JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY DOCUMENT's FORENSICS

1st Parag D. Nathe, 2nd Dr. Prashant B. Shingwekar
1st Lecture, Government Institute of Printing Technology, Mumbai, Maharashtra,
2nd Associate Professor, University Department of Chemical Technology,
Sant Gadge Baba Amaravati University, Amaravati, Maharashtra, India

Abstract: The term 'currency' denotes a mutually accepted medium of exchange; in the case of a nation, its currency serves as the official medium that is administered by the elected governing body. Throughout the annals of time, issuers have encountered a persistent peril: counterfeiting. In spite of the progress made in technology, the resolution of the issue of counterfeit production is still a while off. The scientific verification of authenticity necessitates an in-depth comprehension of the constituent materials and production methodologies. This survey identifies voids in the current literature and functions as a synthesis of the existing research in order to comprehend the mechanics and technology underlying currency production and security. In the end, a strong currency is preferred.

Index Terms – Document Security, Investigation techniques, Diffraction, Interference, DOVID, Currency forensics, Substrate analysis, Ink analysis, Counterfeit currency, Public security devices

I. INTRODUCTION

Throughout our development, we have depended on the ability to trade goods and services with one another. One of the earliest forms of trade was the barter system, which has been largely replaced by formal mediums like coins, banknotes, and electronic currency. In the past, official forms of exchange, known as 'currency,' symbolize a common medium regulated by the government, now made up of standardized items with value. Currency holds value based on the trust in its authenticity. One common issue faced by currency issuers is protecting the design from counterfeiting. In numerous countries, central banks owned by the government, also referred to as "reserve banks," oversee the nation's monetary policy. They are responsible for tasks such as being the sole authorities in issuing banknotes and coins, ensuring security and design, and controlling the circulation levels. Currently, currency is made up of coins, banknotes, and electronic data. Counterfeiting continues to be a concern due to ongoing advancements in reprographic equipment accessible to the public. Society's stability is closely tied to the trust we have in our currency, which in turn depends on security measures. There are numerous challenges in the field of currency forensics. The level of effort needed to identify fake banknotes is linked to the expertise of counterfeiters, and this trend seems to be continuing. Detecting authenticity is a complex task that requires a thorough understanding of all features.

Reserve or central banks are a recent development, with privately owned banks historically issuing their own currency. After years of instability and lack of compatibility between currencies and rampant counterfeit activities, central banks were established to centralize currency issuance and policy control. Legal authority is granted to such entities, and this varies depending on the country. Counterfeiters aim to create realistic replicas by understanding established security elements. Security features are divided into three main categories:

1) Easily noticeable by human senses
2) Concealed from typical observation, detectable with tools like a magnifying glass or UV light
3) Inherent traits from the production process and the combination of materials.

Physical money can deteriorate over time, making it harder to inspect as the damage is not consistent. For example, ink may wear out faster on certain areas of paper currency than on others, and bills in warmer regions tend to wear out more quickly than those in cooler regions. Individuals have been observed exploiting this by intentionally soiling certain parts of banknotes, facilitating discreet circulation and complicating identification. Automatic Teller Machines (ATM) and central banknote sorting machines use banknote recognition software to reduce counterfeit banknote circulation. With expertise in printing technology, this software utilizes image processing, machine learning, and pattern recognition to verify security features based on learned threshold values. Threshold values act as reference points for determining the authenticity and quality of banknotes. If a banknote falls below the specified threshold value, it is considered either counterfeit or too worn out to remain in circulation. Banknote recognition software is usually designed to assess print quality. In the literature, quality is described as the faithfulness of the captured image to a known good value. Even though this method prioritizes print quality, most features still require manual inspection for verification. Those who create counterfeit items may be able to replicate some security features, but not all of them. Reproduction of security features involves Intaglio print press and Offset Lithographic printing methods, along with closely guarded secret ink and substrate recipes.

There is a noticeable shift towards the exploration and advancement of technologies like incorporating Radio Frequency Identification (RFID) devices to enhance security in current banknotes, and the move towards digital currency. Just like traditional mediums, electronic currency comes in various forms, including those issued and backed by the state or issuing authority, mobile payment systems, and complete virtual currency within cyberspace communities. Defining electronic money can be a bit abstract and subjective. It refers to any form of electronic value that can be exchanged similar to physical currency like banknotes and coins, but it lacks consistency or uniformity. At times, the inconsistent and incompatible array of stored value and electronic payment systems can be challenging to regulate. There is a noticeable lack of governance in the electronic currency paradigm, as seen in the various incompatible models in use today like the e-Coin. Electronic currency is often seen as the digital version of physical money, offering users privacy and security through unique encryption methods. In contrast to debit and credit cards, transactions are not reversible. This field is currently a dynamic area of research with practical applications in use today. Irreversible transactions depend on the hashing method used, and the electronic paradigm introduces new governance and security concerns. Identifying counterfeit items has typically been a responsibility for law enforcement agencies. Professionals in this field gain expertise through extensive hands-on experience, much like Questioned Document Examiners (QDEs). Scientific communities promote research aimed at understanding the essence of documents. QDE is a specialized niche within forensic science that focuses on defining methods for analyzing intrinsic document characteristics such as handwriting, signature, paper, and ink analysis.

II. THREAT ON CURRENCY

Even with the rise of electronic payments, physical currency continues to play a crucial role in all countries' payment systems and is still widely used for in-person transactions. In many countries, the majority of the currency in circulation is issued by the national monetary authority. In some instances, foreign currency, like that of the United States, is also commonly used. Irrespective of the particular currencies being used, every country's payment system involves various participants such as consumers, retail businesses, financial institutions, central banks, armored car companies, and third-party currency processors. Anyone involved in handling money within a country's payment system needs to be able to verify the authenticity of currency, easily identify its value, and minimize the costs associated with its management.

For maintaining trust in a circulating currency, banknotes need to include features that allow the public to easily verify their authenticity and identify the notes' values. Designing currency involves various factors, while also aiming to reduce costs and ensure easy handling by others. It is common for monetary authorities to favor banknotes that are cost-effective to produce and have a long lifespan in circulation. These factors combine to make banknote design a blend of art, science, and economics. In general, financial authorities around the world acknowledge that enhancing public knowledge and awareness of their currency's features helps them achieve their objectives. Research on public awareness of currency features indicates that many people are unaware of any security features on their country's banknotes.

Three main threats to currency include duplication, imitation, and mutilation.

1) Replicating
   a) Capturing images - Through capturing detailed images of banknotes, it is possible to create accurate replica banknotes using traditional darkroom photographic enlargement methods. It can be challenging to spot these differences right away because the colors appear realistic, but the texture of the material feels noticeably distinct.
   b) Photocopying - Photocopying was a significant issue leading to the spread of counterfeit currency globally in the 1980s and 1990s. Photocopying is a basic method that may appeal to some, but it is not very effective for creating authentic-looking replicas. Copies made this way often have obvious flaws like repeated serial numbers, unusual texture, and dull colors.
   c) Scanning - Dealing with counterfeiters can be more challenging than handling photocopying due to their ability to manipulate images using Photoshop editing software Enables precise modifications of serial numbers, potentially making duplicates hard to detect based on the print, ink, and substrate quality.
2) Imitating
   a) Desktop publishing - Appealing to those looking to replicate documents on a budget, modern equipment can create high-quality forgeries that appear authentic at first sight. While the current equipment can produce high-quality documents, its capabilities do not yet reach the level of Intaglio and Offset Lithographic methods. The ink may not be as bold and tends to fade more quickly. When examined closely, microtext and intricate patterns are not produced with the necessary quality.
   b) Commercial publishing. Greater precision is attained on the detailed microtext and Guilloché designs. The vividness and lifelike accuracy of colors achieved with premium commercial-grade inks often lead to better print and image quality compared to desktop publishing. Similarly, the material utilized is typically of superior quality, often very close in thickness, weight, and fiber texture. Embedded security components like watermarks, security fibres, and security threads are frequently disregarded due to the lack of control over the substrate.
   c) Intaglio offset lithographic production. Typically used by authorized banknote manufacturers or well-financed criminal groups. Using the same techniques as those used to produce real banknotes makes identification very difficult. At this stage, special attention is typically given to using substrates and inks that closely resemble the original product. This is where unusual irregularities in the printing process seen on established authentic print press machines should be utilized to confirm legitimacy. Moreover, the embedded security features like security fibres, threads, and watermarks differ from the original.
3) Mutilation
   a) Removing ink stains - There are different methods to remove ink, ranging from using mild acid and bleach to more intense laser removal techniques. Removing ink from a note allows for discreetly altering a lower value note to appear as a higher value note while preserving the original substrate.

b) Achieving precise cuts and seamless joins using transparent adhesive. Banknotes can be precisely cut into vertical strips to create new banknotes. At first, it may be challenging to spot, but upon careful examination, you may notice that the edges of the image are slightly disconnected from the original image, varying based on the accuracy and quantity of banknotes utilized. This enables precise modifications, especially of serial numbers, which can make duplicates challenging to identify based on the quality of the print, ink, and substrate.

III. THE IMPORTANCE OF DESIGN IN COUNTERFEIT PREVENTION

Typically, the creation of a security product progresses through a series of steps: starting with identifying a security issue (such as fraud), then analyzing the problem, and moving on to design before reaching the final product. Recognizing or anticipating fraud will lead to the development of a security policy, along with goals and tactics. Objectives form the foundation for a statement (or program) of requirements, which, along with the drafted strategies, will lead to the security program (or security scheme). Both programs, along with a fraud-risk analysis, form the foundation for choosing security measures, designing security, and developing the security product. This article briefly covers the different stages of the development sequence. Emphasis is placed on the iterative aspects of the design process from an industrial design perspective.

Recognizing a security issue and deeming it significant are essential for initiating the creation of a solution that can mitigate its negative effects. An outlined security policy includes objectives and strategies. Goals are established to outline what needs to be accomplished to address or reduce the issue. Issues may arise that could have financial implications or damage the company's reputation due to fraud, which can erode public trust in the product. The goals are expanded upon in the requirements statement. Plans are then created to detail how the established goals will be accomplished. Elaborate solutions are the focus of the security program.

