JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

BSC. INFORMATION TECHNOLOGY

PROJECT TITLE: AUTHENTICATION OF BANKNOTES USING MACHINE LEARNING

STUDENT NAME: TITUS UKILI

REGISTRATION NUMBER: SCT221-C004-0375/2020

SUPERVISOR: MS. JUDY GATERI

This project has been submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Information Technology in the year 2023.

DECLARATION

I declare that this proposal is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: ____________________________ **Reg, No._____________________**

Sign: _________________________ **Date: ________________________**

Supervisor Name: ____________________________ **Date: ______________________**

Sign: ____________________________

ACKNOWLEDGEMENT

My sincere gratitude goes to my supervisor Ms. Judy Gateri who has been instrumental in the development of this project. She has walked with me from the beginning of conceptualizing this topic which was a sketchy idea to a solid academic project. The dedication and her profound wisdom, guidance and encouragement throughout this research has resulted to this work.

DEDICATION

I dedicate this project to my family and friends who have encouraged me throughout this journey. Special appreciation to my parents who believed in me and have supported me morally and financially.

List of figures

ABSTRACT

The authentication of banknotes is of paramount importance to safeguard financial transactions, ensure economic stability, and maintain public trust in the monetary system by preventing the circulation of counterfeit currency. This study outlines a banknote authentication system leveraging the use of supervised machine learning techniques. The system's core objective is to discern between genuine and counterfeit banknotes, employing supervised learning methodologies and compares the performance of three algorithms Random Forest, Logic Regression and Support Vector Machine. We use dataset from UCI that is specifically preprocessed for training classification models, utilizing features like Kurtosis, Variance, Entropy and Skewness to determine genuine and fake currency. Through extensive experimentation and model testing, the Random Forest algorithm demonstrates its efficacy in accurately classifying banknotes. Performance metrics, including accuracy, recall, and F1-score, underscore the algorithm's robustness. Notably, hyperparameter tuning enhances the Random Forest model's superiority over alternative methods. This banknote authentication system, built on the foundations of machine learning, stands as a testament to the potential of advanced algorithms in fortifying the security of financial transactions.

Table of Contents

CHAPTER ONE

1.0 Introduction

1.1 Background Study

Usually, individuals tend to receive banknotes as change from others or during point-of-sale transactions without actively confirming their legitimacy (Klöne et al., 2019). People often refrain from verifying authenticity because counterfeit rates are exceedingly rare, and there is a high level of trust in the retailer (van der Horst et al., 2017). Indeed, instances of authentication might be relatively rare. For instance, they could occur when the individual handling the cash has previous experience with counterfeit banknotes or when the texture or feel of a particular note raises some suspicion. Additionally, when there is a lack of trust in a specific transaction, such as an online purchase involving cash, individuals may opt to verify the authenticity of the banknote.

A more realistic limitation is that the general population possesses limited knowledge about the process of authenticating banknotes. Typically, individuals can only name two security features but they lack precise knowledge of the appearance of these features and their specific locations on a banknote (van der Horst et al., 2017). As a result, a significant portion of counterfeit banknotes remains unnoticed. As an example, van der Horst et al. (2017b) found that approximately 20% of counterfeit banknotes were not detected, even when participants were actively engaged in the authentication process and had all the time they required for the task.

It wouldn't be unfounded to presume that the percentage of undetected counterfeit banknotes is significantly higher in everyday situations, where individuals handling cash aren't explicitly instructed or motivated to verify authenticity. Another factor that may discourage individuals from verifying the authenticity of a banknote is the concern that the authentication process could create a socially awkward or uncomfortable situation. This discomfort is amplified by the fact that the limited knowledge about authentication features would likely prolong the process. If individuals handling cash could authenticate banknotes swiftly and discreetly, it's possible that fewer counterfeit banknotes would escape detection. Moreover, if the authentication of banknotes were made more convenient, it might discourage counterfeiters from attempting to use fake currency in the first place.

1.2 Problem Statement

The widespread circulation of counterfeit banknotes poses a significant challenge to the integrity and security of financial transactions and institutions. Counterfeit currency not only results in financial losses for individuals, businesses, and governments but also erodes public trust in the currency and financial systems. Despite existing efforts to authenticate banknotes, there is an urgent need to enhance and modernize authentication methods to effectively detect counterfeit currency and ensure the continued integrity of financial systems.

Current banknote authentication methods often suffer from limitations such as low detection rates, time-consuming manual verification processes, and vulnerability to increasingly sophisticated counterfeit techniques. Furthermore, the lack of widespread knowledge among the general public regarding banknote security features contributes to the acceptance of counterfeit currency in everyday transactions.

