout the design of the image.

From the banknote GLCM, various descriptive statistics may be calculated to describe image texture, and subsequently comprises the second part of the feature vector in this thesis. The second half of the feature vector consists of texture descriptors, and is concatenated with the colour feature vector to form one single subset of descriptive measures.

As shown in figure Figure 3.7, as the magnification of the grayscale banknote image is increased the individual pixels become evident, the GLCM may be calcu-

lated with variable values. The values which may vary between individual GLCMs are the amount of grey levels present, a threshold is set whereby, pixel values in a grey-level image contains levels from 0 to 255 a GLCM may be reduced to a smaller number of grey-levels, pixels within predefined ranges are scaled up or down to the nearest corresponding threshold value.

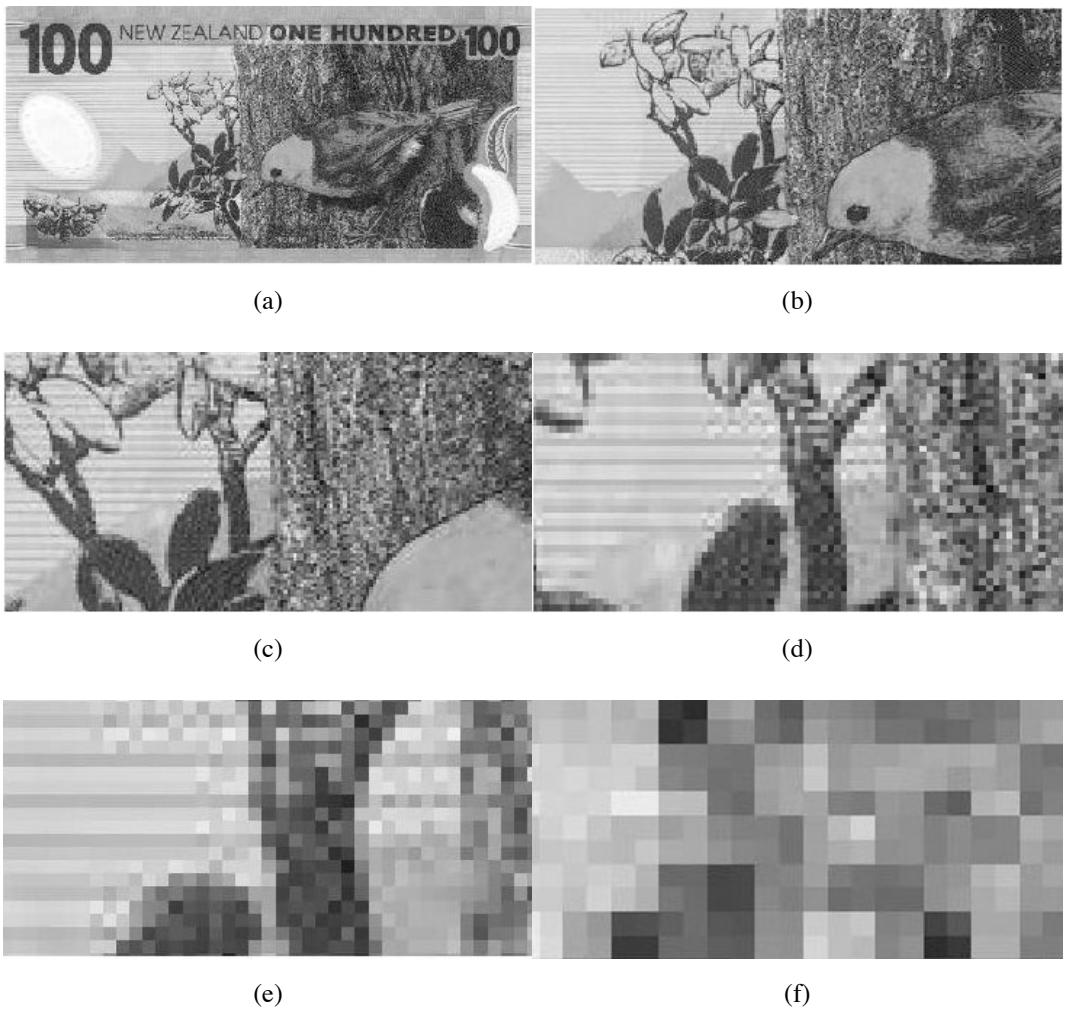


Figure 3.7: Magnification of the RBNZ $100 banknote, demonstrating pixilation (a-f), as we increase magnification we eventually see the individual pixel.

In this thesis, the amount of grey-levels used within the GLCM computation

is 8. Therefore, the possible values from 0 to 255 are reduced to eight different threshold values, resulting in a total of eight possible levels in the GLCM. For illustrative purposes, let's suppose the 640×312 image shown in image Figure 3.8, and a GLCM calculated as shown in table Table 3.1.

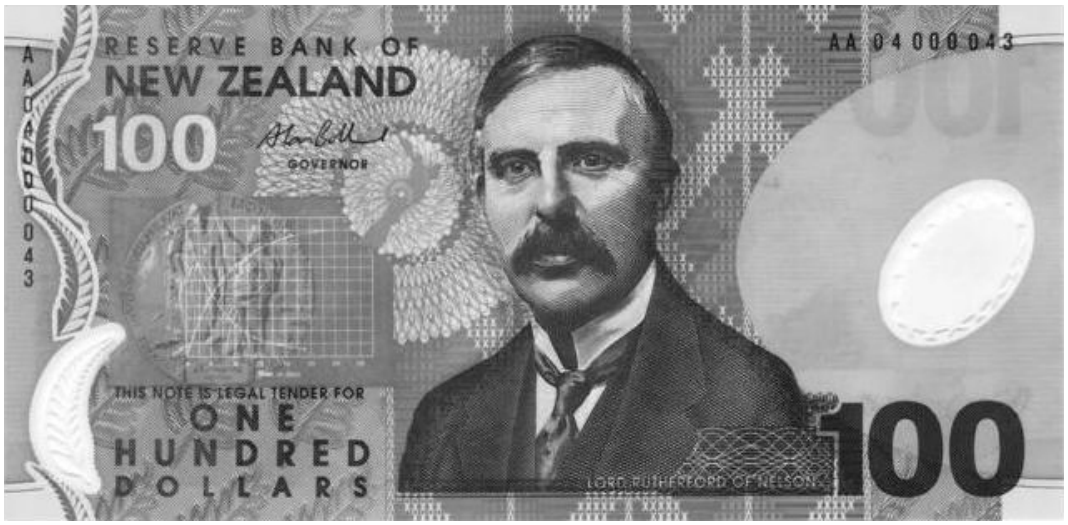


Figure 3.8: Obverse RBNZ $100 banknote image shown as equal weighted grey-scale.

The occurrence of each grey-level value within the reduced range is recorded, as shown in the matrix in table Table 3.1, using the calculation shown in equation (3.9), and equation (3.10). Table Table 3.1 displays the frequency or how often a pixel of grey-level x, occurs next to a grey-level of y. Again, a variable which may be used to determine the characteristics desired from the GLCM, is the offset value that describes how many pixels away from each pixel in question. In this thesis the offset value used is 0,1, thus, for each pixel in question, the value immediately adjacent is recorded.

$$C_{\Delta x,\Delta y}(i,j) = \sum_{p=1}^{n}\sum_{q=1}^{m}\delta_{p,q} \tag{3.9}$$

Table 3.1: The obverse RBNZ $100 banknote image shown in figure Figure 3.8 as equal weighted grey-scale, calculated as GLCM with 8 possible levels of grey.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0	2	1	3	0	0	0	0
2	2	4962	3592	664	180	13	0	0
3	2	3706	17573	3706	877	184	3	0
4	2	608	3742	21092	8289	1167	88	0
5	0	133	964	8318	31602	8233	665	0
6	0	2	170	1128	8228	44459	2964	5
7	0	0	9	77	735	2819	9462	519
8	0	0	0	0	0	6	517	7895

$$\delta_{p,q} = \begin{cases} 1, & \text{if} I(p,q) = i \quad \text{and } I(p+\Delta x, q+\Delta y) = j \\ 0, & \text{otherwise} \end{cases} \tag{3.10}$$

From the resulting GLCM, certain descriptors can be calculated, similar to histogram shape descriptors used for the colour component of the feature vector used in this thesis. Four GLCM descriptors are concatenated to the entropy value obtained by equation (3.8), and thus used to formulate the rest of the texture feature vector. The GLCM descriptors used are: (1) contrast, (2) correlation, (3) energy, and (4) homogeneity.

Contrast is used to describe the level of contrast present in an image, shown in table Table 3.1; in this thesis an offset of 0 and 1 is used. If we consider that contrast is the difference between the dark light parts of the image, we can calculate the contrast by

$$C = \sum_i \sum_j |i-j|^2 p(i,j) \tag{3.11}$$

where the resulting contrast value ranges between 0, and 1. The closer the return

value tends towards 0, less contrast is present in the observed data, whereas, a returned value that tends towards 1, indicates that more contrast is present. As each banknote of a specific denomination must have identical imagery, we would expect a similar level of observed contrast for each within the same class.

Statistical measures may also be used to describe the relationships, across the observations represented by the GLCM. A similarly well known statistical measure used to measure the strength of a relationship between two observations, is the correlation value; therefore, by determining the strength of any such relationship, we can determine whether or not there is any actual relationship to begin with. In this thesis, the correlation is calculated as

$$C = \sum_{i} \sum_{j} \frac{(i - \mu_i)(j - \mu_j)p(j, j)}{\sigma_i \sigma_j} \tag{3.12}$$

where, the returned correlation value is a summation over all pixel values, indicating the relationship between all pixels to their adjacent neighbour. A correlation value between -1, and 1 is returned from the calculation. A correlation value which tends towards 1, indicates that the pixel values in the captured image are closely related, whereas a value which tends towards -1, indicates that the observed image pixel values are not so closely related.

Next, the angular second moment is taken, the angular second moment is also known as the image uniformity measure, or energy; from hereon this feature will be referred to as the energy statistic. The energy statistic of the image is calculated over the GLCM observations by

$$E = \sum_{i} \sum_{j} p(i, j)^2 \tag{3.13}$$

where, the returned energy value is the sum of all elements squared within the GLCM. The possible return values range between 0, and 1; as the returned value tends towards 0, the observed captured image texture is more variable, and as it

tends towards 1 there is less variable. Thus, an energy value closer to 0 indicates that the texture of the captured image is more detailed, when the value returned is closer to 1, the texture of the observed image is less detailed. Intuitively we would expect the GLCM energy values of grayscale banknote images to have a similar amount of energy, as the image should be extremely similar.

Finally, the GLCM homogeneity is taken, the homogeneity is also referred to as the inverse difference moment. The homogeneity is an inversion to the contrast, and is calculated as,

$$H = \sum_{i} \sum_{j} \frac{p(i,j)}{1 + |i - j|} \tag{3.14}$$

where, the resulting homogeneity value measures the closeness of the distribution to the GLCM diagonal. If we consider the GLCM shown in figure Table 3.2,

Table 3.2: The diagonal GLCM from the example image.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	0	0	1	0	0	0
6	0	0	0	0	0	1	0	0
7	0	0	0	0	0	0	1	0
8	0	0	0	0	0	0	0	1

we can see that in this case a value of 1 always occurs next to 1, and so on, indicating the observed image texture contains no abrupt transitions of intensity; thus indicating an image with little detail, and variation in colour. If we consider an observed GLCM which deviates from this diagonal uniformity, we intuitively expect

to observe images with more variability, and abrupt transitions in intensity; indicating, higher detail, and variation in colour, it is expected that a banknote image GLCM homogeneity should deviate considerably from the diagonal as banknotes typically incorporate complex intricate artwork. Though, often, the use of a dominant colour is employed for differentiation between denominations, it is often the case that there are many differing shades within the dominant colour.

Clearly, the key optimisation factor is the determination of the most suitable descriptive characteristics, those characteristics which contribute the most to the system's classification accuracy are identified as key characteristics; those which do not contribute effectively are deemed as redundant characteristics, and following future inference may be discarded. Primarily, we are interested in whether we need to implement both colour, and texture features together in the feature vector; this is determined by comparison of colour feature effectiveness, compared to texture feature effectiveness. As we look deeper into individual feature vectors, questions arise as to the effectiveness of individual characteristics. In total, eleven statistics are used as features, clearly, the question arises as to which features may be dropped to optimize algorithm performance, and accuracy.

Similarly, critical to ensuring optimal classification accuracy is dependent on ideal selection of classification algorithm. Considering the supervised learning paradigm initial pilot tests showed four possible solutions, namely: AdaBoost, Feedforward Neural Network (FNN), Cascade Forward Neural Network (CNN), and Pattern Recognition Feedforward Neural Network (PRFNN). The challenge arises, which of the aforementioned pattern recognition techniques gives optimal performance for implementation into the end system.