IV. FRAUD RISK ANALYSIS

Here are the five steps involved in fraud-risk analysis:

1. Classify the different methods of attack or fraud. Ensure that the categories are consistent. For example, a single category like "counterfeiting" may not be sufficient and needs to be broken down into distinct categories such as "origination", "replication", and "imitation".
2. Evaluate the harm associated with each specific type of attack or fraud. When categories are not uniform, it is not possible to assign a single damage figure to the category.
3. Evaluate the likelihood of each specific type of attack or fraud happening.
4. Evaluate each individual risk.
5. Evaluate each individual risk in comparison to the anticipated expenses of mitigating or minimizing it (cost-risk analysis).

The analysis leads to a detailed report that defines and evaluates the different fraud-risk factors related to calculating the risk. This risk is calculated by multiplying the potential damage by the likelihood of it happening. Listing different types of fraud in a table alongside the impact and likelihood of each. Every item in the table needs to be thoroughly examined and justified in the accompanying report. It's not always possible or required to make a precise evaluation of the damage, its likelihood, and the risk involved. Risk is often described using qualitative terms. In the event of an attack, if sufficient prevention measures have been implemented to minimize the likelihood of occurrence to a "very small" level, any resulting damage could be deemed "acceptable" as long as it is justified in the report. Otherwise, it's important to estimate the risk of damage to the corporate image due to fraud that is widely reported in the media. While the immediate impact may be minimal, the overall consequences for the company could prove to be unsustainable in the future. Seen from that perspective, the possibility of counterfeit products causing inconvenience may not be as insignificant as previously thought.

V. SECURITY LEVELS CONSIDERED FOR DOCUMENT DESIGNING

Level I – Substrate fidelity, Print fidelity, Colour fidelity, Acoustic fidelity, Materials interaction, Serial number, Holograms, Watermark, Security thread, Security fiber, Planchets, Tactile fidelity, Color-shifting ink, Clear window, Matching sides, Latent image

Level 2 – Microtext, UV glowing ink

Level 3 -- Magnetic ink, Screen traps, Manufacture anomalies, Complicated patterns, Complicated design , Fluorescence eminence, Texture analysis

VI. CONVENTIONAL SECURITY FEATURES COMBINED ON SECURITY DOCUMENT

1) Watermark - Creating a watermark necessitates access to a paper mill, a resource that counterfeiters seldom possess. This primarily creates the Watermark, it is a robust security measure. Nevertheless, the watermark is not considered an ergonomic tool and is seldom assessed adequately. This is due to the necessity of holding it against the light, which presents a psychological disadvantage. Its halftone features must be thoroughly assessed, a task that is quite challenging and time-consuming. High-speed paper manufacture has led to the creation of watermarks that do not effectively display lighter halftones. When the ink is darker than the paper around it, it can significantly hinder proper inspection. Counterfeiters exploit this, otherwise, high-quality watermarks can be successfully replicated, displaying both lighter and darker details, deeper shades. These imitations must undergo meticulous scrutiny to be identified as such in figure 1. Therefore, If not correctly designed, the watermark serves solely to falsify.

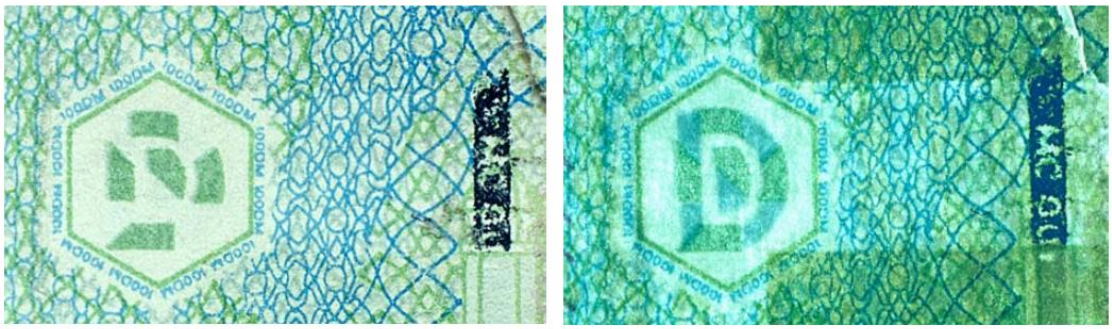


Figure 1 – Watermark and security thread in Italian 100.000 Lire bank note (transmission): (a) genuine watermark, (b) imitation watermark. Although there is a distinct difference in quality, the imitation watermark shows lighter and darker halftones. Also note that the imitation security thread has legible micro text.

2) See through Register - The See through register necessitates the counterfeiter to have precise front and back printing alignment of the note. Similar to check the watermark, hold the see-through register up to the light. Counterfeiters seldom bother to register both sides. Printing is preferred since the public generally does not bother to examine a note against the light. Majority counterfeits lack proper front-back alignment and may even have one side inverted. Even possess two identical sides. The see-through register also faces issues with its ergonomic design. The characteristic, the note displays a full, abstract graphic on both sides, which prevents it from accurately showing a register of two. Distinct visual components. Off-register on both sides is only noticeable in transmission. The user behaves accordingly struggling to comprehend the device's function. Even novice counterfeits may have a front-back print register, making it important to observe proper front-back register. The authenticity of the note is not confirmed by figures 2 and 3. The transparent register is simply a deceiver.



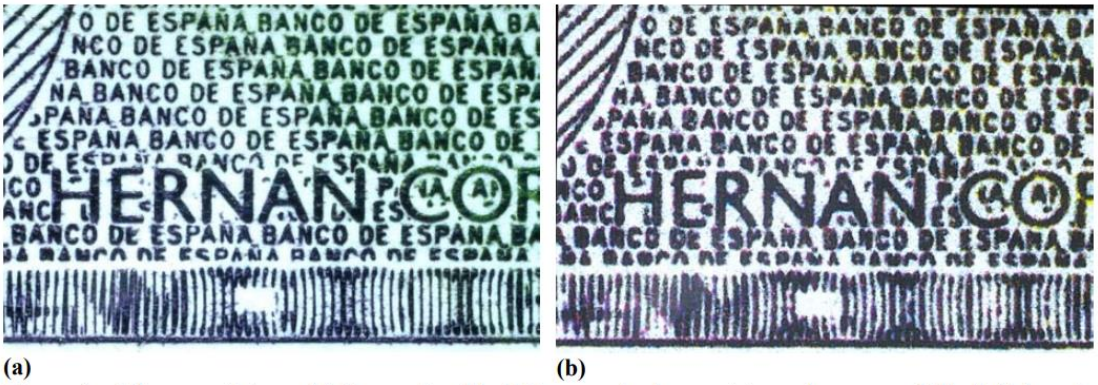
Figure 2 - Counterfeit see-through features in adequate register: (left) screen offset of the former Dutch 100 guilder note, with sub-optimal see-through design, and (right) ink jet digifeit of the Dutch 25 guilder note with optimal see-through design.



(a) (b)

Figure 3 – Micro text (0.3 mm high) around see-through register on a line offset counterfeit German 100 mark note: (a) in diffuse reflection and (b) in transmission. Note the adequate front-back register and the presence of small lettering on an imitation windowed thread that is continuous in transmission.

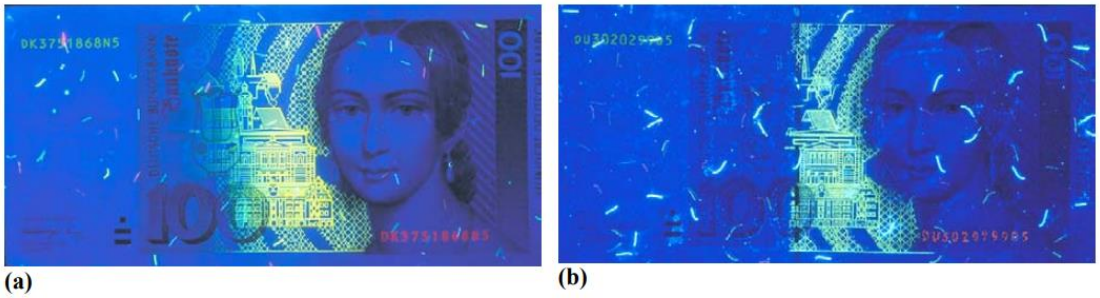
3) Micro Text - Micro text, and other fine printing characteristics help prevent issues caused by the low resolution of color copiers and DTP systems. The ergonomic aspects of fine printing details, such micro text, sometimes lack human elements are not readily apparent and necessitate keen eyesight or a magnifying glass for examination. Alternatively, expertly crafted forged documents ensure sufficient resolution to accurately replicate the micro text in figure 3. Modern color copiers and DTP systems have a resolution of 600 dpi (24 dots/mm) or more, enabling the reproduction of fine details replicated with intricate accuracy (figure 4). The intelligible micro text no longer appears as a result demonstrate authenticity. Generally, intricate printed details only benefit counterfeiters.



(a) (b)

Figure 4 – Micro text (0.4 mm high) on a Spanish 1000 peseta bank note: (a) genuine note and (b) digifeit made with HP Scanjet 6200C scanner and tektronix phaser 740 printer.

4) Fluorescent Printing - During the day or in harsh incandescent lighting, it is difficult to use a handheld ultraviolet source for inspection fluorescent printing is present. Effective examination requires a sufficiently light UV source at the counter. Available with adequate protection against ambient light. Counterfeiters may want to steer clear of such locations. Fluorescent inks are easily accessible and their preparation is not a significant challenge for counterfeiters. The development of fluorescent printing and the replication of fluorescent fibers is within the competence of the industry. A professional counterfeiter minimizes luminous characteristics for counterfeiters (figure 5).



(a) (b)

Figure 5 – Fluorescent printing on a German 100 mark note: (a) genuine note and (b) line offset counterfeit note. Also note the imitation fluorescent fibers and the note number in green (top left) and red (bottom right) fluorescence on the counterfeit note.