This project aims to address these challenges by developing and implementing an advanced banknote authentication system that leverages cutting-edge technology, machine learning algorithms, and computer vision techniques. The system's objectives include improving detection accuracy, reducing verification time, and providing accessible and user-friendly authentication tools for both financial institutions and the general public. By doing so, we aim to mitigate the impact of counterfeit currency on financial stability, protect the interests of individuals and businesses, and uphold public trust in the currency.

This problem statement serves as the foundation for our efforts to develop innovative and reliable banknote authentication solutions that safeguard the financial interests of individuals, businesses, and nations.

1.3 Research Questions

1. What are the most reliable and robust features or attributes that can be extracted from banknotes to distinguish genuine from counterfeit notes?
2. What are the most effective machine learning algorithms for banknote authentication?
3. What are the trade-offs between different machine learning algorithms (e.g., decision trees, neural networks, SVMs) in the context of banknote authentication?
4. How can transfer learning and pre-trained models be leveraged to improve the efficiency and accuracy of banknote authentication?

1.4 Objectives

1.4.1 General Objectives

The objective of this project is to develop and implement a machine learning-based system for authenticating banknotes through classification to determine whether a banknote is real or fake.

The objectives of the study are:-

1. To collect a comprehensive dataset of authentic and counterfeit banknote images, including various denominations and security features.
2. To preprocess the dataset by cleaning, augmenting, and standardizing the images to ensure consistency.
3. To identify and extract relevant features from the banknote images, such as variance, skewness, kurtosis and entropy.
4. To develop and train a machine learning model using the preprocessed data.

1.4.2 Deliverables

1. Banknote Authentication System: The system will be capable of accurately verifying the authenticity of banknotes.
2. Machine Learning Models: Provide the trained machine learning models that enable the system to recognize genuine and counterfeit banknotes.
3. Training Materials: provide data sets that will be needed to determining whether a banknote is real or fake.

1.5 Justification

This study helps maintain trust in the financial system. When people have confidence that the currency they are using is genuine, they are more likely to participate in economic activities, such as spending and investing.

In addition to counterfeiting, authenticating banknotes is crucial for preventing fraud in various financial transactions, including cash payments and withdrawals. It helps ensure that individuals and businesses are not unknowingly accepting counterfeit money.

Authenticating banknotes is vital for international trade. Counterfeit currency can disrupt cross-border transactions and damage a country's reputation in the global market.

Therefore, this study is of great importance to the individual, institutions, nations and the world.

1.6 Scope and Limitations

1.6.1 Scope

The primary purpose of this study is to develop a robust and accurate banknote authentication system using machine learning. This paper evaluates supervised machine learning algorithms to classify genuine and fake notes, and compares algorithms on the basis of accuracy, sensitivity, and specificity. The variables considered in the study include, Kurtosis, Variance, Entropy of image, Skewness and class. The context of application of the developed banknote authentication system will be in areas such as financial institutions, ATMs, or cash handling machines.

1.6.2 Limitations

The system maybe face some limitations like cases counterfeit banknotes are exceptionally well-made and may closely resemble genuine currency, making them difficult to detect even with advanced verification systems. Furthermore, Counterfeiters constantly evolve their techniques to mimic security features found on genuine banknotes. Verification systems may lag behind in adapting to these new methods. The condition of banknotes can be affected by factors such as dirt, folds, and humidity. In conclusion, Verification systems may have reduced accuracy when assessing the authenticity of banknotes in poor condition.

CHAPTER TWO

2.0 Introduction

The authentication of banknotes is a critical aspect of financial security and integrity in the modern world. Ensuring the legitimacy of currency is not only essential for financial institutions but also for individuals and businesses engaging in transactions. This literature review explores the various methods, technologies, and strategies employed in the authentication of banknotes. It delves into the extensive body of knowledge on this subject, examining the evolution of authentication techniques, emerging technologies, and the challenges faced in combating counterfeit currency. By delving into the existing literature, we aim to provide a comprehensive understanding of the advancements, limitations, and future prospects in the field of banknote authentication, ultimately contributing to a safer and more secure financial environment.

2.1 Literature Review

Money has played a role in human history for a span of at least 5,000 years, assuming various forms and representations along the way (Glyn Davies, 2016). Before that time, historians generally agree that a system of bartering was likely used. Historical records indicate that throughout the existence of physical currency, counterfeiting has been a persistent issue. The motivation behind counterfeiting, whether in the distant past or the present, is typically straightforward: the prospect of obtaining money with minimal effort, weighed against the risk of detection and punishment. Nevertheless, the methods employed for counterfeiting have evolved, with rapid technological advancements arguably simplifying counterfeiting while reducing the duration during which a currency remains resistant to such activities.

The act of counterfeiting existed before the widespread adoption of contemporary physical currency, such as coins and banknotes. Identifying the earliest form of currency is challenging, but one contender is the use of cowrie shells, which served as currency as early as 3300–2000 BC. These shells were also replicated using materials like ivory, bone, clamshell, stone, and, later on, bronze (Davies, 1994, Peng & Zhu, 1995).