This system would not be complete without a comparison made between the input suspect banknote image, and that of a predefined known good template image. Forensic analysis regarding authenticity of banknotes requires an estimation

of confidence in similarity, therefore, selection of suitable methods for indicating to forensic investigators an estimation of similarity must be calculated, and finally presented as an output to the user.

3.4 HYPOTHESIS

During this thesis, certain comparisons must be made to determine the most suitable methods for use in the resulting system, currently, the system is designed as such: a banknote image is input, the image is: 1) classified, and 2) authenticated. There are two primary functions namely: 1) classification, and 2) authentication. Classification is imperative to determine the current banknote denomination under examination, once the note is classified it is then authenticated against a known good value in the database, and an estimation of similarity is output.

A series of hypotheses are formulated, first, the motivation is to determine which of the key characteristics is the most effective in contributing the most to overall classification accuracy; if there is no suitable performance by either colour features or texture features alone, a comparison must be made to identify the most important rotation of vector. Finally, analysis of individual key features within each of the two-part vector is necessary to verify individual characteristic effectiveness.

Subsequently, to optimise overall classifier effectiveness and accuracy it has been identified through review of similar applications, the most suitable colorspace for the intended application must be selected. The most prominent colour spaces examined during the literature review were: (1) red, green, and blue (RGB); (2) hue, saturation and intensity (HSI); and (3) Lab, Lightness, 'a' color-oponent value, and 'b' color-opponent value. Each colour space has intrinsic characteristics making it more suitable for use in certain scenarios, the colour space used for the feature extraction is a fundamental determining factor to the overall accuracy of classifi-

cation, and therefore must be tested and compared to find the most suitable one for use in this application.

A comparison between shortlisted candidate classifier, and pattern recognition methods must be made in order to verify suitable candidate classification, feature vector, and colorspace combination. The four shortlisted candidate classifiers are compared by direct side-by-side performance evaluation. Direct performance evaluation is conducted on the classifiers using identified key characteristics combination in section 3.4.1, the highest performing combination of characteristics is selected as the final shortlist, this will comprise the final feature vector used to train the four aforementioned classification algorithms, and then evaluation is performed by side-by-side comparison.

3.4.1 Feature selection

In order to test the effectiveness of this approach, a series of hypotheses have been formulated, to test the contribution of specific characteristics to the overall effectiveness of the classification module of the system. In each hypothesis, it is stated which aspect is to be tested, in particular each hypothesis is a slight modification of the original two-part colour and texture feature vector, whereby an individual element is removed to observe overall effectiveness.

First, the effectiveness comparison between colour and texture takes place in two stages, in the first stage, colour and texture are taken as two separate feature vectors and FNNs are trained accordingly. Secondly, the order in which the texture and feature vector is composed is compared; again, first with colour features first, and texture features second, and compared against the feature vector, composed of texture features first, and colour features second.

In addition to the comparison of texture features and colour features, it is also necessary to identify the key performing characteristics in the system, the key char-

acteristic features are also identified by a comparison process. Here we have a total of eleven feature characteristics, making up the colour and texture vectors. In the third scenario single characteristics are removed from the training set and the testing set, with the intention to observe the contribution of the characteristic to the overall effectiveness to classification accuracy. It is intended that once removed, each individual characteristic will influence the accuracy in which we will be able to identify how much or how little the accuracy has changed accordingly.

A total of five hypotheses are defined by the experimental phase of this thesis, namely:

1. **Hypothesis 1.0:** A feature vector comprised of both colour features, and texture features significantly improves the classification accuracy when applied to currency, where colour is used as a major differentiating feature between denominations .

2. **Alternative hypothesis 1.0:** A feature vector comprised of both colour features, and texture features does not show significant improvement of the classification accuracy when applied to currency, where colour is used as a major differentiating feature between denominations.

3. **Hypothesis 2.0:** Redundant, and non-ideal characteristic features exist in the feature vector, removal of redundant characteristics will improve overall accuracy.

4. **Alternative hypothesis 2.0:** Redundant, and non-ideal characteristic features exist in the feature vector, removal of redundant characteristics will not result in sufficient improvement in overall accuracy.

5. **Hypothesis 3.0:** The colour space used to extract the features influences the overall accuracy of the classification component of the system.

6. **Alternative hypothesis 3.0:** The colour space used to extract the features has no noticeable influence on the overall accuracy of the classification component of the system.

3.4.2 Feature selection

As mentioned previously in this section, initial pilot tests were conducted prior to the development phase to identify candidate classification, and pattern recognition machine learning algorithms suitable for use as classifier; based on observed literature. Initially, a trend observed during the literature review suggested potential candidate classification algorithms were the; SVM, PFRNN, CNN, FNN, AdaBoost, SOMs, and RadialBasis Networks. Following the literature, initial pilot tests were conducted to tentatively narrow down the selection, a shortlist was created of four, the; PFRNN, CNN, FNN, and AdaBoost methods were shortlisted based primarily on available resources and success of pilot tests, here success loosely refers to the cohesiveness, and ease of integration with other system modules.

Hereafter, to select the most suitable candidate, a performance comparison is made directly on trained classifiers using the highest performing combination of shortlisted key characteristics identified in section 3.4.1. A direct comparison is made, whereby, the identical testing set is used during a testing phase to compare accuracy. The classification method with the highest accuracy is selected as the final candidate for use in the classification, and banknote recognition module.

3.4.3 Template matching

A similarity measure is output to the user of the system, the similarity measure is obtained by a direct comparison of a representative pre-selected known good example template image for each denomination. A direct comparison is made between the template and suspect input banknote image, in performing the comparison a

calculation is made between the input vector, and the temple note vector. The calculation performed between the suspect note vector, and the template note vector is performed by usage of the inner product.

3.5 THE RESEARCH DESIGN

As indicated in section 3.3, the primary objective of this research project is to produce a prototype system to demonstrate with sufficient capability for banknote recognition, classification, and authentication; it is intended that this functionality primarily assist forensic investigations, and potentiality, currency security applications. Therefore, the research paradigm adopted by this thesis is the DSRM shown in figure Figure 3.1, the DSRM paradigm is a well established research methodology used to facilitate the design, and development of a useful artefact which solves a clearly defined problem (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008).

The DSRM paradigm loosely defines the overall structure which a project will follow, we may enter the process at any point within the lifecycle, and iterate accordingly, as needed. Initially, in this thesis, we begin with DSRM 1.0 Problem Identification & Motivation. Clearly, during initiation of this project we have demonstrated motivation to investigate the topic of digital currency forensics, and to provide a solution, through a preliminary literature review various enduring problems have surfaced primarily relating to the on-going arms race between, the currency issuing authorities, and counterfeiters, fuelled by continual technological advancements available to both parties.

Consequently, the primary problem has been defined, from a forensic investigation point of view, there is a gap in knowledge; binding knowledge of the top secret security printing industry, counterfeiters, and specialist trained sought after Questioned Document Examiners (QDEs), to formulate systematic, and methodological

investigative methods. From this, a tentative solution shown in figure Figure 3.1, has been formulated in which colour descriptor features, and texture descriptor features are concatenated to one single feature vector for classification, followed by similarity comparison measurement.

During the experimental phase, a collection of 171 banknote images was compiled, consisting of obverse and reverse sides from the \$5, \$10, \$20, \$50 and \$100 Reserve Bank of New Zealand (RBNZ) denominations. Predefined characteristics were identified as colour histogram shape descriptors: *mean*, *skew*, *variance*, *standard deviation*, *kurtosis* and *central moment*. The texture features *entropy*, and GLCM statistics *homogeneity*, *energy*, *contrast*, and *correlation* were extracted, and concatenated with the colour feature vector. The three most prominent colour spaces observed in the literature will be examined, and compared for classification accuracy; it has been observed in the literature, using specific channels of each colour space can provide significant improvement or reduction in classification accuracy depending on the application, and thus the channels within the colour space will be compared also.

To perform a comparison of the colour spaces observed in the literature, three have been shortlisted as the most prominent used throughout the literature, in similar applications. In particular the RGB, HSI and Lab colour spaces appear to be the most prominently used, and thus investigation of these colour spaces will be undertaken. For this, an experiment will be initiated where all eleven of the original colour, and texture features will be extracted from the banknotes; during each iteration of the experiment the variable colorspace will be changed. Through the characteristic colour, and texture extraction phase, the characteristics will be extracted as R, G, B, $((R + B + G)/3), HSI(I), L, a, b$. Secondly, classifiers will be trained to classify based on the respective colour spaces; hence, an observation will take place whereby the only variable changed is the colour space used during

each scenario, and results will be compared to find the scenario with the highest accuracy.

As mentioned in section 3.3, a primary objective of this thesis is the selection of optimal descriptive features, in order to select the optimal features: experiments will be conducted to identify the key features. Initially, four supervised learning algorithms were trained for the task of pattern recognition; firstly, an AdaBoost with 100 weak classifiers, then FNN, CNN, and PRFNN using Bayesian back propagation regulation learning. Experiments are undertaken in three primary phases: 1) where the accuracy of classification is recorded with removal of texture feature vector, and then removal of the colour feature vector for comparison of texture features compared against colour features; 2) removal of individual characteristics whilst recording the accuracy, the accuracy with individual feature removed determines how much the individual feature contributes to the overall performance; 3) once the suitable combination of features has been determined the classifier accuracy is compared, whereby all feature elements are considered, the only variable changed is the classifier used.

3.6 DATA REQUIREMENTS

Section 3.5, specifies that features for computational descriptive ability must be derived for the task of training machine learning algorithms to determine the most suitable classifier to be used in the end solution, otherwise known as the feature vector. Therefore, a selection of descriptive measures regarding the shape of the aforementioned intensity histogram shape have been shortlisted using the literature and initial pilot tests; as this thesis is considering the banknote image as a whole, a classifier must perform recognition purely on the captured image. The literature, and initial pilot tests have demonstrated that texture and colour features must be

used for computational description of images such as banknotes.

The primary data requirements are those descriptive statistics which make up the two-part colour, and texture feature vector. Here, a sample set of banknote images within a specific currency series must be compiled, in this case we are using the current currency series of the Reserve Bank of New Zealand; being that this is the current country this thesis is being undertaken within, however, it must be noted as in (García-Lamont et al., 2012) this same approach can be used for any currency series where colour is used to differentiate the individual denominations from one another.

Subsequently, as mentioned in section 3.5, the three most prominent colour spaces, and their channels will be examined to determine the most suitable colour space and channel for use in the application of recognition, for currency, where colour is a key discriminating factor. Primarily, we will obtain the RGB channels individually for comparison between individual channels, obtain an average value across all channels defining an intensity image data set, the *I* intensity channel from the HSI colour space will be used providing a data set of the *I* channel, the lightness, and 'a' color-oponent, and 'b' color-oponent channels of the Lab colour space will make up the rest of the colorspace dataset.

To determine the overall accuracy, it has previously been indicated in section 3.5 that the primary data or feature vectors will define the variables within the experimental phase, the feature vectors are modified in each scenario in order to perform comparisons between experiments. Resulting from the aforementioned experimental phase data will be collected, indicating the according performance level, a percentage level will be the primary indicating factor stating the observed accuracy, whence, each individual variable is removed from the feature vector thus indicating contributions to overall effectiveness..

3.7 LIMITATIONS OF RESEARCH

The primary limitation on this research project is that of the total amount of banknotes comprising the sample dataset, during a narrow window of time banknote images are to be collected from each of the five denominations on the RBNZ denominations $5, $10, $20, $50 and $100. The lower denominations from $5, $10 and $20 are the most commonly used denominations in every day transactions within New Zealand. The denominations $20, $50 and $100 are the most commonly to be issued by ATMs, a small proportion do however dispense the $10. The lower denominations $5 and $10 move around more frequently than the larger denominations, as the value of the denomination increases it is typically used less.

These factors limit this research in such a way that the variability of banknote wear and tear is not uniform across the denominations, meaning, in the lower denominations we will expect to observe a wider variability in captured image quality; whereas, in the higher denominations we will expect to observe quite uniform results, thus minimum variability. However, it could be argued: as this is data that is collected from real-world examples of banknotes in circulation that this limitation could in actuality be seen as a necessary factor to ensure that the digital currency forensics system is trained for typical real-world data, and thus trained for realistic events.

The fact that the circulation of currency decreases as the denomination value increases, there will clearly be less samples to work with as, thus, being that there are less samples to work with as the denominations increase there is consequently less data in which to train the classifiers, and to test later perform experiments to assess accuracy. Similarly, as it is expected that there will be less variation in observed descriptive statistics as the denominations increase, we may argue that any difference in individual denomination sample size may be inconsequential due to the fact that

this is also pertinent to the real-world, and thus any concern of discrepancy maybe seen as redundant as a result.