5) Foil Printing - Many expert printers have perfected the art of metallic foil printing. Metallic hot stamping foils are easily accessible for purchase, which diminishes the security provided by foil printing. (figure 6) Ordinary metallic gold or silver paints can be used to resemble metallic foils, and metallic foils can be transferred from genuine banknotes without losing their worth. The lack of metallic foils may suggest a counterfeit, but it can also be due to accidental washing of the note. However, the existence of a metallic foil does not confirm authenticity. Metallic foils only serve as deceivers. (figure 7)



Figure 6 – Aluminum foil printing on a UK £50 note: (a) genuine note, and (b) line offset counterfeit note.

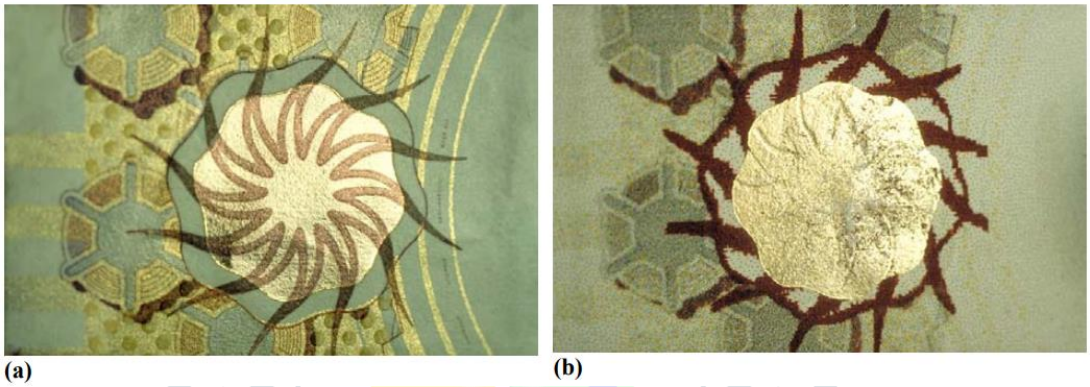


Figure 7 – Metallic gold foils on DFL 100 note: (a) genuine note, and (b) ink jet digifeit with transposed foil (the foil overprinting is lost). Also note the reflection of the pearl luster printing on the genuine note.

VII. COMBINATION OF LIQUID CRYSTAL INTERFERENCE AND DIFFRACTION EFFECTS

Lately, several researchers have managed to combine ISISs with DOVIDs. Presented at a conference by Itsuo Takeuchi et al, a new development by NHK Spring in Japan combines diffractive and interference effects to create a CPL-gram, where CPL refers to circularly polarized light.16 An expert in printing technology would appreciate the intricate details of a semi-transparent thin film of polymerized cholesteric liquid crystals that evoke the interference effect, with embossed diffraction gratings integrated into the liquid crystal film. Specular reflection occurs when the liquid crystal film acts as a highly effective Bragg mirror, reflecting a waveband that transitions from gold to blue-green as the observation angle changes. Both the Bragg reflection and the light diffracted by the embossed features are circularly polarized and can be effectively blocked by a reverse circular polarizer, figure 8 demonstrates the different impacts of the CPL-gram.

The combination of ISISs and DOVIDs, each utilizing unique production technologies, results in strong anti-counterfeiting features, which is intriguing from an inspection perspective. DOVIDs rely on their image effects like three-dimensionality, positive-negative contrast swaps, and kinematic effects for security, rather than iridescent diffraction colors that can be hard to define and might divert attention from the important image effects. Unlike ISISs security features, which typically do not include complex image effects aside from the volume reflection hologram, their strength lies in their distinct color shift. Hence, the strategic blend of precise color variations with unique image enhancements would collectively enhance the security features of the entire product. These combinations have the potential to be strong verifiers.



Figure 8 – Integration of thin film interference and diffraction in a CPL-gram: (a) Bragg reflection of the polymerized liquid crystal layer, (b) Bragg reflection extinguished by a right circular polarizer, and (c) diffractive effects, outside Bragg reflection, integrated within the liquid crystal layer.

VIII. COMBINATIONS OF IRIDESCENT EFFECTS AND LASER ENGRAVING

Another method to generate verifiers is by combining iridescent effects with laser engraving. One illustration involves creating patterns with micro holes on the paper substrate and the attached OVD, like the face value perforation in Swiss bank notes. Microperf, a feature by Orell Füssli in Switzerland, consists of holes with a diameter of around 100 µm that are only visible when held against the light. Aside from its advanced technology and the added security against counterfeiting, laser engraving also enables the inclusion of variable information. As a result, the security against counterfeiting and forgery is increased. Illustrations of this application include laser ablation of account numbers through DOVIDs on plastic cards (figure 9a), and laser perforation of account numbers through checks (figure 9b). Especially the latter characteristic effectively prevents counterfeiting since replacing the perforated number with another is extremely challenging. Brongers recently introduced a new technique called Transgraving in this field. This method includes using laser engraving to add variable information to an OVD in a way that makes the information iridescent once more (figure 9c). Transgraving enables various combinations of interference and diffraction effects, like changing ISIS information in a DOVID, altering DOVID information in an ISIS, and so on. The combination of information variability and iridescence creates a strong defense against counterfeiting and forgery, making it a reliable verifier.

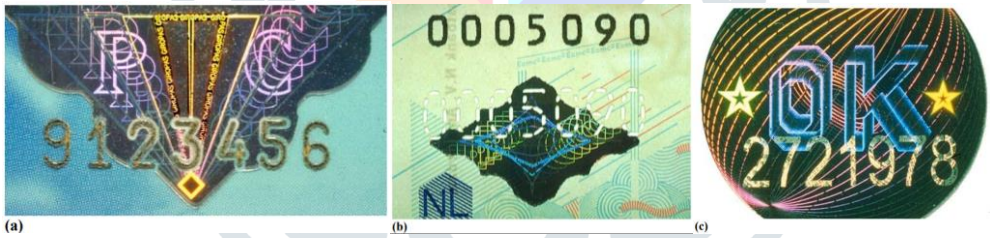


Figure 9 – Combinations of laser engraving techniques with DOVIDs: (a) Account number engraved in the Kinegram on a Dutch guarantee card by laser ablation. (b) Laser perforated slits (width 0.3 mm) constituting the account number through the Kinegram and the paper substrate of a Dutch Postcheque. The account number is printed directly above the perforation for easy comparison. (c) Sample of a transgraved iridescent account number "2721978" in a Kinegram.

IX. COMBINATION OF IRIDESCENT EFFECTS AND IMAGEPERF

ImagePerf is a laser engraving application created by IAI (Industrial Automation Integrators, The Netherlands) specifically designed to combat forgery of ID documents. ImagePerf involves a portrait that is perforated through the substrate of the document (e.g. plastic, paper) in addition to the standard portrait. Image modulation is accomplished through either varying the frequency of perforations or adjusting the size of perforations, or a combination of both methods. ImagePerf may appear invisible or visible as a brownish negative image depending on the production method and observation in diffuse reflection. To replace the original portrait in the document, the forger must now take out the perforated portrait and exchange it for a new one. Even if a skilled forger attempts to carry out these consecutive tasks, it is not a simple feat. These tasks demand a wide range of exceptional skills that are rarely all possessed by one individual. Yet, the author believes that creating a highly skilled forgery can be nearly impossible by combining ImagePerf with an iridescent security feature, ideally an ISIS. To showcase different optical effects, experiments were conducted using ImagePerf in OVI (SICPA Security Printing, Switzerland), Securigrafix thin film foil (Security Foiling, UK), and Kinegrams (OVD Kinegram Corp., Switzerland). The perforated holes have a conical shape because of the cone-shaped waist of the focused laser beam. Therefore, the white substrate is clearly visible at each perforated hole against the iridescent background. Consequently, a few notable Optically Variable ImagePerf effects can be seen in conjunction with an ISIS:

1. On a light background, a clear image of the portrait is visible (figure 10a).
2. The iridescence of ISISs is brighter in specular reflection compared to the diffuse reflection of the white substrate, resulting in a negative image of the portrait being observed (figure 10b).
3. The reversed image in specular reflection is visible against a background that changes color depending on the viewing angle.

4. When there is diffuse reflection, the white of the substrate appears brighter than the iridescent background, resulting in a positive image of the portrait (figure 10c).



Figure 10 – ImagePerf portrait in a substrate printed with an OVI background: (a) positive image in transmitted light, (b) negative image in iridescent specular reflection and (c) positive image in diffuse reflection. Clearly, for DOVIDs the second effect would not only be visible in specular reflection, but also in first order diffraction, while the 3rd effect is much more intricate and also includes variable image effects. These visually striking effects are best displayed when the iridescent background is consistent. Thus, the ISIS type of OVD is better suited for combining iridescent effects and ImagePerf compared to the DOVID type. One can achieve the desired effects using DOVIDs, but it is important to ensure that the diffractive background is uniform and that the diffractive image effects do not interfere with the OV ImagePerf effects. The higher the efficiency and reflectivity of the OVD, the more pronounced the OV ImagePerf effects appear from different viewing angles. Figure 11 displays the different OV ImagePerf effects for a thin film foil (Securigrafix, Security Foiling, UK). In summary, the pairing of ImagePerf with ISISs showcases four beneficial traits:

1. It projects a favorable impression during transmission. Due to the relatively large size of the perforated holes (up to 200 µm), you can view this image without needing to hold it up to a light source. One way to notice this is by placing the feature on a white background with less lighting on the image.
2. The display shows a clear color shift when viewed from different angles (iridescence).
3. It demonstrates a change between positive and negative images based on the angle of observation, switching between diffuse and specular reflection.
4. It enables the creation of variable information that can be readily compared with the printed information on the document. All four effects of OV ImagePerf can be easily noticed during regular observation, depending on the image background and viewing angle. As a result, these traits can be examined during regular use of the product. When faced with OV ImagePerf, the forger must now restore the iridescence of the perforated locations to successfully swap the portrait. Thus, OV ImagePerf can be seen as a robust verifier that effectively guards against counterfeiting and forgery.



Figure 11 – ImagePerf portrait in a substrate with a Securigrafix thin film device: (a) positive image in transmitted light, (b) negative image in specular reflection, and (c) positive image in diffuse reflection.