Figure 1. Cowrie shells.

2.2 Coins and counterfeiting

Transitioning to the more recognizable forms of currency, early coins faced counterfeiting through various techniques. For instance, around 400 BC, Greek coins were frequently counterfeited by applying a layer of precious metal over a less valuable one (Markowitz, 2018). Another approach involved creating a mold from a genuine copper coin of lesser value, which was then filled with molten metal to produce a counterfeit. The prevalence of coin counterfeiting prompted the emergence of official coin inspectors tasked with the responsibility of weighing and dissecting coins to verify the metal composition at their core.

Coin 'shaving' or 'clipping' represented another commonly observed method of early coin deception, involving the gradual removal of silver coin edges, which were then melted down. In 17th century England, for instance, the weight of legitimately minted currency had fallen to half the legal standard, and approximately one in ten British coins was counterfeit (Levenson, 2010). To rectify this situation, all British coins had been recalled and reminted by the mid-1690s. Sir Isaac Newton, renowned for formulating the laws of motion and gravity and serving as the warden of the Royal Mint, was assigned the responsibility of preventing a recurrence of this issue. By the conclusion of 1699, he had successfully identified the primary counterfeiter as William Chaloner, who had produced counterfeit coins with a face value of £30,000 (equivalent to around A$10 million today). Chaloner was ultimately executed for his offenses.

2.3 Early Banknotes and counterfeiting

Early paper banknotes also fell victim to counterfeiting. Some of the earliest banknotes in history emerged during the Song Dynasty in China towards the latter part of the 10th century and were referred to as 'jiaozi' (Von Glahn, 2006). Initially, jiaozi were privately issued by various entities. However, in 1005, authorities restricted the right to issue jiaozi to only sixteen merchant houses.

To deter counterfeiters, elaborate designs, unique colors, signatures, seals, and stamps were employed on specially crafted paper. Counterfeiters caught in the act faced severe penalties, including the death penalty. Despite these measures, counterfeiting grew over time, leading to inflation. In 1024, the government assumed exclusive control over printing and issuing currency. Officially issued notes had a two-year lifespan, after which they could be redeemed with a 3 percent fee. This policy, possibly one of the earliest instances of a 'clean note' policy in history, aimed in part to prevent circulated currency from becoming overly worn and tattered. The introduction of higher-quality notes was intended to facilitate the differentiation between counterfeits and genuine currency.

2.3.1 Banknotes and counterfeiting history in the US

In 1690, the Massachusetts Bay colony introduced the first paper currency in the United States, denominated in British Pounds ("Paper Currency"). However, when the American Revolution erupted among the colonies, the initial U.S. paper currency lost its value due to rampant counterfeiting by the British and uncertainty regarding the war's outcome. Consequently, it wasn't until the mid-1800s that paper currency was reintroduced in the United States. During this period, as many as 1600 distinct types of paper money circulated in the United States, and up to a third of it was counterfeit ("Paper Currency"). To address this issue, the United States Congress sanctioned the issuance of a stable and universally accepted paper currency in 1863 (Warner, 2005).

Over the following two years, this widely accepted paper currency encountered numerous instances of counterfeiting. Consequently, President Abraham Lincoln established the Secret Service in 1865, with its primary mission being the eradication of counterfeiters. While stopping counterfeiters is a commendable effort, the ultimate objective is to prevent unauthorized duplication from occurring in the first place. In their book titled "Introduction to Security Printing," authors Richard Warner and Richard Adams articulate the aim of security printing by asserting, "Today's security printer aims to create documents, labels, packages, and cards incorporating multiple layers of innovative counterfeit deterrence measures while preserving the visual appeal and functionality of the printed product" (Warner, 2005).

2.3.2 Banknotes and counterfeiting history in Australia

The earliest forms of paper currency used in Australia did not resemble the fixed-denomination banknotes we are familiar with today. Instead, they were more akin to promissory notes or personal IOUs. These notes were redeemable for coins and were issued either by government authorities in exchange for goods or by private individuals. In the case of the latter, they were often simply handwritten on pieces of paper. Predictably, these early notes lacked significant security features, making them susceptible to counterfeiting.

On October 1, 1800, Captain Philip King, the Governor of the Colony of New South Wales, observed that "[due to] the indiscriminate manner in which every description of persons in the colony have circulated their promissory notes … numerous forgeries have been committed, for which some have suffered, and others remain under the sentence of death." While Governor King issued orders to standardize the issuance of such notes, privately issued handwritten notes continued to circulate and be counterfeited in the subsequent years (Vort-Ronald, 1979).