The solution proposed in this research is to evaluate the similarity of the suspect note in relation to the template note based on an inner product comparison, this comparison considers the image fidelity of the suspect compared to the template. The template image is a pre-selected image, based on a the choice of the system designers, the template image for each denomination is a randomly chosen sample out of a given set of known good samples. This sample is subjective, and representative of the entire database, however if an average were to be taken across the entire database of known good templates, it could be said that we are taking the average rather than specific comparison to one banknote image in particular. Clearly, the comparison made is subjective to the choice of template banknote, it could be argued that we know in advance that the randomly selected template image is known to be authentic and therefore is a good candidate, however it could also be argued that we must take an average across the entire data set of known good templates for each vector comparison. Therefore, it may be seen as a limitation in that we have decided to select a known good sample rather than using the average across the template dataset as the comparison values.

3.8 CONCLUSION

This research project on digital currency forensics uses the DSRM research paradigm to manage the overall structure of the project lifecycle, shown in figure Figure 3.1. The DSRM is a well established research methodology which used to facilitate the development of an artefact that is needed to solve a problem, the DSRM is well suited to projects where the solution outcome can not be clearly defined at the initial moment of problem conception.

Initially, it was identified that the process of forensic investigation regarding the analysis of questioned currency is dependent on the usage of specialist trained QDEs; such experts are highly sought after thus analysis is based on their availability. It was also identified that the continual technological advancements available to both the currency manufactures and the currency counterfeiters is constant. Therefore, there is an incessant arms race between those designing, developing, and manufacturing currency, and those who fraudulently reproduce and pass banknote replicas.

The primary issue noted is that the process of analysis is based on human evaluation, and is therefore subject to human error, it was also identified that to be fully robust, any forensic analysis process must be both methodological and systematic meaning that it must be repeatable and verifiable. Clearly, a process which is entirely reliant on manual labor is subject to human error, and dispute between potential opposing experts, therefore, it has been identified that an automated digital currency forensics system would satisfy the aforementioned requirements.

Primarily, as such a system is automated we can ensure that the process will be systematic and repeatable, therefore, if an investigation required forensic analysis of currency, we could ensure similarity between results from both opposing sides with any discrepancy being due to the prior acquisition process. Secondly, as this is an automated system we can verify its methodological approach to analysis, the analysis process is as such performed computationally by an algorithm thus repeating the same process for each banknote in question. Therefore, this process follows a tested method throughout the study of this thesis and is open to peer review for future improvement.

In particular, the aforementioned process can be loosely summarised as such: a pre-acquired banknote of an arbitrary size is input to the system. The banknote is converted from the raw RGB colorspace to an equally weighted average of the RGB

channels, otherwise referred to as the intensity channel, thus, giving an intensity image representing the intensity of colour. Computationally, the intensity image is a Cartesian based array storing values in the (x, y) coordinate system, particularly as 640×312, representing one individual array element for each individual pixel, each pixel, thus, has a grey-level intensity level assigned.

To determine ideal colour space for acquisition the RGB, HSI and Lab, colour spaces will be compared whereby a process of identical comparison will take place, a direct comparison where the successful and unsuccessful classifications will be recorded. The colour space which achieves the highest level of accuracy will be determined to the the final candidate for selection in the end system, in particular we have shortlisted the RGB, HSI and Lab colour spaces as they are the most prominently used throughout the literature.

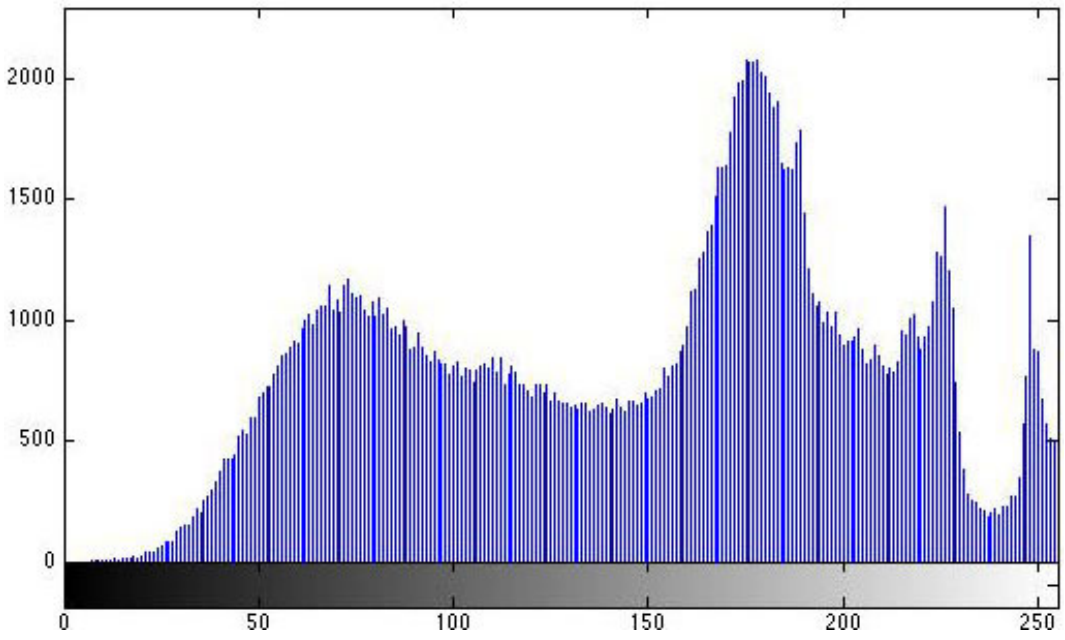
From the resulting banknote array, we will take two primary forms of characteristics: the colour characteristics and the texture characteristics, colour refers to the characteristics of the dominant colours of the observed banknote, texture refers to the characteristic nature of the occurrence of the observed colours adjacent to other colours observed. The approach employed in this study is to calculate an intensity image histogram of the captured image, and deriving shape descriptors as measurements in the colour feature vector. It was demonstrated that each denomination should produce a telltale shaped histogram, and thus using shape descriptors for comparison is a computationally sound method. To describe the texture features, the GLCM is calculated with adjacent pixels by an offset of 0, and 1 ,where the direct, neighbouring pixels are analysed. Clearly, the key features for both the colour features, and texture features are the defining determination factor for both classification, and authentication phase; the best fit must be selected, for this an experiment will take place whereby the texture features and colour features will be first compared against each other, and then analysis of the individual features'

contribution to the overall system.

Similarly, the most prominent classifiers throughout the literature will be evaluated, it was noted in the literature that the *AdaBoost, PNN, CNN, SVM, FNN, PRFNN* classifiers were the most commonly used and therefore are the shortlisted candidates. The classification step is a necessary step in the forensic analysis process, as to make a fully automated system we need a system which is capable of identifying the denomination its self without human intervention. This is because the end implementation, is, at this point unknown, for best performance no human intervention must take place, and therefore classification is necessary. It is widely known that certain classifiers will perform differently under different circumstances, and thus, it is imperative to select the most suitable one for any application where such is required.

Finally, after the template database has been established, feature vectors have been extracted and defined, and template known good banknotes have been selected, a direct comparison will take place. The direct comparison is performed by the pre-selection of the known good value for the banknote denominations, a feature vector is extracted, and defined, a direct comparison takes place by calculating an inner product calculation for comparison.

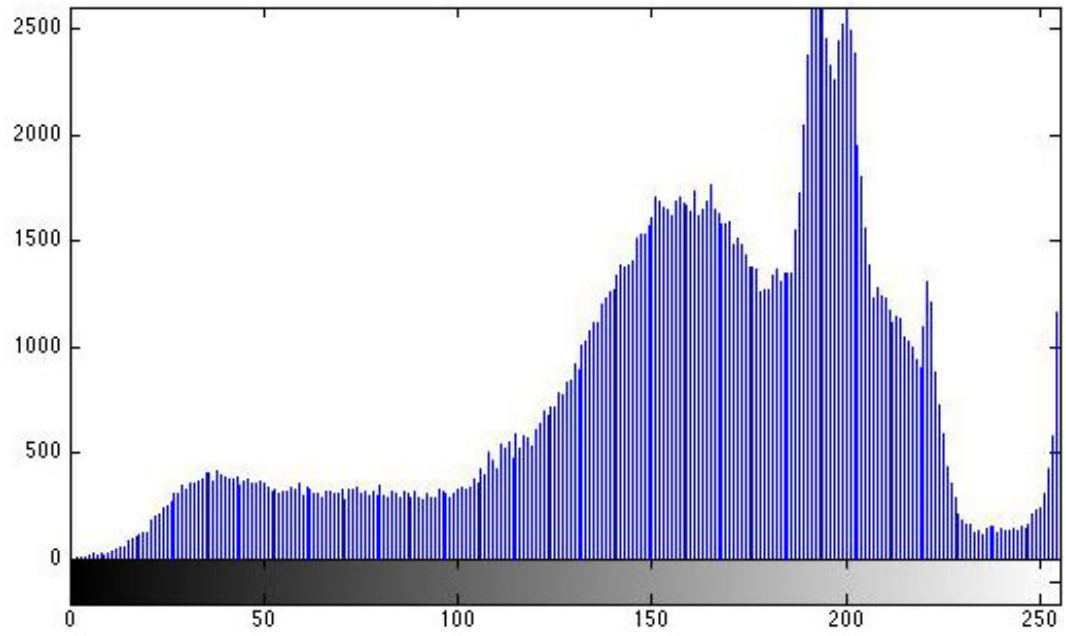
(a)



(b)

Figure 3.5: Gray level histogram. (a) gray-level RBNZ $100 banknote image, and (b) the gray-level histogram calculated.

(a)



(b)

Figure 3.6: Grey level histogram. (a) grey-level RBNZ $10 banknote image, and (b) the grey-level histogram calculated.

Chapter 4

Findings

4.1 APPROACH

The approach in this thesis is to use a combination of image processing, and classification techniques to identify banknote denomination by colour, and texture features. Banknote recognition, and denomination identification is made possible by extracting computable features for describing colour, and the texture of acquired banknotes, then, classifying against a database of learned known good template images. Once the banknote has been identified, and classified, a similarity measurement is calculated and output for side-by-side comparison.

To test the algorithm proposed by this thesis, a number of comparisons were undertaken to identify the most suitable feature vector, classifier, and colorspace combination. From this point forward, various tables are presented demonstrating the accuracy of each scenario in percentage values, collected during the data collection phase. Please note, for presentation purposes, some key information has been truncated, and where information has been truncated, an explanation is present. For example, experiments were conducted, comparing the direct accuracy from one scenario versus another, identical samples were used for comparison; in

this case, identical side and denomination, $5 Front represents one class comprising all selected samples within that class. For example: $5 Front, $5 Back, $10 Front, $10 Back, $20 Front, $20 Back, $50 Front, $50 Back, $100 Front, and $100 Back; will be truncated to: $5 F, $5 B, $10 F, $10 B, $20 F, $20 B, $50 F, $50 B, $100 F, and $100 B; representing the front and back sides of the note, and thus all samples of that type within the respective class.

4.1.1 Pre-processing

Initially, pilot tests were conducted to investigate the potential accuracy of the most prominent colour spaces observed throughout the literature, following this: RGB, HSI, and Lab colour spaces were shortlisted as final candidates. As shown in table Table 4.1, the intensity or grey-level, which in this thesis is the combined average of the R, G, and B channels, weighted equally, is found to provide the highest level of accuracy. It was observed, that when performing the classification task across all possible denominations combined, an accuracy totaling 97.66% occurs under the conditions of this experiment; as expected, the variability primarily appears to occur within the lower denominations. Interestingly, the R, and G channels provide the next best performance, at 28.65%, and 27.49% respectively. Clearly, the combined grey-level of the RGB colour space is the most suitable candidate, and in conclusion, the digital currency forensics system will use the the grey-level, or grey-world algorithm.

Please note, in the following table the colorspace components have been abbreviated for display purposes. The HSI Intensity is shown as 'HSI(I)', Lab Lightness is shown as 'Lab(L)', the 'a' and 'b' color-opponent values of Lab are Lab(a), and Lab(b) respectively. The color components of the RGB color space have been separated to 'RGB(R)', 'RGB(Green)', and 'RGB(Blue)', and averaged to Grey 'RGB/3' with equal weightings. Equal weightings were used for the color inten-

sity calculation. The motivation for using an equal weighting, RGB, to intensity level conversion scheme, is purely to perform a direct comparison between the RGB, HSI, and Lab color spaces, with the intention to identify the most suitable color space. The results in this thesis show RGB intensity is the most accurate for this application, and thus, it is concluded RGB intensity is the successful candidate. It is noteworthy, that there is potential for expanding this aspect of research, to conduct further exploration into accuracy; by altering the scope to restrict experiments to R,G,B to intensity conversion weightings, and then conducting experiments with the intention to observe accuracy under specific conversion to intensity level weightings.