X. DOCUMENT / CURRENCY'S FORENSIC ANALYSIS

To effectively distribute fake money, the final product needs to be discreet by overcoming security features. Success hinges on the product's similarity to the original. Forensic analysis must carefully observe and measure specific intrinsic characteristics of established security components to determine if any deviations from standard values are present. Table 1 outlines the three levels of security components typically present in banknotes. In security applications like ATMs and banknote sorting machines, a threshold value is usually used to define known good values of image and color fidelity to determine authenticity and fatigue. The primary focus of the initial security level is on human senses, particularly sight, touch, and sound. It is important to highlight that most security features are located at this level. The second level of security is not easily detectable without the use of specialized equipment like a UV lamp or magnifying glass. Level three characteristics are typically associated with QDEs or forensic examiners, and are often natural traits that stem from the materials and printing methods employed. Security components are assessed based

on their level, which impacts the complexity of the determination process. The level of confidence needed may prompt additional investigation, especially if the quality of the note is in doubt.

A) Characteristics

When it comes to color application, there are three key components involved: pigment, solvent, and drier. Examining the individual components, pigment determines the color; solvent mixes the pigment with the drying agent, which in turn attaches the pigment to the substrate. There are differences between the two primary banknote printing methods, Intaglio press and Offset Lithography, based on the solvents chemical composition used. Intaglio press printing ink dries through evaporation, which is a slower process compared to Offset Lithography. With increased time, the ink spreads more, resulting in the feathering effect where the edges seem to run. Offset Lithographic ink is oil-based and dries by heating the substrate. Chemical polymerization creates sharper edges and a brighter overall result compared to Intaglio press printing. Examining forensics involves distinguishing between different printing methods, scanning at a high resolution, and closely examining edges or using a microscope to identify unique characteristics. However, this method is susceptible to human error.

Ink ingredients vary between different currencies to ensure durability and prevent counterfeiting. Developing these unique blends of raw materials is crucial, as each combination results in varying levels of radiation. Throughout the past century, the US Secret Service has been developing an ink library for forensic use. This library aids in analysis by serving as a reference point for distinguishing ink compositions and estimating age. Understanding spectrography involves using a tool to split incoming light waves bounced off objects into a frequency spectrum, allowing for the analysis of the light waves reflected from the ink. Exploring a new realm for analyzing banknotes, examining features beyond what is visible to the naked eye. Security features can be programmed for uniqueness, with currencies emitting distinct levels in the infrared and UV spectrum. This has been explored in a forensic context using a spectrography microscope, to examine layer three security features. Mössbauer spectroscopy provides a nondestructive method for determining the atomic composition of pigments. Research indicates that the black ink on US banknotes is more stable than the green ink. Black ink has a stable structure high in iron, whereas green ink is more erratic. Similarly, a two-photon microscope is utilized as an advanced technique for visualizing emitted photons. Research indicates that the fluorescence characteristics of authentic banknotes vary significantly in terms of wavelength and photon emission compared to counterfeit paper. Analyzing inkjet inks involves the use of Raman spectroscopy and laser desorption mass spectrometry techniques. Discrimination of color inkjet ink is more reliable compared to black inkjet documents because manufacturers use various raw materials for color inks but typically use common black carbon in their black inks. Raman spectroscopy was unable to distinguish between counterfeit and authentic Euros based on ink color spectra. The fake and genuine Euro banknotes showed similar color spectra, but Raman Spectra can still be used to identify fake banknotes by examining different areas of fake Euro banknotes with the same color that exhibit similar spectra.

An innovative method for automatically determining ink age involves utilizing a Region Of Interest (ROI). Examining the ROI in various documents reveals a noticeable decrease in color intensity in both RGB and HSV color spaces, showing encouraging outcomes. While their expertise is not specifically in banknote research, their approach can be applied since banknotes share a consistent design within a currency series. Special ink that remains hidden under regular light but becomes visible under UV light is used as an additional security measure. Tests have shown that fluorescence only covers certain areas of the banknotes, making it challenging for machines to detect features like microprinting and watermarks.

Counterfeiters with enough motivation and financial resources can easily replicate fluorescent ink. This was demonstrated during operation Bernhard in WWII. Through various experiments, it has been proven that UV characteristics can be adjusted to produce counterfeit notes with comparable features. Color-shifting ink creates an effect where the color changes as the viewing angle changes. Many currency issuers utilize this technique in Optical Variable Devices (OVDs) like holograms and Kinegrams. The Euro currency features a color shift on the denomination numerals located at the bottom right corner of the reverse side. Securency Australia has recently introduced a new technology named Aurora that mimics nature. Recreating color-shift ink accurately can be challenging, as it requires precise levels of shift to ensure the authenticity of currency. When a note changes colors at the wrong speed, it may be considered fake. Used on US banknotes from the early 1960s, magnetic inks were originally designed for machine-readable cheques. These inks have dark pigmentation, which limits the color options to dark green, stone red, sienna brown, and purple violet, thus restricting design possibilities. There is a specific amount of magnetism needed for each currency and denomination. Automated banknote detection methods have been created to validate by measuring the emitted electromagnetism levels. One significant issue is that the level of magnetism decreases with use, resulting in a higher error rate for lower denomination notes compared to higher ones.

Thermochromic inks are temperature-sensitive and are formulated to change color temporarily when the substrate reaches a certain temperature range. No research has demonstrated the use of thermochromic inks on paper currency; they have mainly been used on bank cheques and identity cards.

With the advancement of security inks, the authentication methods must also evolve. Switching to grayscale enables edge detection to better distinguish image details. With the increasing variety of colors used in printing paper currency, especially on polymer, excluding color from the analysis process could overlook valuable information. Converting images to grayscale involves generating new values for each pixel, which compresses the data and reduces complexity for analysis. Pixel values are calculated based on grayscale values through a linear transformation function. Converting the RGB channels into a single intensity channel, referred to as intensity thresholding above noise level, results in the remaining binary image known as the mask. The conversion from the RGB channel to grayscale results in. One issue with these methods is that colors with similar brightness but different hues, like white and yellow, may not be distinguishable when converted to grayscale. This leads to a loss of important data, especially for currencies with similar colors. Grayscale histogram generation through previous methods also overlooks crucial details about the contamination level of banknotes. When converting to grayscale, the HSV color space is a more accurate measure of color in printed documents compared to RGB. It separates intensity (luminance) and color information chromacity. Utilizing the YIQ color space involves analyzing color characteristics through histogram comparison, with the Y or 'luminance' channel playing a key role. Pixel averaging has its drawbacks. While it helps in reducing noise, it may also result in the loss of some inherent print imperfections.

Identifying print defects in currency is crucial during investigations to differentiate between different printers. Every printer system prints with minor imperfections that create distinct print signatures, even in high-quality commercial printers like Offset Lithographic and Intaglio press machines. Signatures from prints can help identify specific printers, so it's important to use pixel averaging cautiously. Studying the interaction between substrate surface, materials, and printing methods is crucial in the field of printing. Every printing method possesses distinct traits, and analysis is utilized to differentiate between printing techniques like inkjet and laser. Intaglio print press and Offset Lithographic machines in the same category can create unique irregularities that can be traced back to specific machines on counterfeit notes. Only a select group of computer users have had the opportunity to use advanced printing equipment like Offset Lithography and Intaglio print press machines. Inkjet printers have resolution capabilities that can compete with laser printers, but they are more sensitive to substrate quality, leading to greater variation when comparing the same characters at the microscopic level. There are two types of ink available for inkjet printers: pigment-based and dye-based. Pigment inks are generally more durable compared to dye inks. When observed closely, both images should ideally display round pixels, although in reality, the shape usually appears consistent. Among inkjet printers, there are noticeable differences in the quality of the printed output, especially in the scattered droplets and blurred edges. Calculating satellite scatter and edge roughness for printer signatures and profiles is essential when identifying the specific printer used to produce questioned currency. An offset is noticed between the Intaglio print press and Offset Lithographic print components of verified €10 notes. By utilizing a technique known as Maximally Stable Extremal Region (MSER), it becomes feasible to measure displacement at coordinates (x, y) using particular pixels at Points of Interest (POI) as reference markers. This brings up the question of whether the method can be utilized to forensically authenticate banknotes. Simply distinguishing based on displacement alone is not enough, as there is a noticeable variation among verified genuine notes. Extracting a print signature involves taking the outer boundary of a text glyph, known as Model Based Signature Profile (MBSP). Each document is assigned a unique signature value based on the statistical anomalies generated during printing. Regarding the substrate and printing process. Documents printed with inkjet or laser technology may result in stray toner flecks on the surface of the substrate. Identifying signatures can be determined from the consistent features of these irregularities, enabling investigators to potentially identify a laser printer by its make and model. Printer signatures are determined based on the geometric distortion features of printed materials. Geometric distortion in EP printers is primarily caused by inconsistencies in the OPC drum and polygon mirror, leading to misalignment between the original and printed output. Calculating the center of a satellite droplet of ink or toner fleck, compensating for rotation, extracting geometric signature, and measuring correlation of halftone dots from input to printer. Calculating a distortion displacement vector for each halftone dot in 2D.

Various edges, ink droplets from satellites, assessing the consistency and evenness of ink or toner on the printed surface can serve as distinguishing features.

They use three specific measures to assess this.

1) Edge roughness based on perimeter. An algorithm that quantifies the texture of a character by analyzing the perimeter variation between a regular and a smoothed image.

2) Edge roughness determined by distance mapping. An evaluation of the connection between edge pixels using distance mapping.

3) Distribution of gray values across the printed area. The variations lie in the consistency of ink or toner coverage within printed areas, which can be determined by employing a thresholding technique.

Providing evidence is a critical component of any investigation involving suspected currency or documents. Ruling out known methods of print by unique intrinsic satellite droplets and edge characteristics provides investigators with sound methods and resulting evidence subject to peer review.