Table 4.1: Colour space channel performance and comparison.

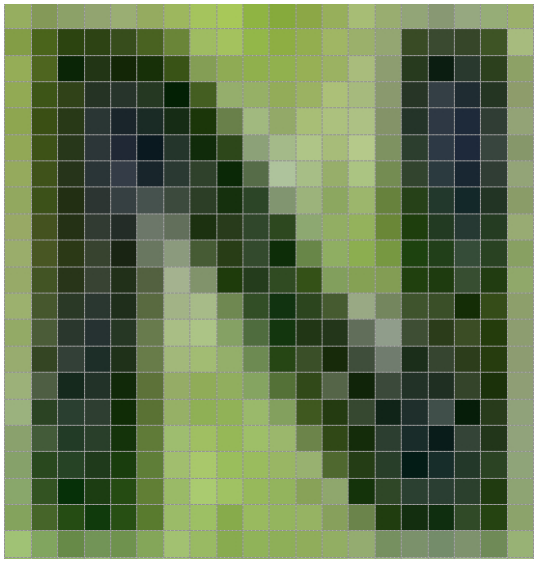
	HSI(I)	**Lab(L)**	**Lab(a)**	**Lab(b)**	**RGB(B)**	**RGB/3**	**RGB(G)**	**RGB(R)**
$5 Front	5.26%	0.00%	15.79%	0.00%	0.00%	100.00%	21.05%	0.00%
$5 Back	0.00%	0.00%	0.00%	0.00%	0.00%	94.74%	21.05%	0.00%
$10 Front	5.56%	0.00%	55.56%	50.00%	50.00%	94.44%	11.11%	0.00%
$10 Back	44.44%	0.00%	0.00%	0.00%	0.00%	100.00%	38.89%	77.78%
$20 Front	68.42%	31.58%	0.00%	0.00%	0.00%	94.74%	78.95%	21.05%
$20 Back	5.56%	0.00%	0.00%	0.00%	0.00%	94.44%	0.00%	83.33%
$50 Front	0.00%	31.25%	0.00%	0.00%	0.00%	100.00%	6.25%	0.00%
$50 Back	43.75%	100.00%	87.50%	0.00%	0.00%	100.00%	75.00%	25.00%
$100 Front	0.00%	0.00%	0.00%	0.00%	7.14%	100.00%	0.00%	0.00%
$100 Back	7.14%	0.00%	0.00%	28.57%	28.57%	100.00%	14.29%	85.71%
Total	**18.72%**	**15.79%**	**15.79%**	**7.60%**	**8.19%**	**97.66%**	**27.49%**	**28.65%**

To conclude the results shown in table Table 4.1, the average of the *RGB* colorspace grey-level provides the highest accuracy to extract the colour features from captured banknote images. To reduce complexity for later computational requirements, the image is pre-processed, the image is preprocessed in two ways: firstly,

it is rescaled from an arbitrary size, to a uniform size of 640×312 pixels. Secondly, as the raw input image is in the *RGB* colour space, the data in actuality is calculated as $640 \times 312 \times 3$, there is 640×312 for each of the individual R, G, and B channels; by using the grey-world algorithm, the amount, and the complexity of data is greatly reduced, and also differences in illumination during the acquisition process is minimised.

The grey-world theory is such, an image with variations in colour can be reduced to a single grey level value. Obtaining the average of the R, G, and B channels of an image should result in a common value across a set of samples with exact imagery; thus, given a set of images with the same scene, such a banknote denomination, similar grey level values from one sample to the next should result. Banknotes within any currency issue must have uniform imagery, excepting of course the serial number, henceforth as the serial number is a minor discrepancy between individual banknotes it can be said that the grey-world theory is sufficient for banknote classification and can be verified by observing the results shown in table Table 4.1.

As previously mentioned, each of the RGB channels from the acquired banknote image are represented separately as three individual arrays, each arrary consisting of 640×312, as shown in figure Figure 4.2, with each array element storing the R, G, and B, colour component respectively. Each element stores a value between 0, to 255, representing the respective colour component's contribution to the colour at that pixel location. For instance, if we take an arbitrary location of the RBNZ $20 obverse side shown in figure Figure 4.1, the letter 'N' of the word 'New Zealand' has been selected, the individual pixels are shown as squares in a grid formation, as retrieved by analysis with the MATLAB image processing toolbox for illustrative purposes.



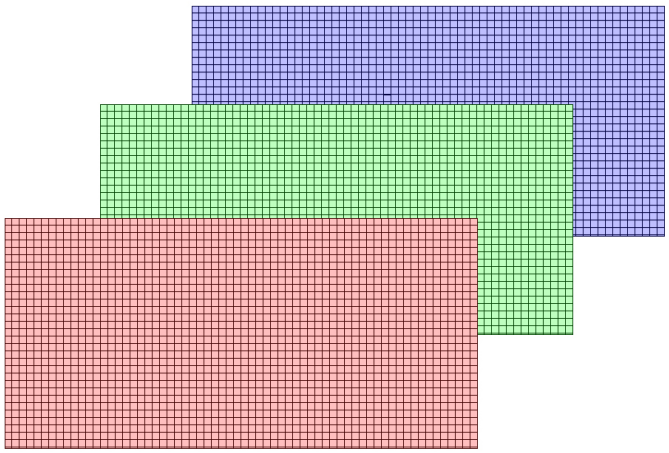
(a)

R: 60 G: 83 B: 5	R: 34 G: 54 B: 0	R: 36 G: 53 B: 8	R: 43 G: 63 B: 14	R: 58 G: 81 B: 13	R: 89 G:117 B: 30	R:144 G:178 B: 66	R:149 G:185 B: 59
R: 62 G: 84 B: 11	R: 11 G: 29 B: 0	R: 27 G: 42 B: 13	R: 16 G: 30 B: 4	R: 19 G: 37 B: 0	R: 44 G: 66 B: 2	R:116 G:144 B: 57	R:126 G:159 B: 52
R: 48 G: 69 B: 0	R: 37 G: 52 B: 13	R: 28 G: 39 B: 25	R: 29 G: 40 B: 32	R: 28 G: 43 B: 24	R: 7 G: 25 B: 0	R: 54 G: 78 B: 16	R:132 G:161 B: 79
R: 45 G: 64 B: 0	R: 31 G: 44 B: 14	R: 32 G: 41 B: 38	R: 20 G: 27 B: 33	R: 21 G: 32 B: 28	R: 19 G: 34 B: 15	R: 22 G: 43 B: 0	R: 87 G:111 B: 51
R: 48 G: 66 B: 6	R: 30 G: 43 B: 17	R: 33 G: 41 B: 43	R: 24 G: 30 B: 42	R: 11 G: 20 B: 25	R: 28 G: 41 B: 32	R: 14 G: 33 B: 5	R: 35 G: 56 B: 15
R: 49 G: 66 B: 11	R: 29 G: 41 B: 17	R: 32 G: 40 B: 42	R: 39 G: 45 B: 57	R: 19 G: 28 B: 33	R: 33 G: 44 B: 38	R: 36 G: 51 B: 30	R: 12 G: 31 B: 1

(b)

Figure 4.1: Pixel values. (a) an arbitrary location, the letter ‘N’ is selected on the RBNZ $20 obverse; (b) the area shown in (a) magnified showing the individual pixel location.

(a)



(b)

Figure 4.2: RGB Channel separation. (a) RBNZ $20 banknote obverse before conversion separated into three individual channels for each of the R, G, and B channels; (b) RBNZ $20 banknote, computationally, the individual colour spaces are represented as individual R, G, and B arrays, of 640×312 pixel colour values.

The reduced channel I, is now one single array of 640×312, consisting only of the grey-scale intensity values, shown in figure Figure 4.3. From hereon in, all image classification, comparison, and authentication procedures will be performed on this newly created grey-level array representing the original colour image. To conclude, RGB, to grey-scale conversion is a process, whereby, the RGB components are averaged, significantly reducing data complexity, whilst, also minimising the illumination effect, resultant of, different lighting conditions during the acquisition of banknote images.

It has been stated, that where images consist of variations in colour, the same, or similar, average values represent the different levels of colour from the RGB color space, from the range, 0, to, 255. Initial tests have shown, the RGB colorspace provides the best performance when applied to the data set used in this thesis, 'RBNZ banknotes', providing a significant performance increase over HSI, and Lab, the other prominent colorspaces explored in literature. Therefore, it is concluded, the RBG intensity image gives the most accurate results for the application of digital currency forensics, and is the colour space adopted by this thesis.

(a)

(b)

Figure 4.3: RGB to grayscale conversion. (a) original RBNZ $20 banknote before conversion, (b) RBNZ $20 banknote grey-level intensity image after averaging the R, G, and B colour space channels.

4.1.2 Feature extraction

Grey-levels are obtained from the intensity image array described in section 4.1.1, as stated, this is an array of 640×312 pixels, two sub-categories of features are extracted, calculated, and extracted to form a colour feature vector. Firstly, colour features are extracted, a grey-level histogram is calculated with 256 bins describing the frequency of dark to light colour. From this histogram, six shape descriptor metrics are obtained: (1) *kurtosis*, (2) *central moment*, (3) *mean*, (4) *variance*, (5) *standard deviation*, and (6) *skew*; for further information refer back to section 3.3.

Secondly, five texture features are extracted, the entropy level is calculated along with four features from the grey-level co-occurrence matrix (GLCM), namely: *correlation*, *contrast*, *energy*, and *homogeneity*. Together, the colour features, and texture features are concatenated into a single feature vector, which is input into a classifier.

The feature vector obtained in the feature extraction step is directly input as a scalar to a FNN classifier, as shown in figure Figure 4.5. A, to K, represent the 11 individual characteristics (input scalar), 30 hidden nodes, and 10 output classes from \$5, to \$100, front and back, representing the possible classes.

The grayscale image histogram is then calculated consisting of 256 bins, shape descriptors are then used as part of a two-part feature vector. We take the *kurtosis*, *central moment*, *mean*, *variance*, *standard deviation*, and *skew* shown in figure Figure 4.4. The second part of the feature vector is computed from the texture features. First, the entropy is calculated, then the grey-level co-occurrence matrix (GLCM) *contrast*, *correlation*, *energy*, *homogeneity*.

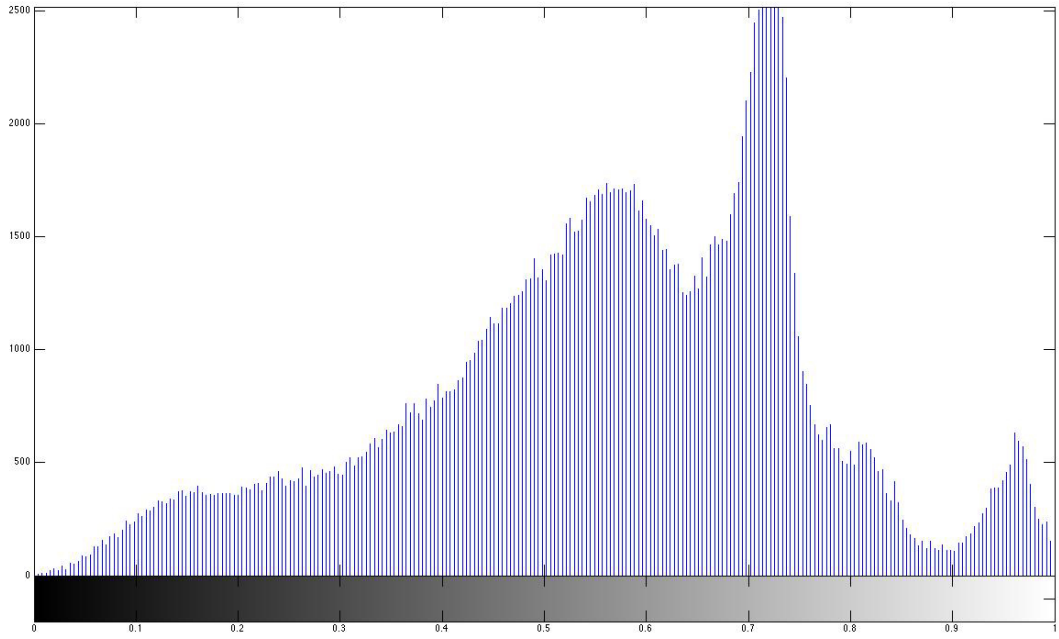


Figure 4.4: Grayscale level histogram showing the occurrence of grey-level values in the example image.

4.1.3 Classification

The note is then classified into its respective denomination, back, or front side. The FNN was trained using Bayesian regulation back-propagation, Bayesian regulation back-propagation can train any network where the weight, input, and transfer functions have derivative functions. Training stops when any of the following conditions occur: maximum epoch is reached; a maximum time is reached; goal performance is reached; or the performance gradient falls below a minimum gradient level (MacKay, 1992). Initial pilot tests were conducted, it was concluded *AdaBoost*, *Pattern Recognition trained Feed forward Neural Network (PRFNN)*, *Cascade forward Neural Network (CNN)*, and *FNN* were suitable candidates.

The FNN was trained using $f(x) = \Sigma w_i N_i(x)$, x is the input vector, w_i is the weight at vector i. The training set is defined as $T = (t_i, \ldots, t_n)$, and weights initialised $w' = (w'_1, \ldots, w'_n)$. Testing starts from: $f(x) = \Sigma w'_i N_i(x)$.

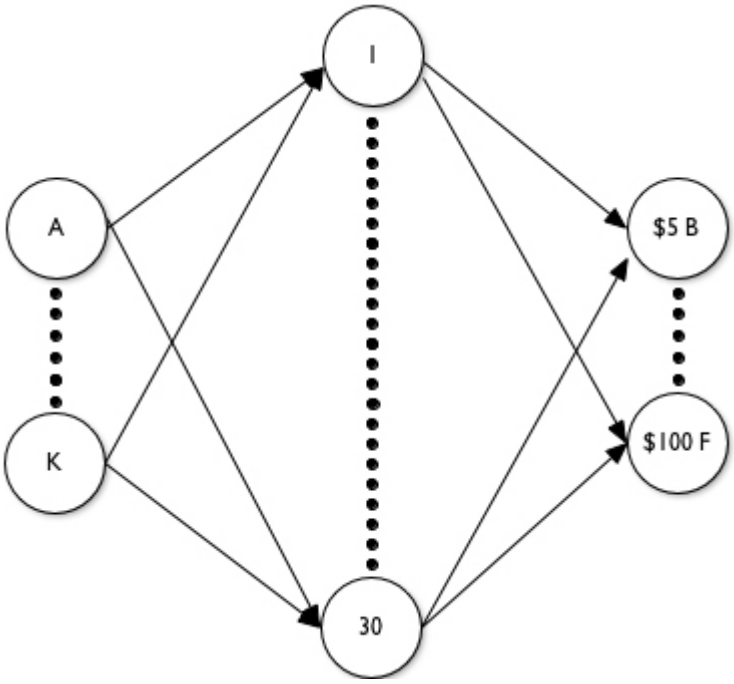


Figure 4.5: Currency forensics FNN structure.

4.1.4 Authentication

Currency forensics is the measurement of similarity or dissimilarity based on a comparison between suspect note, and template. When a note in question does not meet the required threshold it is not authentic. To analyse a note, the note must be compared against known good values. An initial database consisting of 171 template banknote images was compiled. This database is comprised of obverse and reverse sides of the banknote denominations. Once the denomination has been determined, the feature vector from the suspect note is then compared against a vector from the template database using the inner product of the two vectors.

The algorithm for the digital currency forensics system is shown in the algorithm (1).

input : Test image.

output: Classification of banknotes and similarities.

Procedure:

Step 1 Normalisation of the input image;

Resize the banknote image to 312×640;

Histogram equalisation;

Step 2 Extract features from the grayscale image;

Calculate Histogram Features;

Calculate Entropy;

Calculate GLCM;

Step 4 Classify the test image using the classifiers;

Step 5 Measure similarities.

Algorithm 1: Banknote classification & similarity measurement.

$$S = \frac{v \cdot u}{\|v\|_2 \|u\|_2} \times 100\% \tag{4.1}$$

where *S* is the measure of similarity, *V* represents the suspect note vector, and *U* represents the template note vector. We take the suspect note vector:

$$A = U^H \cdot U \tag{4.2}$$

$$B = V^H \cdot V \tag{4.3}$$

$$|\lambda I - A| = 0 \tag{4.4}$$

$$|\lambda' I - B| = 0 \tag{4.5}$$

$$\lambda_{\text{max}} = max(\lambda_1, \lambda_2, \ldots, \lambda_n) \tag{4.6}$$

$$\lambda'_{\text{max}} = max(\lambda'_1, \lambda'_2, \ldots, \lambda'_u) \tag{4.7}$$

and obtain the spectral norm of *v*, and *u* respectively:

$$\|U\|_2 = \sqrt{\lambda_{\text{max}}} \tag{4.8}$$

$$\|V\|_2 = \sqrt{\lambda'_{\text{max}}} \tag{4.9}$$

4.2 EXPERIMENTS

4.2.1 Experiments settings

The currency forensics system shown in figure Figure 4.6, has been prototyped in the MATLAB environment running under the Apple Mac OSX Lion platform. A second experiment was performed, 11 FNN networks were trained, each using the feature vector minus one characteristic. The intention was to determine the level of accuracy upon removing a particular characteristic, therefore, determining each characteristic's contributing effectiveness.

4.2.2 Data collection

During the initial training phase, a database was compiled consisting of 171 banknote images. The database includes 19 $5 obverse, 19 $5 reverse, 18 $10 obverse, 18 $10 reverse, 19 $20 obverse, 18 $20 reverse, 16 $50 obverse, 16 $50 reverse, 14 $100 obverse, and 14 $100 reverse. Samples were collected from a number of sources: Brother Professional Series Multi-Function Centre MFC-J6910DW; Hewlett Packard HP PSC 1410 All-in-One Printer; and a Canon PIXMA MP150.

Notes of the lower denominations make up a higher proportion, as these banknotes are both more abundant, and frequently used, the variation in quality is higher in the lower denominations. Notes were obtained under varying conditions,

providing a mix of quality and lighting. An arbitrary database subset was compiled consisting of 10 notes from each sub-category, selected at random. The subcategories are used as the training set, with a total of 100 sample notes for training, leaving the remaining 71 for testing.

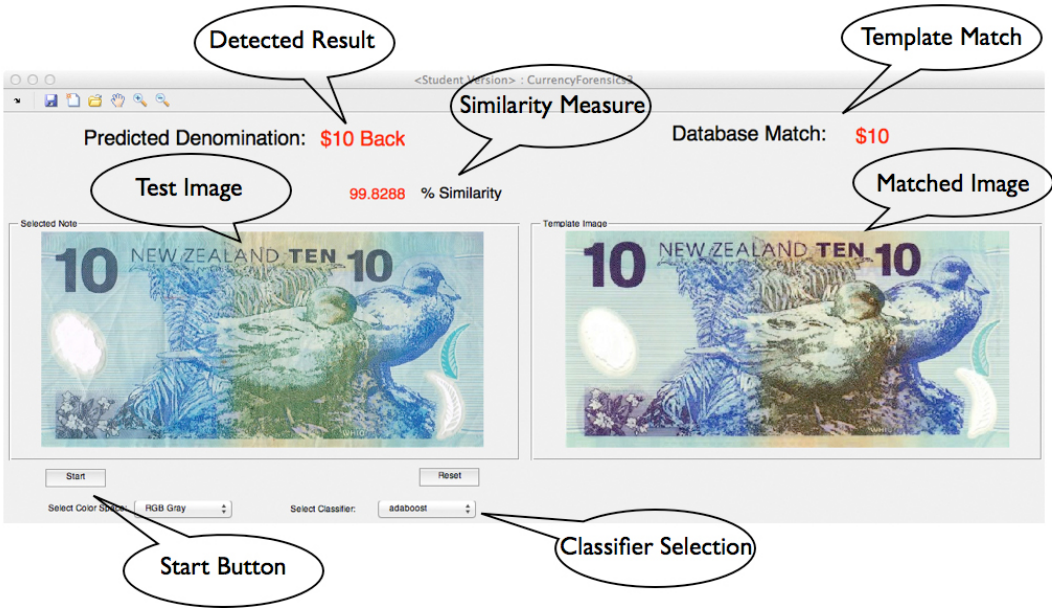


Figure 4.6: Interface of prototype currency forensics system.

4.2.3 Prototype

As shown in figure Figure 4.6, a prototype currency forensics system has been developed. The prototype allows the forensic investigator to perform side-by-side comparisons. Once the note has been classified, the forensic investigator is provided with a level of similarity. CNN, PRFNN, and FNN classifiers were trained using supervised learning by the Bayesian regulation back-propagation training function, and an AdaBoost classifier.

4.2.4 Results

When classifying notes against the FNN classifier, we a achieved a 92.40% accuracy rate on recall from outside of the training set, shown in table Table 4.2. Compared with the Adaboost 58.48%, PRFNN 91.23%, and CNN 90.06%, it is concluded that when considering all variables of this thesis, the FNN classifier gives the highest accuracy. Notes within the training set, match to the pre-selected template image vector within the range of 99.44% - 99.99% for the output similarity measurement.

With removal of unusual outliers, which at this stage we can surmise may potentially originate from samples collected at an unusual rotation. This is tentatively surmised, as a similar amount of captured images appear to show a border of white pixels around the edges compensating for the rotation, which was added by the scanning process, as shown in figure Figure 4.7. In this example, the black border has been used for illustrative purposes highlighting the significance of the additional border of completely white pixels. By potentially limiting observations to captured images of similar alignment, we achieved a 98.60% accuracy rate with FNN, Adaboost 53.00%, PRFNN 95.70%, and CNN 94.30%.

4.2.5 Experimental analysis

4.2.5.1 Feature analysis

A two-part feature vector was compiled, the feature vector is made of 6 histogram shape descriptors, and 5 texture descriptors. To describe the shape of the grey-level histogram obtained, we have used the *central moment*, *kurtosis*, *mean*, *standard deviation*, *skew*, and *variance*. To describe the texture of the resulting grey-level image, we calculated the *entropy* value, and, the *contrast*, *correlation*, *energy*, and *homogeneity* from the GLCM.

Figure 4.7: Example of sample banknote image collected at an unusual rotation, a white border appears to be present compensating for the rotation.

It is concluded from the results shown in table Table 4.4, variance is the least effective characteristic showing the lowest level of misclassifications when removed. *Central moment*, *contrast*, *correlation*, *energy*, *entropy*, *homogeneity*, *kurtosis*, *mean*, *skew*, and *standard deviation* contribute substantially to the overall effectiveness, as a high misclassification rate is observed when these descriptors are removed.

4.2.5.2 Classifier analysis

Four classifiers were trained and compared in this thesis, namely, a PRFNN, FNN, CNN and an AdaBoost classifier. In total, there were 171 sample banknote images, 100 images from each side of each denomination were used as the training set. The following accuracy measurements shown in table Table 4.4 were obtained when testing on the remaining 71 images. The results show, that under the conditions of this experiment, the FNN shows optimal performance at 92.40% accuracy when classifying outside of the training set, whereas AdaBoost achieves 58.48%, PRFNN 91.23%, and CNN 90.06%, respectively.

Table 4.2: Classifier comparison showing the percentages of correct classifications.

	Adboost	**PRFNN**	**CNN**	**FNN**
$5 Front	73.68%	89.47%	89.47%	89.47%
$5 Back	0.00%	84.21%	89.47%	84.21%
$10 Front	94.44%	100.00%	100.00%	100.00%
$10 Back	83.33%	88.89%	88.89%	88.89%
$20 Front	78.95%	94.74%	72.22%	94.74%
$20 Back	88.89%	100.00%	94.44%	94.44%
$50 Front	0.00%	81.25%	100.00%	87.50%
$50 Back	0.00%	81.25%	93.75%	93.75%
$100 Front	64.29%	92.86%	87.71%	100.00%
$100 Back	100.00%	100.00%	92.86%	92.86%
Totals	**58.48%**	**91.23%**	**90.06%**	**92.40%**

Table 4.3: Confusion matrix showing accuracy of FNN on the dataset, please note F, and B, represent the front, and back, of the note respectively.

		Predicted									
		$5 F	**$5 B**	**$10 F**	**$10 B**	**$20 F**	**$20 B**	**$50 F**	**$50 B**	**$100 F**	**$100 B**
Actual	**$5 F**	17	1	-	-	-	-	-	-	-	-
	$5 B	-	16	-	-	-	-	-	-	-	-
	$10 F	-	-	18	-	-	-	-	-	-	-
	$10 B	-	-	-	16	-	-	-	-	-	-
	$20 F	1	1	-	1	18	-	2	1	-	-
	$20 B	-	-	-	-	-	17	-	-	-	-
	$50 F	1	-	-	-	-	-	14	-	-	-
	$50 B	-	-	-	1	-	-	-	15	-	-
	$100 F	-	-	-	-	1	1	-	-	14	-
	$100 B	-	1	-	-	-	-	-	-	-	13

Table 4.4: Characteristic comparison, showing percentage of incorrect classifications with removal of characteristic, information has been truncated for display purposes, F, and B represent front, and back of the note respectively.