Matching contraband documents with specific printers through signature analysis is a significant advancement in forensic investigations, particularly in currency and questioned document analysis. Identifying a particular printer and sometimes even its serial number raises the question of where the document was printed. Legal cases may require further investigation to understand how signatures change over time due to machinery wear and tear, which can cause geometric distortion from the physical internals of the machinery. Over time, the machinery internals may experience wear and tear, potentially leading to further distortion in the observed measurements. Profiles for printers are determined for particular character sets at various toner levels. This method relies on the toner levels, degradation of the final print, and the specific time frame. The goal is to identify if there has been any alteration of particular text values. Banknote serial numbers should be altered to avoid arousing suspicion, as sequential or repeating serial numbers can be a cause for concern. Based on accurate toner level measurement at any given time, new profiles need to be created for varying toner levels. This approach would be extremely useful for creating profiles with different toner levels. Authenticating a banknote involves identifying the unique bumps and grooves created during the Intaglio print press process. Proposing a novel algorithm for feature extraction based on incomplete shift invariant Wavelet Packet Transform (WPT) tailored for Intaglio. One specific concern is the deterioration of tactility, with the Intaglio print press tactile effect being a crucial security feature. Special markings on Hungarian notes that help the visually impaired identify notes degrade quickly within a few weeks of circulation.

B) Analysis of Components

Paper is fibrous, thus raw materials are mixed extensively in a huge vat. binding agents, chemicals, and colors create liquid-fibre pulp. Pulp is pressed rolling into thin, carefully defined layers and squeezing out remove any remaining moisture, then set. The substrate Paper cash is called ‘security paper’ by the security printing industry. The secret, unique recipe of raw paper makes security paper different from conventional paper, materials, unclear dimensions, watermarks, security threads and fibers. Microscopically, paper has a fibrous structure of meshed plant fibers. lengths vary by source material. Standard paper is mostly manufactured from wood pulp, security paper is created from reeds, flax, and cotton. Stronger and longer fibres are visible under a microscope. Fluorescence appears in particular areas of a note under UV light. areas create a unique signature that should be similar across currencies.

One can identify forged security paper using this signature by comparing sides. Due to raw material conditions and soil type, UV properties vary. can be drastically affected, therefore signatures provide evidence for questioned substrate. BOPP was developed by the Reserve Bank through a cooperative effort, of Australia (RBA), CSIRO Melbourne University is the next-generation security

substrate. Polymer money feels like paper money. The core is a thin translucent plastic film coated by additional layers for durability. BOPP security substrate from Securency According to RBA and Inovia Films, guardian is stronger and cleaner. Non-fibrous and nonporous, unlike paper. BOPP feels and looks smooth to the naked eye. Under microscopic scrutiny, the surface has random scatter craters. Advocates for BOPP security substrate claims durability beyond paper. substrate, and security advantages paper cannot provide. In particular, the transparent windows feature Fig. 12 that scans or copies black.

Development of embeddable security components is gaining popularity, through production and printing. Research indicates Lepidopetra scales, Microstructures in Coleoptera butterfly elytra cause distinct polarization. effects. Unique intricate texture with too-small-for-desktop detail from scales publishing equipment to create banknote iridescence. Iridescent ink allows basic counterfeit reproduction targeting. layer one may work. Paper texture can be fingerprinted like printer signatures and identified commodity scanners. Nature gives surfaces a unique signature, texturing flaws in paper. The unique 3D properties are calculated. exceedingly rare that two surfaces will have identical 3D properties. A document made from the same basic materials and manufacturing technique will show similarities. A one-way hash value can be calculated and saved in a database, registered against the banknote serial number or printed on it to add security. This method of document authentication is resilient, especially through data saved in databases. Substrate printing is more fatigue-prone, suitable for rarely touched security papers like diplomas certifications, land titles. Frequently handled banknotes are crumpled and smeared. As banknotes age, their signatures change. Thus, any initial hash value recorded will not apply to banknotes. on a database. Most security paper makers prefer paper over polymer due to cost. BOPP is pricey at first, but adopting countries have reported lower long-term expenditures due to its lifespan. One One of the world's largest security paper manufacturers uses polymer. A paper hybrid. Polymer is counterfeitable, and counterfeiters are getting smarter. Clearly, as counterfeiters get more sophisticated, forensic study of texture BOPP must be evaluated as security paper; forensics could benefit. understanding BOPP surface fingerprints. This would enable development of Recognition techniques to validate BOPP substrates without image and color accuracy. Many plant fibers are compressed into paper. Common substrate properties include that some transparency will always exist. Faced with light, the opposing side will mix through, therefore manufacturers embed subtle layer-security components. Also applies to polymer substrate, latent images, component visibility is restricted. Layers are randomly woven using colored security fibers. While holding a note to a light source, individual threads appear under UV-lit threads shine. Fake notes with fake threads or fibers appeared. These fakes are inserted and drawn on, making forensic analysis easy. They're not clear to most people. Like the security fiber, the security strip or thread is usually one thread, inserted between note layers, usually a metallic thread, occasionally with Bangladeshi Takka notes include strip micro-text. A windowed thread unique variety, harder to manufacture since threads weave in and out of the note surface, typically 10 mm spans. Normal view shows disconnected metallic pieces. The strip appears as a continuous thread when illuminated. Typically phony attempts are obvious. Discontinuous printing or drawing is widespread, tiny metallic ink lines. Planchets, one-millimetre disks, are implanted. Throughout banknote. When illuminated, the disks appear like watermark, security fiber, windowed thread. Plans come in many forms. Disks that react solely to UV light or show through in regular light. Light planchets can have micro-printing and micro-text for security. Moiré patterns are optical illusions with various variants, are absent. These are secret measures only revealed by unauthorized parties. Such measures are called screen traps.
Digitizing a real note and printing it gives the effect, from digital file. Printer Benjamin Franklin supported paper. money over precious metals, he purposefully misspelled ‘Pennsylvania’ to capture spelling-corrector forgers. His second move was more sophisticated. Actual leaf was included in the printing process, creating delicate leaf veins, incredibly tough to recreate by hand-etching copper plates, the only method. accessible , this design complexity has stood out for paper currencies, security defense nowadays. Security patterns are complicated geometrical repeating designs with fine detail. It still makes hand-forging banknotes difficult. The company leads in security by utilizing the fact that existing desktop publishing technologies cannot generate complex pictures. Detail in Intaglio and Offset Lithography. Guilloché, a medieval armor and pottery security design, was first employed. applied to Dutch National Bank paper currency (AD 1814). The Guilloché from simple repeating symmetrical design to sophisticated spirographical design.

Intaglio printing produces a latent image only under certain conditions. Huge pressure makes a fine raised ink pattern changeable, unlike the foreground. This is done by printing perpendicular lines to indicate a Viewing angle affects foreground and background. Limitations exist, latent Damage to the Intaglio print press limits image viewing angles. Tactile relief declines. Although counterfeiters cannot replicate latent pictures without specific equipment, purpose Intaglio print press machines, whose sale and possession are tightly regulated by authorities. Their security is weak for frequent use. Austria, Germany, Switzerland, and others employed latent pictures before the Euro. Given the inevitable wear and tear, this may not become a standard. Traditional chapter or section vignettes are rich and detailed. section dividers in books, usually good for monetary protection. Vignette Most currencies have examples, but the Australian dollar is notable. Australian polymer $5 notes from 1992 include a vignette inside the transparent. window, showing that security components can be merged to create more complex barriers for counterfeiters, although their usage alone is doubtful. Not all scanners, copiers, and desktop publishing applications can recreate documents. Screen traps detect anti-copy marks. Plan is to prevent attack by After capturing an image, image recognition checks for banned images. take occur. Software or devices will refuse to load forbidden security images. Continue supposedly preventing unauthorized reproduction. However, this is sound. restriction, software or hardware must have such measures embedded or screen trap fails. Euro notes include the EURion constellation, five circles in all. separation, size, proportion, and color. A tailored copier, scanner, or software EURion stops and removes documents with this pattern. give the user an error message. Tests reveal the constellation must be of precise readings and color qualities if the constellation changes even much Copying, variation are conceivable. Screen traps may contain concealed information that changes printed material when copied. output, like writing word copy across a page to nullify it . Similar This metric uses typical optical effects and is more resilient than the Moiré effect. occurring in nature than on software activities. Some laser printers generate yellow dots sequentially, making the gadget recognizable. These yellow dots are hidden codes that determine manufacture and model. Similar steganographic methods are shown in bicolor printed sheets by pseudo-randomly dispersing tiny black dots, preliminary studies demonstrate that unlike prior methods, this method may be used on any bicolor document with visuals, not just numbers. When calculating screen trap effectiveness, security strength might be used.

Printing methods include thermal injet, dry electrophotographic, and liquid electrophotographic. Investigating color-tile, standard barcode, and 2D, color-tiles prove to effectively measure color fidelity. Such findings enable discrimination. Recent documents with monotone ink from long-term light lack Thus, conventional and 2D barcodes seem more reliable. Paper watermarks are intentionally thin to increase visibility. more transparent than the rest of the paper to let light in. A watermark is implanted using the dandy roll or cylinder molding process. As pulp comes out the vat, virtually entirely water, the water is compressed. Fibres by pressing a wire stencil against the pulp before drying. remains. Numerous attempts have been made to stamp the watermark on this impression. recreate watermarks. Even though watermarking is almost as old as paper forgeries have failed. Art Williams, the US maestro, When counterfeiter inserted a central substrate layer with a hand-drawn watermark, A semi-passable facsimile watermark appeared when held up to light. Optical Variable Watermark improves typical watermarks. A sequence of pulse width micro holes are placed directly in polymer substrate, modulated pixels. The framework has two channels are interlaced so each second row shows a different image. Phase modulation embeds a secret payload in each layer. Superposing layers with different carrier structures using the correct combination is called the 'key'. This seems possible for one-time, Authenticating diplomas and certificates with one key particular document, banknote key management is difficult. A new method watermarks photos with a payload, data integrated by Peak Position after DSS processing Modulation. The majority of watermarking methods embed data in one color. in each color component separately. Microtext, printed inconspicuously, is often only visible, magnifying glass or microscope. Traditional desktop publishing cannot render Guilloché-like text. Text forgeries are detected. as a line, higher-end desktops may render it, however as we When magnified, edges blur. Serial number uniquely identifies each banknote and is stored in a database On real cash, serial numbers never repeat, many Serial number repetition has revealed fraudulent attempts. The exact procedure for creating serial numbers changes from one country to the next. Clearly the serial number is a simple yet effective security precaution. The serial number allows issuing authorities to track the circulation of cash. ATMs and banknote sorting machines assess this by character recognition techniques, comparing values stored in the database. The age of ink can be established using many means such as the secret service ink database, perhaps enabling automated identification of counterfeit additionally employing valid duplicated or cloned serial numbers distinguishing the ink age against the reported serial number age.

C) Validation of Security Components

Enhanced security measures for paper currency are integrated through external authentication devices in ATMs and automatic banknote sorting machines. By utilizing banknote recognition software, you can effectively manage the circulation of counterfeit and damaged banknotes for disposal. Here is a brief overview of the software, focusing on three main functions: image processing, feature extraction, and classification. Once the banknote image is captured, it needs to undergo pre-processing to isolate specific characteristics of interest. Initially, it is important to identify and capture the edges of the banknote image. Usually, preparing an image of a banknote involves a binarization stage, an edge detection stage, and distortion correction. Utilizing a modified Canny edge detection technique is employed for eliminating noise and background from captured images. The Canny algorithm identifies a point as an edge based on the amplitude compared to its neighbors, without verifying if the differences exceed a certain threshold. As a result, the algorithm becomes highly responsive to faint edges, especially in areas with similar colors or image blurriness. Conventional line fitting methods are inadequate for banknote recognition due to the presence of erroneous edge points in images. The Hough transform is utilized to identify paper edges and eliminate distortion, drawing from Optical Character Recognition (OCR) methods. The Hough transform method is ideal for identifying banknotes that have been in circulation due to its capability to detect lines in images with gaps. Image segmentation heavily relies on the thresholding technique. Thresholding enables applications to distinguish and isolate a specific target from the surrounding background of varying grayscale levels or textures within image objects. Identifying the appropriate threshold value involves utilizing adaptive thresholding [29]. This approach demonstrates resilience to significant variations in lighting, allowing the system to function effectively in diverse environments. Getting the correct data at the beginning is crucial before moving on to the next stages. Identifying particular features is crucial for verifying authenticity, which depends on choosing the right security elements. Most of the existing research emphasizes extracting specific regions of interest to analyze banknote color, printing quality, and image accuracy. When analyzing a banknote image, it is typically divided into smaller sections for individual template matching processes. Each subsection utilizes a threshold, which contributes to a threshold ratio or T-ratio. Utilizing LBP and BP network methods, the entire paper currency image is divided into M×N blocks, with each block undergoing a Local Binary Pattern (LBP) process. Every pixel in the block is computed and given an LBP value based on its pixel value. A histogram is created for each block to simplify the histogram dimensions, and the LBP values are quantized. Some currencies use a wide range of colours, this is especially vital when the colours used are close to each other in both location on the colour spectrum and physical location. In a digital image processing approach incorporates concepts such as eigen-face and Principle Component Analysis (PCA) to recognize U.S. banknote denominations for visually impaired individuals through smartphones. An expert in printing technology would understand the PCA functions for image feature extraction and compression. PCA is ideal for extracting features from banknotes due to their high quality nature and the abundance of classification data available. Time is a crucial factor when integrating smart detection devices into ATM and banknote sorting machines. The PCA is utilized to identify the essential features, ensuring that only relevant elements are being examined. After extracting the data, the Self-Organizing Map (SOM) model is utilized to cluster the data into similar regions. The SOM creates a map that represents the data distribution, allowing the regions on the map to be understood as clusters in the data space. Utilizing Speeded Up Robust Features (SURF), which draws inspiration from Scale Invariant Feature Transform (SIFT). Identifying an image of a banknote in any orientation can be achieved through feature selection based on the location of interest points. Banknote images can be easily recognized in different environments, orientations, and distances from the camera with a 100% accuracy level, as demonstrated by tests. This would be an attractive option when considering development of surveillance devices detecting fraudulent currency for instance Closed Circuit Television (CCTV) footage located in a convenience store. Utilizing Discrete Wavelet Transform (DWT) for scaling and shifting alongside Packet Wavelet Analysis (PWA), and Maximum Overlap Algorithm (MOA). This method is ideal for extracting features in situations where issues like wrinkles and holes due to wear and tear are challenging. In developing countries, currency tends to stay in circulation for extended periods, increasing the chances of counterfeit notes remaining undetected. It's crucial to consider wrinkles, holes, dust, and discoloration caused by age when handling notes. When applying

geometric masks to specific areas of interest, the character is determined based on the number of pixels obtained. Utilizing single masks is not enough; Axis Symmetric Masks (ASM) enhance accuracy by incorporating various geometric shapes to gather additional data about the area. Feature classification involves the use of different machine learning and pattern recognition methods. Utilizing established values or templates for comparison, the threshold is determined based on previous characteristics. Embracing a flexible approach to understanding the medium is more beneficial than imposing rigid values that could limit creativity. Artificial Neural Networks (ANN) are frequently utilized in a variety of publications. Combining Genetic Algorithm (GA) with Back-Propagation (BP) has been explored in various studies. Performance improvements were noted in each instance when using ANN in combination with other methods. An ensemble neural network (ENN) consists of a finite collection of neural networks trained to perform the same task, with input vectors applied simultaneously to all networks in the ensemble. For diversity among the individual ENN networks, Negative Correlation Learning (NCL) is utilized. It has been noted that notes with more noise are classified more accurately compared to single NN. There is a study that shows a Counter Propagation Network (CPN) is more accurate for banknote classification compared to BP. Through the utilization of a Bi-directional Associative Memory (BAM) technique, a recognition rate of 96.08% was achieved, with the remaining items being uncategorized due to wear and tear. Support Vector Machines (SVM) are commonly utilized in various research studies and offer a diverse range of potential applications, including banknote classification.

SVM has been effectively utilized to identify serial numbers on banknotes, and for detecting stains to assess the condition of banknotes. The results indicate that the classification accuracy is similar to that of ANN. However, it has been found that utilizing multiple kernel SVM can enhance accuracy and overall performance. Vector Quantization (LVQ) was introduced by tt is considered less efficient in comparison to other algorithms. As noted in a previous study, utilizing PCA prior to classification aims to enhance reliability. However, this approach necessitates a follow-up clustering step to address the intricacies of the classified data, ultimately impacting the overall performance. An AdaBoost machine learning algorithm was utilized on the N most discriminating features. The ratio between red and blue intensity channels is then measured for those areas. Using color channels instead of grayscale intensity channels leads to a notable enhancement in classification performance with identical training sets. Utilizing Hidden Markov Models (HMM) with Gaussian techniques, a study was conducted comparing HMM, SVM, and ANN. One study revealed that HMM achieved the highest performance with 93.92%, followed by ANN with 92.8% and SVM with 88.52%. Seems like an appealing choice because of its higher classification accuracy. Additionally, it can learn feature sets over time, allowing us to fine-tune for specific checks using distinct features. The security printing industry is constantly evolving technologically, requiring both forensics and public authentication devices to keep up with the advancements. There is still unexplored potential in polymer security substrate characteristics, security fibers, security threads, and watermark authentication.

D) Systems for Component Analysis

Several tools and systems have been created to verify banknotes by analyzing specific security features. Most of the focus is on identifying incorrect or duplicate serial numbers, as well as evaluating image quality. Despite extensive research on new document security techniques, issuers continue to primarily depend on checking these traditional components. Identifying a specific banknote is crucial, as some currencies can trace back to the machinery used. The Euro currency comes with a prefix that indicates the country of issue. Manufacturers of intaglio print press machinery are closely monitored by authorities like Interpol and the US Secret Service. Serial numbers help forensic examiners determine the origin of genuine notes. An affordable microcontroller device has been developed, indicating that specialized devices for authentication tasks can be created and utilized as needed. Serial number recognition plays a crucial role in banknote security and currency forensics applications.An integrated hardware and software solution is offered by to differentiate between genuine and counterfeit Euros banknotes, achieved by using a near infrared camera to capture the banknote image. This method also gives us the Euro's denomination. Physical currency, like banknotes, will continue to be popular for the foreseeable future. However, there has been a noticeable trend towards the adoption of electronic currency in recent years. Electronic currency introduces a fresh perspective on currency security and forensics, covering various forms such as debit cards, Electronic Cash (e-Cash), and virtual money.Here, a comprehensive analysis is carried out to create a cohesive understanding of the differences found in the literature, focusing on their significance for currency security and forensics. Noticing the absence of regulation over numerous lesser-known variations could explain the growing number of incompatible models. Mobile Cash (m-Cash) architectures enable users to securely withdraw physical cash from ATM machines by using smartphones with compatible RFID tags and ATMs equipped with RFID readers. This involves a secure architecture where users have the option to withdraw paper money through their phone instead of using the traditional Personal Identification Number (PIN). Mobile payment architectures facilitate direct transactions between individuals, businesses, and combinations of both. Various options are available for linking the phone to a Subscriber Identity Module (SIM) card, personal bank account, or temporary deposit account resembling a prepay system for exchanging credit for goods and services. The access level in the mobile payment model directly impacts the associated risk. When a SIM card is connected to a personal bank account, the user may face greater risks of incurring significant losses compared to using temporary deposit accounts. It is crucial to have adequate security measures in place to mitigate the risks associated with person-to-person transactions over wireless networks using mobile devices. The main focus is on ensuring the security of public networks and the communication protocols used for encryption. Electronic cash or (e-Cash) system is closely tied to physical paper currency. Surprisingly, e-Cash can offer anonymity. An electronic cash scheme allows users to withdraw money from a bank and spend it anonymously, using cryptography and one-way hashing functions. A recommended e-Cash scheme is suggested, a user can provide cash for payments offering multiple instances of the same e-Cash item. Nevertheless, the merchant can only proceed with the transaction after a third party has endorsed the e-Cash instance, like an issuing entity or trusted authority, which helps prevent double spending. There are architectures for e-Cash where virtual currency is transferred and managed on a server. The currency remains in a holding location until the transaction is confirmed through the endorsement process and ultimately finalized. After the transaction is confirmed through the endorsement process, the currency or funds are transferred to the recipient's account. Anonymity is ensured for users through blind signatures, utilizing cryptographic protocols. The proposed e-Cash transaction architecture incorporates the RSA public key cryptography system. While the transaction remains concealed from third parties, maintaining this level of anonymity may result in a loss of security, including crucial information that could aid in detecting money laundering during audits. A proposed method suggests trust relationships in

the form of rings of trusted banks. Only trusted third parties, specifically banks within the same ring, may have knowledge of the users' transactions. Anonymity is limited to trusted third parties. Famous websites and online communities like iTunes, Facebook.com, and World Of Warcraft (WOW) provide options for using real money to purchase virtual currency.