	$5 F	**$5 B**	**$10 F**	**$10 B**	**$20 F**	**$20 B**	**$50 F**	**$50 B**	**$100 F**	**$100 B**	**Total**
Central Moment	66%	77%	75%	100%	87%	88%	100%	88%	75%	100%	**82%**
Contrast	66%	88%	75%	87%	75%	88%	100%	83%	75%	75%	**81%**
Correlation	55%	66%	75%	100%	87%	66%	80%	83%	50%	75%	**74%**
Energy	55%	88%	75%	87%	75%	77%	60%	66%	75%	75%	**74%**
Entropy	77%	66%	75%	62%	87%	66%	80%	83%	75%	75%	**74%**
Homogeneity	66%	77%	75%	75%	87%	77%	60%	66%	75%	75%	**74%**
Kurtosis	66%	66%	37%	62%	87%	66%	80%	66%	75%	75%	**67%**
Mean	66%	66%	62%	100%	100%	77%	100%	50%	75%	75%	**77%**
Skewness	77%	77%	75%	75%	87%	77%	40%	83%	75%	75%	**74%**
Standard Deviation	66%	55%	62%	87%	87%	77%	80%	83%	50%	100%	**74%**
Variance	0%	0%	0%	0%	0%	0%	40%	0 %	25%	0%	**4%**

As shown in table Table 4.5, colour features, and texture features appear in this scenario, when applied to banknotes, where colour is used as a major differentiating feature between different denominations, to be suitable descriptors. It is interesting to note that the particular combination of colour, and texture features used in this thesis appear to both provide similar weightings, and discriminability to overall accuracy. It appears that the combination of the texture and colour features do influence the overall performance where colour appears to provide slightly higher accuracy when placed in the feature vector before the texture features.

Table 4.5: Classification results using the training set.

Scenario	Training Set	Testing Set	Combined Total
Texture Only	95.00%	64.79%	**82.46%**
Color Only	98.00%	60.56%	**82.46%**
Color FIrst	98.00%	70.42%	**86.55%**
Texture First	98.00%	73.24%	**87.72%**
WIthout Central Moment	100.00%	81.69%	**92.40%**
WIthout Contrast	97.00%	81.69%	**90.64%**
WIthout Correlation	96.00%	71.83%	**85.96%**
WIthout Energy	98.00%	73.24%	**87.72%**
Without Entropy	96.00%	74.65%	**87.13%**
Without Homogeneity	100.00%	73.24%	**88.89%**
Without Kurtosis	100.00%	64.79%	**85.38%**
Without Mean	96.00%	73.24%	**86.55%**
Without Skew	99.00%	73.24%	**88.30%**
Without Standard Deviation	99.00%	74.65%	**88.89%**
Without Variance	98.00%	71.83%	**87.13%**

Chapter 5

Discussion

5.1 REFLECTION

A digital currency forensic method has been defined, an authentication method has been formulated based on classification of currency notes using intrinsic colour, and texture features, followed by template matching. Template matching is conducted using the inner product of the suspect banknote, and a known good template banknote image. This gives the forensic investigator a level of confidence, indicating the measure of similarity as a percentage for suspect banknote images, against known good images within a template database. Experiments have been conducted to assess the accuracy of candidate features, and classifiers, the results suggest that a suitable framework has been constructed.

There are remaining areas of interest to be explored, currently we have explored the relationships between colour, and texture features when applied to classification of New Zealand banknotes; final tests show that the classification accuracy has been able to be increased from 82.46%, to, 92.40%, and then, 98.60%. The first increase was observed during an experimental phase, whereby individual characteristics were removed from the feature vectors to observe the accuracy of each. It

was found that both the central moment, and the contrast contribute the least to the overall discriminability, and the final increase was achieved with the removal of unusual outliers.

Therefore, the central moment within the feature vector is removed, and we are left with a feature vector containing five colour descriptors, and five texture descriptors. Therefore, the final feature vector is comprised of the colour features: *mean*, *skew*, *standard deviation*, *variance*, and *kurtosis*; and texture features: *homogeneity*, *correlation*, *contrast*, *energy*, and *entropy*. Based on the findings shown in table Table 4.5, this two part feature vector appears to be sufficient in providing approximately 92.40% accuracy.

5.2 EVALUATION

Evaluation of this proposed method is primarily based on classifier accuracy, and the similarity measurement of suspect banknote when compared against the template banknote. Consequently, in section 3, specific hypotheses were defined stating determining factors relating to the final selection of characteristic descriptors, the key descriptors are fundamental to classification accuracy. Therefore, the hypotheses of this thesis focus primarily on key characteristic feature selection.

In the following, an analysis of the accuracy of each characteristic will be evaluated, and related back to the initial hypotheses defined in section 3:

1. **Hypothesis 1.0:** A feature vector comprised of both colour features, and texture features significantly improves the classification accuracy when applied to currency, where colour is used as a major differentiating feature between denominations .

2. **Alternative hypothesis 1.0:** A feature vector comprised of both colour features, and texture features does not show significant improvement of the clas-

sification accuracy when applied to currency, where colour is used as a major differentiating feature between denominations.

3. **Hypothesis 2.0:** Redundant, and non-ideal characteristic features exist in the feature vector, removal of redundant characteristics will improve overall accuracy.

4. **Alternative hypothesis 2.0:** Redundant, and non-ideal characteristic features exist in the feature vector, removal of redundant characteristics will not result in sufficient improvement in overall accuracy.

5. **Hypothesis 3.0:** The colour space used to extract the features influences the overall accuracy of the classification component of the system.

6. **Alternative hypothesis 3.0:** The colour space used to extract the features has no noticeable influence on the overall accuracy of the classification component of the system.

Hypothesis 1.0, and, 2.0, regard the outcome of classifier accuracy when using either colour, or texture features, from the results in table Table 4.5, and table Table 4.4, considerably similar accuracy is contributed to the overall accuracy. Consequently, it is interesting to note, classification accuracy during the experimental phase concluded that we can obtain more, or less, the same results when using either colour, or texture. Similarly, when concatenating colour, and feature vectors together, we observe a slight increase in accuracy, from 86.55%, to, 87.72% when the order of concatenation is texture and colour, compared against colour and texture, respectively. Therefore, we can conclude; when considering all variables present in this thesis, the order of the characteristics in the feature vector does influence the accuracy of the digital currency forensics system.

5.3 JUSTIFICATION

To justify the proposed solution for digital currency forensics, a prototype has been formulated, and developed in the MATLAB programming environment using the image processing, and neural network toolboxes to demonstrate the applicability of this solution. The system is capable of 92.40% accuracy when applied to the current data set used within this thesis, results have been tabulated similarly for comparison of classifier against determined suitable candidate classifiers observed in the literature.

The following percentages, are results from a direct comparison made between candidate classifiers, where FNN achieved 92.40%, CNN achieved 90.10%, PRFNN achieved 91.23%, and AdaBoost achieved 58.48%, all the key characteristic variables remained the same. Therefore, the FNN is the final selected candidate from the shortlist of possible candidates, FNN was selected as it provides the highest accuracy, although it must be noted that PRFNN provides similar accuracy with 91.23%.

Secondly, providing the forensic investigator with a calculated percentage level of similarity between suspect note and template note simplifies the process of analysis, when compared to performing manual analysis, this increases the applicability of using the same methods across multiple currencies of similar types. Thus, this process can be made more streamlined, as this is a repeatable process it satisfies the requirement of forensic analysis to be systematic, and methodological in nature.

5.4 CONCLUSION

In conclusion, an empirical approach to the design and development of a functional prototype for the digital currency forensics application has been developed. The

system is able to classify banknotes of the RBNZ denominations, and provide a level of similarly. The system is able to achieve 92.40% accuracy when applied to the combined dataset of 171 banknote images, and 81.69% when applied to images purely outside of the training set. It was hypothesised in section 3, that a combination of colour, and texture features of the banknote images would increase the accuracy over using either colour or texture alone. It turns out that an increase of roughly, 4% - 5%, may be observed when providing the classifier both colour and texture features in one two-part feature vector.

Interestingly, an improvement in accuracy was observed when providing a feature vector containing first colour features, and then texture features, rather than texture, then colour features. When the colour features are put into the feature vector, first the accuracy rate observed was 87.72%, when texture was put first, we observed an accuracy rate of 86.55% of recognition accuracy on those images outside of the training set. Therefore, it is concluded that the order in which the key characteristic features are passed through to the classifier in the feature vector, do in fact influence the overall accuracy.

Through the experimental phase, the candidate classification algorithms shortlisted from the literature were compared through direct comparison, the shortlisted candidates were selected through initial pilot tests, and were the FNN, CNN, PRFNN, and Adaboost. It is concluded, that FNN is the most suitable candidate for use in the digital forensic system, when considering currency which uses colour as a primary differentiating factor between denominations. In the experimental phase, an accuracy of 98.00% was observed when applied to the entire dataset including training, and testing images for FNN, 95.00% for PRFNN, 94.00% for CNN, and 53.00% AdaBoost. FNN, PRFNN, and CNN were each set to eleven input nodes, thirty hidden nodes, and ten output nodes using the Bayesian regulation back propagation method, whereas the AdaBoost classifier was set to 100 weak classifiers.

Clearly, FNN is the ideal candidate classifier in this application, a key feature two-part vector containing both colour and texture features, placing the colour features first, and texture second. A subsequent hypothesis stated that certain characteristics extracted may have higher weightings than others, this means that certain characteristics may provide more discriminability, as a result, a determination of redundant characteristics may be in the feature vector or even hindering the overall performance. Identification of redundant characteristics or those which decrease the performance should be removed from the feature vector so as to ensure optimal accuracy.

Therefore, an experiment to determine the redundant or non-desirable characteristics was performed, table Table 4.5 shows that both the central moment in the colour features, and contrast in the texture features provide the least to the overall accuracy. Experiments were conducted to determine whether we are using redundant or non-desirable features, the results are shown in table Table 4.5, from the experimental results it is concluded that the central moment, and the contrast contribute the least to the overall effectiveness of the classifier. When the aforementioned characteristics are removed from the feature vector, an increase in accuracy was observed from, 87.72%, to 92.40%, and 90.64%, respectively for central moment, and contrast therefore these characteristics should be removed.

The final module in this system is the similarity measurement, which is output to the forensic investigator to determine how similar the suspect note is to the pre-selected template image in the database. The comparison is made between the vector of the suspect note, and the vector of the template note using the inner product, and finally output to the user.

Chapter 6

Conclusion

The following section concludes this thesis by firstly summarising the previous chapters, and then by identifying future research directions.

6.1 SUMMARY

In conclusion, currency is a formal medium for exchange used to facilitate the transfer of property or ownership from one party to another, the current currency systems are composed of a complex combination of coins, banknotes, and electronic currency variants. Throughout history, issuing authorities have faced one common threat, the threat of counterfeiting, today it appears that counterfeiting remains an on-going arms race, fuelled by the continual technological advancements in reprographic equipment available to both the currency designers, and the general public.

The currency forensics analysis process is hindered by the fact that the banknote manufacturing industry is extremely secretive, the fundamental mechanics of security components are often closely guarded trade secrets, where much of the security is ensured by this obscurity. Similarly, the currency counterfeiters are widespread, and dispersed from one another, often working independently; subsequently, the

methods ,and techniques that counterfeiters use are equally as widespread, and are therefore difficult to specify typical counterfeit traits.

The current trends observed in the literature suggest that banknote recognition software is a growing area of research, banknote recognition software is implemented on a wide array of devices from ATMs, banknote sorting machines, self service payment kiosks, and more recently portable device enabled software assisting the visually impaired. Much of the existing research is primarily based on the recognition of banknote denominations, this is based on a captured image, where an infinitesimally comparable amount provides authentication enhancing security, and only a few combine both.

Consideration of banknote authenticity from a computational perspective, we must determine the key computable features, the literature shows that computable features can be derived from three broad categories: (1) the captured image of a banknote as a whole, (2) authentication of specific known ROIs, like the serial number, and (3) sensing of intrinsic physical properties associated with the banknote. The former two typically rely on a combination of image processing techniques, and pattern recognition to process the banknote, and determine its denomination, whereas the latter typically requires some extra components during the acquisition phase, such as, acquisition of the electromagnetic properties of specific areas of the banknote (Qian et al., 2011).

In this thesis, paper currency is taken into consideration, an empirical approach for automated currency forensics is formulated, and a prototype is developed, we consider the analysis of the banknote as a whole, where two primary components are used to facilitate the forensic process. Firstly, the banknote is preprocessed and characterised using image processing techniques; to classify notes against a database of known good values, the second module authenticates an identified banknote image by comparison against a pre-selected template image from the classi-

fication database.

A two-part feature vector is formulated, consisting of colour features, and texture features, in this thesis the intensity histogram shape descriptors: *mean*, *kurtosis*, *central moment*, *skew*, *standard deviation*, and *variance*; the texture features are calculated from the image *entropy* and the GLCM features *homogeneity*, *correlation*, *contrast*, and *energy* have been used. Experimental results shown in section 4.2, have shown that the central moment is the least effective measurement, and in fact decreases the overall classification accuracy when included as part of the feature vector, when removed, a total accuracy of 92.40% was observed from 87.72%, similarly with the contrast feature removed 90.64%.

The note in question is classified against a FNN classifier, the literature suggested a total of 6 candidate algorithms for application to currency recognition, namely: *SVM*, *FNN*, *PRFNN*, *CNN*, *SOM*, *AdaBoost*, and *Radial Basis networks*. Initial pilot tests were conducted to assess each candidate classification paradigm with regards to ease of integration with existing models, this is a subjective choice, and made primarily based on availability of resources at hand. A shortlist of candidates was reached including *FNN*, *CNN*, *PRFNN*, and *AdaBoost*, in order to select the highest, most suitable candidate, a subsequent experiment performing direct comparison between candidates. It turns out, that the FNN classification method gives us the best performance when applied to the current data set, a performance of 92.40% for FNN, 91.20% PRFNN, 90.05% CNN, and 58.48% AdaBoost.

Finally, a measurement of the similarity between a known good database template vector, and suspect note vector, is output. The measure is calculated by using the inner product of the two vectors, thus, producing an estimation to the forensic investigator, in which, to make a decision as to how similar the note in question is, when compared to known good template images. Clearly, this reduces the effort involved in performing forensic investigation analysis on currency, subsequently,

as this is an automated process, we can increase the consistency between results obtained, thus, satisfying the methodological, and systematic requirement.

Future research will include refining the characteristics chosen, as mentioned previously during experiments, we have removed single features from the two-part feature vector increasing the overall accuracy, further research will be undertaken to assess specific combinations of characteristics removal. It turns out, that both the contrast of the banknote image, and the central moment contribute the least to the classification effectiveness, and, in fact, reduce it as when removed the performance increases substantially, future research will assess the performance with both removed simultaneously.

Interestingly, it was observed that colour features, and texture features, both provide similar discrimination power to the classification accuracy when considering the data set of 171 banknote images. The results suggest that the order of colour, and texture features, slightly influences the accuracy, as when colour is placed before texture, we observe a slightly higher rate of accuracy than the other way around. This same trend is observed on results obtained from both the images within the training set, the testing set, and both images outside of the dataset.

Future work will be conducted to assess the effectiveness of the training, and testing set size, as mentioned in section 3.7 a specific dataset size of 171 images was collected over a certain duration of time during the development phase. It was noted that the lower denominations have more variable physical quality as they are typically exchanged more often during their lifetime resulting in higher wear and tear, whereas, the denominations increase the observed physical quality of samples remains less variable. This same trend is observed in the findings where the classification accuracy is higher for the larger denominations, and decreases as the denomination value decreases.

However, it is noted that the discrepancy is minimal, and substantially noticed

where there are particular sample notes captured under undesirable lighting conditions. It was noted also in section 3.7, that this difference in quality is in fact reflective of the real-world, and therefore is crucial to develop a system for use in the real-world. Future research will be conducted to explore the relationships between differing sample sizes whilst observing effectiveness of each size by comparison to further increase accuracy.

In this thesis, we have combined the texture features of the GLCM, and the entropy value, future research work will also see other texture features examines like the Gabor texture features, and will be compared against those of the GLCM used in this thesis. Therefore, it has been identified in this scenario that colour, and texture features provide comparable results, a variable which may be altered in future research is to modify the actual texture method used with the intention to also increase accuracy.

A digital currency forensics system has been prototyped to demonstrate the function of a system, which can give forensic investigators the ability to minimise the human error component, thus reducing any impact of human error, forensic investigation involving questioned currency is a complicated, time-consuming and ad-hoc process. This process may require specially trained, questioned document examiners to examine various characteristics of the banknote, such as print, ink, or substrate fidelity, and verification of specific embedded security components, like the watermark.

One potential factor influencing the success of forensic analysis regarding currency is the verifiability of results, therefore when a forensic investigation takes place, it must not only be a thorough examination, but also systematic, and methodological, where methods are verifiable through peer analysis. It is stipulated by this thesis, that when automatic currency authentication assists currency forensic investigations, the method employed by this system is open to peer review, so algorithms

may be refined to be as accurate as possible, becoming a potential tool in currency security and forensics. Analysis of internal core algorithms may be published, and made available for peer review, publicly accepted methods within the forensic expert community will ensure the validity of analysis results.

6.2 FUTURE WORK

To date, there is little research in the area of forensic science focusing strictly on currency when compared to other areas of dedicated forensic science specialities. Other areas of discipline were examined to build a foundation through a literature review, and survey paper; the survey was conducted with the primary focus in mind that we as forensic investigators must understand the fundamental mechanics of banknotes including the process of security printing, and banknote manufacturing, the ingredients, and characteristics of substrates, inks, and complexities of integrated security components.

Extensive research exists for computer vision, and machine learning for application in ATMs, banknote sorting machines, self service payment kiosks, and visual impairment assistance, the primary focus in these applications is to ensure security, by determining the correct denomination at time of transaction. 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. The focus in the literature to date has shown lesser concern for the security and authenticity of banknotes regarding counterfeit detection.

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 forensic science is equipped to identify forgery. Continual advancements such as these allow banknote manufacturers to place hurdles in the way of counterfeiting, however, a trend has been observed since the development of polymer shows a steady increase in counterfeit notes detected, clearly, no method is 100% robust.

Analysing 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 evidently not always used 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.

Future work will see in-depth analysis of the current methodology employed by this proposed solution, it is required that a 99% accuracy rate be achieved, such analysis will focus on the training, and testing size of the sample set, this will be made possible whereby over a longer duration of time, a wider array of banknote images will be acquired for testing purposes. Consequently, the characteristics used to computationally describe the acquired banknote images will be refined, further

analysis of the colour descriptors, and texture descriptors will be explored.

Through the experiments conducted during the process of this thesis, it was observed that the RGB color space is the most suitable for the application of digital currency forensics. In particular, the equally weighted grey-level, intensity level, provided the most accurate results, and thus is selected as the final candidate. The equal weighting between the R, G, , and B, channels was used purely to perform a direct comparison between the shortlisted colorspaces observed in Section 2, namely: HSI, Lab, and RGB. In addition, it would be beneficial to adjust the scope to expand the current research with the intention to explore the relationship of the individual R, G, and B, channels, with such exploration it is envisaged that the accuracy will be improved and fine tuned to bring the digital currency forensics system accuracy closer to the 99% goal.

In particular it was observed in Section 4, that with removal of unusual outliers, the system accuracy of this system was able to be increased. It was tentatively surmised that the outliers may be due to slight rotations during the data acquisition phase, this was demonstrated in figure Figure 4.7, whereby the sample images were scanned; it appears that those images which were slightly off alignment during the acquisition process appear to have a border of completely white pixels compensating for the misalignment on the scanning apparatus. When the system was retrained minus the outliers, the overall accuracy was able to be increased across all of the classifiers, and in particular a rise from 92.40%, to 98.60% accuracy was observed by the final FNN schema.

Therefore, it would be beneficial to increase the current research scope to accommodate exploration into automatic banknote image rotation. Thus adjusting the currently implemented algorithm to automatically correct, and compensate for rotation, whereby the image it's self is rotated rather than compensating by adding in a border of redundant pixels. As it was demonstrated, this may potentially cause

a misclassification, and thus reduction in observed accuracy.

On a final note, it is interesting to note that the technique of describing banknote images by their colour, and texture features can be employed on any currency, world wide, where the use of colour is one of the key points determining which denomination is currently being analysed (García-Lamont et al., 2012). Therefore, this same technique will be applied to other such currency where colour is used to differentiate the denominations from one another, with the intention to increase the scope of applicability in the forensic investigation.

References

Adams, G., Pollard, S., & Simske, S. (2011). A study of the interaction of paper substrates on printed forensic imaging. *Proceedings of the 11th ACM symposium on Document engineering (DocEng '11)*, 263-266.

Beekhof, F. P., Voloshynovskiy, S., Koval, O., Villan, R., & Topak, E. (2008). Document forensics based on steganographic anti-counterfeiting markings and mobile architectures. *Proceedings of the 1st international conference on forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics'08)*, 1-5.

Bender, K. (2006). *Moneymakers*. Berlin: John Wiley and Sons.

Berthier, S., Boulenguez, J., & Bálint, Z. (2007). Multiscaled polarization effects in Suneve coronata (Lepidoptera) and other insects: application to anti-counterfeiting of banknotes. *Applied Physics A: Materials Science and Processing*, *86*(1), 123-130.

Bulan, O., Mao, J., & Sharma, G. (2009). Geometric distortion signatures for printer identification. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'09)*, 1401-1404.

Burger, A. (2009). *The Devil's workshop: a memoir of the nazi counterfeiting operation*. Barnsley: Frontline Books.

Cao, B.-Q., & Liu, J.-X. (2010). Currency recognition modeling research based on BP neural network improved by gene algorithm. *Proceedings of the 2nd International Conference on Computer Modeling and Simulation*, *2*, 246-250.

Chae, S.-H., Kim, J. K., & Pan, S. B. (2009). A study on the Korean banknote recognition using RGB and UV information. *Communication and Networking*, *56*, 477-484.

Chang, C. C., Yu, T. X., & Yen, H. Y. (2007). Paper currency verification with Sup-

port Vector Machines. *3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System (SITIS '07)*, 860-865.

Chia, T. H., & Levene, M. J. (2009). Detection of counterfeit U.S. paper money using intrinsic fluorescence lifetime. *Optics Express*, *17*(24), 22054-22061.

Clarkson, W., Weyrich, T., Finkelstein, A., Heninger, N., Halderman, J. A., & Felten, E. W. (2009). Fingerprinting blank paper using commodity scanners. *30th IEEE Symposium on Security and Privacy*, 301-314.

Daraee, F., & Mozaffari, S. (2010). Eroded money notes recognition using wavelet transform. *6th Iranian Machine Vision and Image Processing (MVIP)*, 1-5.

Dasari, H., & Bhagvati, C. (2007). Identification of non-black inks using HSV colour space. *9th International Conference on Document Analysis and Recognition (ICDAR'07)*, *1*, 486-490.

Debnath, K., Ahmed, S., Shahjahan, M., & Murase, K. (2010). A paper currency recognition system using negatively correlated neural network ensemble. *Journal of Multimedia*, *5*(6), 560-567.

Debnath, K. K., Ahdikary, J. K., & Shahjahan, M. (2009). A currency recognition system using negatively correlated neural network ensemble. *12th International Conference on Computers and Information Technology, 2009.*, 367-372.

García-Lamont, F., Cervantes, J., & López, A. (2012). Recognition of Mexican banknotes via their color and texture features. *Expert Systems with Applications*, *39*(10), 9651-9660.

Gaubatz, M. D., & Simske, S. J. (2009). Printer-scanner identification via analysis of structured security deterrents. *1st IEEE International Workshop on Information Forensics and Security (WIFS'09)*, 151-155.

Gaubatz, M. D., Simske, S. J., & Gibson, S. (2009). Distortion metrics for predicting authentication functionality of printed security deterrents. *16th IEEE*

International Conference on Image Processing (ICIP'09), 1489-1492.

Geusebroek, J.-M., Markus, P., & Balke, P. (2011). Learning banknote fitness for sorting. *International Conference on Pattern Analysis and Intelligent Robotics (ICPAIR'11)*, *1*, 41-46.

Glock, S., Gillich, E., Schaede, J., & Lohweg, V. (2009). Feature extraction algorithm for banknote textures based on incomplete shift invariant wavelet packet transform. *Pattern Recognition*, *5748*, 422-431.

Gonzalez, R. C., Woods, R. E., & Eddins, S. L. (2009). *Digital image processing using MATLAB* (2nd ed.). Knoxville: Gatesmark Publishing.

Gou, H., Li, X., Li, X., & Yi, J. (2011). A reliable classification method for paper currency based on LVQ neural network. *Advances in Computer Science and Education Applications*, *202*, 243-247.

Grijalva, F., Rodriguez, J., Larco, J., & Orozco, L. (2010). Smartphone recognition of the U.S. banknotes' denomination, for visually impaired people. *IEEE ANDESCON*, 1-6.

Guo, J., Zhao, Y., & Cai, A. (2010). A reliable method for paper currency recognition based on LBP. *2nd IEEE International Conference on Network Infrastructure and Digital Content*, 359-363.

Halder, B., & Garain, U. (2010). Color feature based approach for determining ink age in printed documents. *20th International Conference on Pattern Recognition (ICPR'10)*, 3212-3215.

Hasanuzzaman, F. M., Yang, X., & Tian, Y. (2011). Robust and effective component-based banknote recognition by SURF features. *20th Annual Wireless and Optical Communications Conference (WOCC'11)*, 1-6.