This digital currency is used within specific online platforms, like in-game marketplaces where users can buy, sell, and trade virtual items such as weapons in games like WOW, or purchase apps and music on platforms like iTunes. There has been a recent comparison between one-way and two-way virtual currency exchanges, revealing that many operators are not required to offer two-way exchange and usually do not. It seems that this will result in a decrease in profits and issues with physical money, ultimately showing that mutual exchanges are advantageous for both operators and users in the future. An innovative solution to this issue called Common Money (CONEY) has been recently introduced, focusing on managing virtual currency within local jurisdictions. Every area establishes and manages its own virtual currency that can be used interchangeably with traditional money. The architecture demonstrates the seamless integration of local virtual currency and local physical currency. Personal accounts are connected, allowing for transfers from digital to physical within one's own jurisdiction overseen by local servers. Many issues arise when it comes to electronic currency, especially in terms of security and forensic analysis. One of the main concerns is ensuring the safety of cryptographic protocols for data transmission. There are numerous opportunities for money launderers to exploit due to the lack of governance in the electronic realm. Concealing an electronic trail by manipulating blind signatures and utilizing various obscure entities offering virtual currency services can obscure transaction details. An up-and-coming area of research involves hybrid electronic-physical currency. So far, the main focus has been on combining Radio Frequency Identification (RFID) devices with paper currency. Research indicates the use of RFID devices for banknotes.

Banknotes are equipped to convey signatures for authentication to merchant devices. Proposed as a potential security component for banknotes are RFID tags embedded with encoded spectral signatures in printable thin flexible substrate circuit. RFID technology has been utilized for tracking notes by law enforcement and authentication by merchants. Security measures such as adding memory cells and implementing challenge response protocols have been shown to prevent unauthorized access. Proposing a system to manage paper currency for distributing uniform size wads of banknotes. An antenna utilizing an Ultra High Frequency (UHF) dipole tag with a short stub and meander lines. RFID management systems are useful for supply chain management. Streamlining the process of banknote distribution to local bank branches reduces the likelihood of human error in recording track and trace details of in-transit wads.

XI. UPCOMING SCOPE IN SECURITY DOCUMENTS

It may not be long before electronic currency replaces paper currency. Physical currency will continue to be used for the foreseeable future. Several factors contribute to this phenomenon:

(1) a perceived anonymity during transactions

(2) inadequate infrastructure in many parts of the world for electronic currency

(3) a general distrust due to recent media reports of security breaches

(4) a sense of national pride reflected in the unique artwork on local currency.

Based on the current trend, it seems that physical paper-based currency will persist in the near future, possibly due to the cost advantages favored by most substrate manufacturers. Polymer banknotes, despite the higher initial cost, seem to be increasing in popularity. Countries like Australia, New Zealand, Romania, Singapore, and Vietnam have completely switched to polymer notes. All these nations have noted a reduction in the expenses linked to their extended lifespan and a decrease in the number of counterfeit products compared to the previous ones. Louisenthal, a leading manufacturer of security paper substrates, has introduced a new hybrid-paper substrate made from polymer. This integration demonstrates that the advantages of polymer are being recognized not only by countries that have fully embraced it, but also by security paper manufacturers who can offer it as an alternative to their customers. Research in banknote security and counterfeit detection is expanding, focusing on developing software for smart devices that are integrated into ATMs and central banknote sorting machines. While many devices prioritize traditional aspects such as serial number and print quality. Installing security detection devices at ATMs to monitor and prevent the circulation of fake money to central locations for disposal has become a standard practice. While most existing literature focuses on paper currency, there is a noticeable demand for research on polymer. It has been noted that polymer has distinct surface characteristics. Authenticating these characteristics could impact future research and development aimed at machines recognizing specific intrinsic features of polymer. Examining signature or printer profile analysis can enhance the forensic investigator's confidence by potentially linking document origination to specific printers.

Displayed, anomalies can be identified and quantified to generate a unique signature using pixel distribution and satellite droplets. Similarly texture analysis of paper investigates various qualities of the texture and roughness of surfaces relating to documents and banknotes, similarly investigates the texture of the ink pattern. Understanding the categories of ink, paper, and printing methods is crucial for forensic analysis and the development of security features in banknote recognition software. Security features like watermarks, security fibres, security threads, and security patterns seem to be some of the oldest yet most effective methods for preventing counterfeit attempts.

Basic efforts have been demonstrated to disrupt initial security measures, but seem to be commonly identified through electronic scrutiny by the mentioned ATMs and currency sorting devices. Embracing innovative methods is essential to remain at the forefront of advancements in technology, such as exploring different types of holograms like the Kinegram and implementing cryptographic techniques with RFID technology. The move towards electronic currency as a medium seems to be firmly established and likely to endure, just like how RFID technology enables electronic currency through cryptographic algorithms. Historically, credit and debit

cards have been the main payment methods. In recent years, there has been a significant increase in the range of electronic currencies, including virtual currencies used for online community transactions and mobile person-to-person or person-to-business payments. There is still a lot of infrastructure that is not compatible with each other and lacks proper governance. Suggestions have been made for the adoption of interoperable governed virtual currency systems.

The physical currency will remain in circulation for the foreseeable future, with polymer banknotes providing enhanced security features compared to paper notes. Most of the research conducted so far has been centered on creating devices to detect worn-out and counterfeit notes in ATM and central bank note sorting machines. Distinguishing between a worn-out or counterfeit note and an authentic one in good condition relies on image fidelity. Studying the texture analysis of paper and ink is making progress in identifying the specific printer make and model used.

There is currently limited research in the field of forensic science that specifically focuses on currency in comparison to other areas. Exploring various fields of study was essential to establish a strong base. It was crucial to grasp the intricacies of security printing processes, the properties of substrates and inks, as well as the challenges posed by integrated security features. There is a wealth of research on the use of computer vision and machine learning in ATM and banknote sorting machines. Exploring this field involves examining the substrate surface texture, pixel distribution patterns, ink pigments, fluorescence levels from different areas of the note, and detailed analysis of elements like watermarks and overall design. In the end, what is desired is a strong form of currency that is resistant to both forgery and wear, with polymer being the most recent innovation in banknote material. Even polymer is susceptible to counterfeiting, and it seems that the level of sophistication is increasing. Given the innovative nature of polymer, it is crucial for the forensic field to be prepared to detect forgery. Studying the interaction between ink and polymer could help identify the age of ink on polymer substrates. When examining the ink used in the forgery, analyzing its commercial origin and material composition can help pinpoint the location and kickstart the investigation. There are numerous facets of physical currency that remain unexplored, such as watermarks, security threads, and fibers, which are among the oldest and most straightforward yet highly effective methods for securing documents. While some have tried to replicate these methods, they are not recognized by banknote authentication devices. There is a need to review the governance of electronic currency systems due to its current shortcomings. There have been suggestions for models to combine virtual currency and physical currency to bridge the gap. It is essential to review systems for integration models, taking into account jurisdictional issues that define rules and regulations when systems collaborate with each other in this widespread paradigm.

XII. CONCLUSION

The latest advancements in the field of forensics related to currency security. Conducting a survey was essential since there is a lack of existing research focused on counterfeit currency or electronic fraud from a forensic investigator. Exploring the history of currency helps us understand its evolution into what we use today. Money has existed for centuries and has come in various shapes and sizes. To identify defects and analyze with scientific validity, it is essential to comprehend the process of currency production. We should also explore the composition, raw materials, and special features like watermarks, security threads, and micro-text, and how they all work together. Every element possesses distinct characteristics that gradually reveal themselves throughout the currency series. Electronic currency has become the primary medium for exchange, with its various forms making it challenging to define. Describing the situation is made more challenging by the fact that the different types are frequently incompatible with each other and with traditional currency, all while lacking governance. Even with the rise of electronic transactions, paper money still offers advantages over electronic currency, such as complete payment anonymity and a more controlled form of currency. Banknotes are crafted through a meticulous engineering process that combines stunning artwork with optical security features. Most people do not actively seek out established security features; they tend to trust products that appear and feel genuine at first sight. As shown above, the first layer represents one of the three layers of banknote security. Primarily, the initial layer is what humans can easily recognize at first sight and feel. Further exploration is needed, such as using UV light or a magnifying glass. The third one combines those characteristics that need further analysis in a specialized laboratory. In the past, the intricate design of paper currency served as a strong form of protection. Replicating the artwork demanded a high level of expertise and creativity. Today's quality and complexity remain a significant challenge, as intricate designs are still not achievable with commonly available reprographic equipment. With ongoing technological advancements, desktop publishing capabilities are constantly improving, potentially making design less of a barrier and more of a traditional element. In the past, banknotes have been verified by highly trained professionals known as Questioned Document Examiners (QDE). These experts assess factors such as ink quality, print quality, paper type, and handwriting features. The Secret Service was initially tasked with combating counterfeiters of US currency and remains a leader in currency forensics. Successful counterfeiters achieve their goals through determination and access to resources. It's fascinating how the security features of banknotes keep advancing, while counterfeiters also enhance their skills and resources. Banknote sorting and authentication systems are widely used by banks globally, integrated into ATMs and central banknote sorting machines. These devices assess the color quality and features of the note. If the specific threshold is not met, the note is considered either counterfeit or no longer suitable for circulation. It is crucial for safeguarding a nation's economy. Those involved in counterfeiting may focus on perfecting specific security features to pass them undetected. Thus, a comprehensive approach is necessary. While it may seem like a distant concept, the notion is that verifying all components will enhance the security of the currency system. The banknote polymer substrate is becoming increasingly popular, to the point where the well-known

security paper manufacturer Louisenthal has embraced it by introducing a hybrid paper-polymer note. However, there is very little research on polymer currency. It is evident that there is a necessity to create techniques for currency forensics that focus on advancing towards specialized automatic polymer banknote authentication devices, leveraging the distinct intrinsic features of polymer.

REFERENCES

[1] R. R. Pearce, "SECURITY DOCUMENT". United State Patent 4186944, 05 Feb 1980.

[2] H. P. M. Joseph Shulman, "PROTECTIVE COATINGS FOR DOCUMENTS". United State Patent 4428997, 31 Jan 1984.

[3] P. H. Skene, " FOIL EMBOSSING METHOD". United State Patent 4503110, 05 March 1985.

[4] R. L. v. Renesse, "Optical Inspection Techniques for Security Instrumentation," in *Optical Security and Counterfeit Deterrence Techniques*, United State, 1996.

[5] R. L. v. Renesse, "Security design of valuable documents and products," in *Electronic Imaging: Science and Technology*, San Jose, CA, United States, 1996.

[6] J. Pieters, "Trends in security evaluations," in *Electronic Imaging: Science and Technology*, San Jose, CA, United States, 1996.

[7] S. Spannenburg, "Optically and machine-detectable copying security elements," in *Electronic Imaging: Science and Technology*, San Jose, CA, United States, 1996.

[8] P. J. Harrop, "Smart printing technology for counterfeit deterrence," in *Electronic Imaging: Science and Technology*, San Jose, CA, United States, 1996.

[9] H. Souparis, "Combined machine-readable and visually authenticated optical devices," in *Electronic Imaging: Science and Technology*, United States, 1996.

[10] J. H. Lemelson, "BAR CODES AND METHODS". United State Patent 5563401, 08 Oct 1996.

[11] S. K. Harbaugh, "DETECTOR FOR A SECURITY THREAD HAVING AT LEAST TWO SECURITY DETECTION FEATURES". United States Patent 5535871, 16 July 1996.

[12] Wittich Kaule, "SECURITY DOCUMENT AND A METHOD FOR PRODUCING IT". Unites States Patent 5516153, 14 May 1996.

[13] T. T. Crane, "SECURITY THREADS HAVING AT LEAST TWO SECURITY DETECTION FEATURES AND SECURITY PAPERS EMPLOYING SAME". United States Patent 5486022, 23 Jan 1996.

[14] A. Dames, D. Ely and C. Ager, "HARMONIC-BASED VERIFIER DEVICE FOR A MAGNETIC SECURITY THREAD HAVING LINEAR AND NON-LNEAR FERROMAGNETIC CHARACTERISTICS". United States Patent 5614824, 25 March 1997.

[15] M. R. M. Knight and Duncan H. Reid, "SECURITY THREAD, A FILM AND A METHOD OF MANUFACTURE OF A SECURITY THREAD". Unites State Patent 5631039, 20 May 1997.

[16] R. L. v. Renesse, "PAPER BASED DOCUMENT SECURITY - A REVIEW," in *European Conference on Security and Deteclion*, United States, 1997.

[17] G. T. S. K. R. L. C. D. P. I. R. C. L. J. Natarajan Ramachandran, "SERVICE METHOD FOR AUTOMATED BANKING MACHINE". United States Patent 6010065, 04 Jan 2000.

[18] R. L. v. Renesse, "Synergistic combination of document security techniques," in *Conference on Optical Security and Counterfeit Deterrence Techniques III*, San Jose, California, United States, 2000.

[19] S. V. N. W. E. M. M. Mallol, "Security element having a digitised mark and security support or document comprising same". France, Europe Patent EP1674286A1, 28 June 2006.

[20] H. B. W. S. A. B. Oliver Muth, "SECURED DOCUMENTS IDENTIFIED WITH ANTI-STOKES FLUORESCENT COMPOSITIONS". United States Patent 6686074B2, 03 Feb 2004.

[21] S. H. a. J. K. Wu, "Optical Watermarking for Printed Document Authentication," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,*, vol. 2, no. 2, pp. 164-173, 2007.

[22] J. D. H. M. D. D. K. F. Schützmann, "Security element for securing valuable documents". Germany Patent 102006055170A1, 29 May 2008.

[23] R. L. v. Renesse, "Optical Security and Counterfeit Deterrence Techniques VI," in *ELECTRONIC IMAGING*, San Jose, California, United States, 2006.

[24] A. W. S. S. HENRI ROSSET, "SECURITY SHEET". India Patent 22150, 24 Jun 2008.

[25] P. M. K. N. M. T. W. P. F. S. Gabriel IFTIME, "DOCUMENT AND METHOD OF MAKING DOCUMENT INCLUDING INVISIBLE INFORMATION FOR SECURITY APPLICATIONS". United States Patent 2008/0220187A1, 11 Sep 2008.

[26] F. J. P. HOWLAND PAUL, "A METHOD FOR PRODUCING A SECURITY DOCUMENT". India Patent 194182, 24 July 2009.

[27] X. L. a. B. Y. Wenfa Qi, "Bilinear Coons patch and its application in security pattern design," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Chengdu China, 2009.

[28] K. I. Z. V. Zijak, "CMYKIR security graphics separation in the infrared area," *Scinece Direct, Infrared Physics & Technology* , vol. 52, no. 2-3, pp. 62-69, 2009.

[29] A. D. P. D. C.-A. M. E. BLEIKOLM, "SECURITY DOCUMENT, METHOD FOR PRODUCING A SECURITY DOCUMENT AND THE USE OF A SECURITY ELEMENT". India Patent 240084, 30 April 2010.

[30] N. R. Z. W. Z. N G Shankar, "A real time print-defect detection ststem for web offset printing," *Science Direct-Measurement*, vol. 42, no. 5, pp. 645-652, 2009.

[31] G. A. J. A. M. S. Steven Simske, "New Findings in Security Printing and Imaging," in *NIP & Digital Fabrication Conference*, Louisville, KY, USA., 2009.

[32] M. H. B. W. André Gregarek, "SECURITY FEATURE AND METHOD FOR MANUFACTURING THE SAME". Unites State Patent 2010/0164217 A1, 01 July 2010.

[33] J. L. M. B. A. G. A. Verikas, "Advances in Computational intelligence-based print quality assessment and control in offset colour printing," *Science Direct- Expert System with Applications*, vol. 38, no. 10, pp. 13441-13447, 2011.

[34] M. m. S. Steven J. Simske, "SECURITY PRINTING ANALYSIS SYSTEM AND METHOD FOR ENHANCING SECURITY RINTING". United State Patent 8532330B2, 10 Sep 2013.

[35] J. C. &. W. Y. &. A. G. &. M. Kankanhalli, "Currency security and forensics: a survey," *Springer- Multimed Tools Applications*, vol. 74, no. 1, pp. 4013-4043, 2014.

[36] N. V. E. W. M. M. Stephane Mallol, "SECURITY ELEMENT HAVING A DIGITISED MARKAND SECURITY SUPPORT OR DOCUMENT COMPRISING SAME". United State Patent 8684417B2, 01 April 2014.

[37] R. B. o. India, "DBR No.Leg.BC.21/09.07.006/2015-16 - Currency Note Excahnge," Reserve Bank of India, Mumbai, India, 2015.

[38] R. B. O. INDIA, "Withdrawal of Legal Tender status of banknotes of ` 500 and ` 1000: Activity at Banks during November 10-27, 2016," RESERVE BANK OF INDIA, Mumbai, India, 2016.

[39] R. B. O. INDIA, "Issuance of ` 500 bank notes without inset letter, in the Mahatma Gandhi (New Series)," RESERVE BANK OF INDIA, Mumbai, India, 2016.

[40] R. B. O. INDIA, "Issue of ` 500 banknotes in Mahatma Gandhi (New) Series with the inset letter ‘E’ having ‘star’ mark in the number panel," RESERVE BANK OF INDIA, Mumbai, India, 2016.

[41] K. P. Chitra Thinger, "Guilloche Pattern for Security in Confidential Documents," *International Journal of Innovative Science, Engineering & Technology*, vol. 3, no. 10, pp. 376-378, 2016.

[42] R. B. O. INDIA, "RBI Introduces ₹ 200 denomination banknote," RESERVE BANK OF INDIA, Mumbai, India, 2017.

[43] R. B. o. India, "DCM(NE)No.G - 1/08.07.18/2017-18 - Master Circular – Facility for Exchange of Notes and Coins," Reserve Bank of India, Mumbai, India, 2017.

[44] G. D. R. RITTER, "OPTICALLY VARIABLE SECURITY THREADS AND STRIPES". France, Europe Patent EP2882597B1, 02 Feb 2017.

[45] I. S. K. S. T. Bozhkova*, "Overview of security printing types and trends in its future development," *Bulgarian Chemical Communications,* vol. 49, no. L, pp. 195-201, 2017.

[46] R. B. O. INDIA, "RBI Introduces 50 banknote in Mahatma Gandhi (New) Series," RESERVE BANK OF INDIA, Mumbai, India, 2017.

[47] R. B. O. INDIA, "RBI Introduces `10 banknote in Mahatma Gandhi (New) Series," RESERVE BANK OF INDIA, Mumbai, India, 2018.

[48] R. B. O. INDIA, "RBI to Issue New Design ₹ 100 Denomination Banknote," RESERVE BANK OF INDIA, Mumbai, India, 2018.

[49] R. B. O. INDIA, "RBI Introduces ₹ 20 banknote in Mahatma Gandhi (New) Series," RESERVE BANK OF INDIA, Mumbai, India, 2019.

[50] M. F. E. Feky, "Securing Helwan University Graduation Temporary Certificate against the risks of forgery and counterfeiting by using security features," *Semantic Scholar -Computer Science,* vol. 1, no. 1, pp. 1-9, 2020.

[51] P. D. X. L. F. Y. ,. Gebhard Ritter, "OPTICALLY VARIABLE SECURITY THREADS AND STRIPES". United state Patent 10,166808B2, 01 Jan 2019.

[52] R. B. o. India, "SECD/BRDS.S147/02.16.001/2023-24 - Annual Report 22-23," Reserve Bank of India, Mumbai, India, 2023.

[53] H. B. W. S. A. B. Oliver Muth, " SECURED DOCUMENTS IDENTIFIED WITH ANTI-STOKES FLUORESCENT COMPOSITIONS". United State Patent 6686074B2, 03 Feb 2004.