Hasanuzzaman, F. M., Yang, X., & Tian, Y. (2012). Robust and effective component-based banknote recognition for the blind. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *42*(99),

1-10.

Hassanpour, H., & Farahabadi, P. M. (2009). Using Hidden Markov Models for paper currency recognition. *Expert Systems with Applications*, *36*, 10105-10111.

He, K., Peng, S., & Li, S. (2008). A classification method for the dirty factor of banknotes based on neural network with sine basis functions. *International Conference on Intelligent Computation Technology and Automation (ICICTA'08)*, *1*, 159-162.

Hong, Z. (2009). The impact of e-money on the economy. *WRI World Congress on Computer Science and Information Engineering*, *3*, 126-130.

Hrishikesh, C., & Shefali, S. (2009). Printed document watermarking using phase modulation. *2nd International Conference on Emerging Trends in Engineering and Technology (ICETET'09)*, 222-227.

Huang, S., & Wu, J. K. (2007). Optical watermarking for printed document authentication. *IEEE Transactions on Information Forensics and Security*, *2*(2), 164-173.

Huber-Mörk, R., Heiss-Czedik, D., Mayer, K., Penz, H., & Vrabl, A. (2007). Print process separation using interest regions. *Computer Analysis of Images and Patterns*, *4673*, 514-521.

Ishigaki, T., & Higuchi, T. (2008). Dynamic spectrum classification by divergence-based kernel machines and its application to the detection of worn-out banknotes. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'08)*, 1873-1876.

Jahangir, N., & Chowdhury, A. R. (2007). Bangladeshi banknote recognition by neural network with axis symmetrical masks. *10th international conference on Computer and information technology (ICCIT'07)*, 1-5.

Jin, Y., Song, L., Tang, X., & Du, M. (2008). A hierarchical approach for banknote

image processing using homogeneity and FFD model. *IEEE Signal Processing Letters*, *15*, 425-428.

Jing, L., Shuang, L., Jin, M.-S., & Wei, W. (2010). About RMB number identification with genetic evolution neural network. *International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE'10)*, *1*, 286-288.

Kee, E., & Farid, H. (2008). Printer profiling for forensics and ballistics. *Proceedings of the 10th ACM Workshop on Multimedia and Security (Sec '08)*, 3-10.

Kersten, J. (2009). *The art of making money: the story of a master counterfeiter*. New York: Gotham.

Kim, H. Y., & Mayer, J. (2007). Data hiding for binary documents robust to print-scan, photocopy and geometric distortions. *XX Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI'07)*, 105-112.

Kulčar, R., Friškovec, M., Hauptman, N., Vesel, A., & Gunde, M. K. (2010). Colorimetric properties of reversible thermochromic printing inks. *Dyes and Pigments*, *86*(3), 271-277.

Kumpulainen, P., Mettänen, M., Lauri, M., & Ihalainen, H. (2011). Relating halftone dot quality to paper surface topography. *Neural Computing & Applications*, *20*(6), 803-813.

Lee, K.-H., & Park, T.-H. (2010). Image segmentation of UV pattern for automatic paper-money inspection. *11th International Conference on Control Automation Robotics Vision (ICARCV'10)*, 1175-1180.

Li, L., Yu-tang, Y., Yu, X., & Liang, P. (2010). Serial number extracting and recognizing applied in paper currency sorting system based on RBF network. *International Conference on Computational Intelligence and Software Engineering (CiSE)*, 1-4.

Li, Z., Zhou, X., & Chen, Y. (2009). Research for the intelligent RMB sorter based on ANN. *9th International Conference on Electronic Measurement and Instruments (ICEMI '09)*, 99-103.

Liu, X. (2008). A camera phone based currency reader for the visually impaired. *Proceedings of the 10th international ACM SIGACCESS conference on Computers and accessibility*, 305-306.

MacKay, D. J. C. (1992). A practical Bayesian framework for backpropagation networks. *Neural Computation*, *4*(3), 448-472.

Marques, O. (2011). *Practical image and video processing using MATLAB*. New Jersey: Wiley.

Morshidi, M. A., Marhaban, M. H., & Jantan, A. (2008). Color segmentation using multi layer neural network and the HSV color space. *International Conference on Computer and Communication Engineering*. *ICCCE 2008*., 1335-1339.

Nah, J., Kim, J., & Kim, J. (2009). A new image watermarking using peak position modulation for ID photos. *11th IEEE International Symposium on Multimedia (ISM '09)*, 595-599.

Neumann, C., Ramotowski, R., & Genessay, T. (2011). Forensic examination of ink by high-performance thin layer chromatography - The United States secret service digital ink library. *Journal of Chromatography A*, *1218*(19), 2793-2811.

Nieves, J., Ruiz-Agundez, I., & Bringas, P. G. (2010). Recognizing banknote patterns for protecting economic transactions. *IEEE Workshop on Database and Expert Systems Applications (DEXA'10)*, 247-249.

Nishimura, K. (2009). Banknote recognition based on continuous change in strictness of examination. *ICCAS-SICE*, 5347-5350.

Omatu, S., Yoshioka, M., & Kosaka, Y. (2009). Reliable banknote classification using neural networks. *3rd International Conference on Advanced Engineer-*

ing Computing and Applications in Sciences (ADVCOMP '09), 35-40.

Paisios, N., Rubinsteyn, A., Vyas, V., & Subramanian, L. (2011). Recognizing currency bills using a mobile phone: an assistive aid for the visually impaired. *Proceedings of the 24th annual ACM symposium adjunct on User interface software and technology*, 19-20.

Papastavrou, S., Hadjiachilleos, D., & Stylianou, G. (2010). Blind-folded recognition of bank notes on the mobile phone. *ACM SIGGRAPH 2010 Posters*, *68*, 1.

Parlouar, R., Dramas, F., Macé, M. M.-J., & Jouffrais, C. (2009). Assistive device for the blind based on object recognition: an application to identify currency bills. *Proceedings of the 11th international ACM SIGACCESS conference on Computers and accessibility*, 227-228.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). THE DESIGN SCIENCE RESEARCH PROCESS: A model for producing and presenting information systems research.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45-77.

Pollard, S. B., Simske, S. J., & Adams, G. B. (2010). Model based print signature profile extraction for forensic analysis of individual text glyphs. *IEEE Workshop on Information Forensics and Security (WIFS'10)*, 1-6.

Pramoun, T., & Amornraksa, T. (2009). Improved image watermarking using pixel averaging and unbiased retrieval. *9th International Symposium on Communications and Information Technology (ISCIT'09)*, 1142 -1147.

Qi, W., Li, X., & Yang, B. (2009). Bilinear coons patch and its application in security pattern design. *5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '09)*, 881-884.

Qian, S., Zuo, X., He, Y., Tian, G., & Zhang, H. (2011). Detection technology to identify money based on pulsed eddy current technique. *17th International Conference on Automation and Computing (ICAC'11)*, 230-233.

Rusanov, V., Chakarova, K., Winkler, H., & Trautwein, A. X. (2009). Mössbauer and X-ray fluorescence measurements of authentic and counterfeited banknote pigments. *Dyes and Pigments*, *81*(2), 254-258.

Russ, J. C. (2007). *The image processing handbook* (5th ed.). New York: CRC Press.

Ryu, S.-J., Lee, H.-Y., Cho, I.-W., & Lee, H.-K. (2008). Document forgery detection with SVM classifier and image quality measures. *Advances in Multimedia Information Processing - PCM 2008*, *5353*, 486-495.

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

Schulze, C., Schreyer, M., Stahl, A., & Breuel, T. M. (2008). Evaluation of graylevel-features for printing technique classification in high-throughput document management systems. *Computational Forensics*, *5158*, 35-46.

Shan, G., Peng, L., Jiafeng, L., & Xianglong, T. (2009). The design of HMM-based banknote recognition system. *IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS'09)*, *4*, 106-110.

Shankar, N. G., Ravi, N., & Zhong, Z. W. (2009). A real-time print-defect detection system for web offset printing. *Measurement*, *42*(5), 645-652.

Simske, S., Adams, G., Aronoff, J., & Sturgill, M. (2009). New findings in security printing and imaging. *25th International Conference on Digital Printing Technologies and Digital Fabrication 2009 (NIP25)*, *25*, 158-160.

Simske, S., Aronoff, S., Sturgill, M., Collins, F., Golodetz, G., & Israel, R. (2007).

Security printing deterrents: A comparison of TIJ, DEP and LEP printing. *International Conference on Digital Printing Technologies and Digital Fabrication*, *23*, 543-548.

Simske, S. J., Aronoff, J. S., Sturgill, M. M., & Golodetz, G. (2008). Security printing deterrents: a comparison of thermal ink jet, dry electrophotographic, and liquid electrophotographic printing. *Journal of Imaging Science and Technology*, *52*(5), 1-7.

Singh, B., Badoni, P., & Verma, K. (2011). Computer vision based currency classification system. *International Journal of Computer Applications*, *2*(4), 34-38.

Solymar, Z., Stubendek, A., Radvanyi, M., & Karacs, K. (2011). Banknote recognition for visually impaired. *20th European Conference on Circuit Theory and Design (ECCTD'11)*, 841-844.

Sun, B., & Li, J. (2008a). Recognition for the banknotes grade based on CPN. *International Conference on Computer Science and Software Engineering*, *1*, 90-93.

Sun, B., & Li, J. (2008b). The recognition of new and old banknotes based on SVM. *2nd International Symposium on Intelligent Information Technology Application (IITA '08)*, *2*, 95-98.

Tarnoff, B. (2011). *Moneymakers: the wicked lives and surprising adventures of three notorious counterfeiters*. New York: The Penguin Press HC.

Trémeau, A., & Muselet, D. (2009). Recent trends in color image watermarking. *Journal of Imaging Science and Technology*, *53*(1), 1-15.

van Beusekom, J., Schreyer, M., & Breuel, T. (2010). Automatic counterfeit protection system code classification. *Proceedings of SPIE, Media Forensics and Security II*, *7541*, 1-8.

van Beusekom, J., & Shafait, F. (2011). Distortion measurement for automatic document verification. *International Conference on Document Analysis and*

Recognition (ICDAR'11), 289-293.

Verikas, A., Lundstram, J., Bacauskiene, M., & Gelzinis, A. (2011). Advances in computational intelligence-based print quality assessment and control in offset colour printing. *Expert Systems with Applications*, *38*(10), 13441-13447.

Verma, K., Singh, B., & Agarwal, A. (2011). Indian currency recognition based on texture analysis. *Nirma University International Conference on Engineering (NUiCONE)*, 1-5.

Vila, A., Ferrer, N., & Garcia, J. F. (2007). Chemical composition of contemporary black printing inks based on infrared spectroscopy: Basic information for the characterization and discrimination of artistic prints. *Analytica Chimica Acta*, *591*(1), 97-105.

Žiljak, V., Pap, K., & Žiljak, I. (2009). CMYKIR security graphics separation in the infrared area. *Infrared Physics and Technology*, *52*(2-3), 62-69.

Wenhong, L., Wenjuan, T., Xiyan, C., & Zhen, G. (2010). Application of support vector machine (SVM) on serial number identification of RMB. *8th World Congress on Intelligent Control and Automation (WCICA)*, 6262-6266.

Wu, Q., Zhang, Y., Ma, Z., Wang, Z., & Jin, B. (2009). A banknote orientation recognition method with BP network. *Proceedings of the WRI Global Congress on Intelligent Systems (GCIS '09)*, 3-7.

Wu, Y., Kong, X., You, X., & Guo, Y. (2009). Printer forensics based on page document's geometric distortion. *IEEE International Conference on Image Processing (ICIP'09)*, 2909-2912.

Xie, J., Qin, C., Liu, T., He, Y., & Xu, M. (2009). A new method to identify the authenticity of banknotes based On the texture roughness. *IEEE International Conference on Robotics and Biomimetics (ROBIO'09)*, 1268-1271.

Yeh, C.-Y., Su, W.-P., & Lee, S.-J. (2011). Employing multiple-kernel support vector machines for counterfeit banknote recognition. *IEEE Applied Soft Com-*

puting, *11*(1), 1439-1447.

Yoshida, K., Kamruzzaman, M., Jewel, F. A., & Sajal, R. F. (2007). Design and implementation of a machine vision based but low cost stand alone system for real time counterfeit Bangladeshi bank notes detection. *10th international conference on Computer and information technology (ICCIT'07)*, 1-5.

Zhao, L.-l., Gu, Z.-c., & Fang, Z.-l. (2008). A morphology screen coding anti-counterfeiting method based on visual characteristics. *Optoelectronics Letters*, *4*(5), 371-374.

Zhou, W.-c., Xie, G.-s., & Liu, B. (2008). The application of mixed GA-BP algorithm on remote sensing image classification. *Geoinformatics 2008 and Joint Conference on GIS and Built Environment: Classification of Remote Sensing Images*, *7147*(1), 8.