The issuance of proper banknotes in Australia commenced in 1817 with the Bank of New South Wales, which serves as the precursor to today's Westpac. Throughout the 1800s, various private banks (as well as the State of Queensland) continued to issue banknotes. However, the wide array of different notes created confusion among the public, and counterfeiters exploited this confusion by transforming low-value or essentially worthless notes into what appeared to be higher-value notes (Vort-Ronald, 1979).

2.3.3 Banknotes and counterfeiting history in England

In 1797, when the Bank commenced widespread issuance of its banknotes, they were crafted through the process of copperplate engraving. This method was concurrently employed in the creation of various other popular and transient printed materials of that era. Additionally, it was approximated in 1819 that more than ten thousand individuals in England had acquired at least a basic skill in engraving (Cambridge, 1953).

In October of 2013, an article titled 'How to Spot a Fake Banknote’ was featured in The Guardian newspaper. Amidst a collection of guidance on examining contemporary English banknotes, the public was informed that they had the option to embark on an online "virtual tour" of banknotes. This tour aimed to assist individuals in their scrutiny of any notes they suspected might be counterfeit.

To justify why we should be concerned about accepting counterfeit banknotes, the author noted that if we unintentionally accept a fake note, there is no recourse to replace it with a genuine one. In other words, the Bank of England does not offer compensation for one's lack of discernment. The article further elaborated that individuals who receive what they suspect to be a counterfeit note in payment have the legal right to hold onto it for potential inspection by the police. It may appear surprising that such information needs to be presented to the public, given that a policy of not compensating individuals for counterfeit notes has been in place for over three centuries.

2.4 Banknote design requirements

Ensuring a secure document's effectiveness involves striking a balance between aesthetics and meticulous design. This approach encourages individuals to recognize and treat the document as secure. For instance, "Aesthetics can significantly enhance users' ability to identify a genuine document and detect stylistic discrepancies caused by counterfeits" (Renesse, 2002). Therefore, security designers must seamlessly blend the talents of fine artists with the expertise of forensic scientists (Renesse, 2002). Failure to integrate these design and scientific skills can result in reduced security against counterfeiters and forgers.

A well-designed secure banknote should convey a sense of authority and the utmost security on behalf of the country it represents. Conversely, if a banknote gives the impression of being a mere bus ticket, it will be treated as such (Renesse, 2002). It's crucial to recognize that banknotes serve as a significant representation of a nation. Frequently, when foreign travelers visit a different country, a banknote is the first document they encounter, shaping their initial impression of that nation's status. As such, "by their very nature, security documents [including banknotes] often mirror a nation's prestige and culture" (Renesse, 2002).

2.4.1 Polymer banknotes

When delving into the components of polymer banknotes, which represent a significant evolution in banknote production, and the distinctive attributes of this banknote model, numerous countries have found compelling reasons to adopt polymer banknotes. It is crucial to recognize that the environmental and security advantages associated with polymer banknotes, setting them apart and making them superior to other alternatives, hinge on the unique materials, composition, and design inherent in polymer banknotes.

It's worth noting that the materials used to create polymer banknotes, derived from specific compounds, have been developed by prominent companies and major educational institutions worldwide. Some formulas and production guidelines have remained confidential to this day.

Nevertheless, the outcomes of research and development into polymer banknotes have unveiled a multitude of components within these banknotes (Spencer, C. ,2011, Han, T.-H.; Lee, Y.; Choi, M.-R.; Woo, S.; Bae, S.-H.; Hong, B.H.; Ahn, J.-H.; Lee, T.-W, 2012).

Traditional paper banknotes employ aging materials like cotton and fabric fibers, arranged parallel to the lines of the banknote paper, leading to premature banknote wear and tear. In contrast, polymer banknotes consist of three layers of polymer film and feature a triangular fiber arrangement. Additionally, their vertical design with banknote lines mitigates the risk of polymer banknote tearing.

It's essential to note that paper banknotes lack transparency due to their widespread use of cotton fibers and wood pulp. Furthermore, they exhibit low heat absorption rates and react swiftly to heat exposure. This swift response results in the breakdown and deformation of their network structure, rendering the banknote nonfunctional. In contrast, the presence of polymer films in the structure of polymer banknotes enhances their heat absorption capacity, making them more resistant to deformation and collapse. The composition of polymer banknotes is inherently more complex (Dam, 2021).

It's worth mentioning that the central layer attributes its porosity to heat and moisture. Consequently, polymer banknotes exhibit exceptional resistance and durability in the face of temperature fluctuations and potential tearing. These specifications and standards for polymer banknotes adhere to the international standard S.C.A., a validation process refined over the years. Polymer banknotes, in contrast to paper banknotes, offer enhanced cleanliness and transparency, as they do not incorporate wood fibers or pulp in their composition (International Monetary Fund Bosnia and Herzegovina, 2015, Xia, R.; Heliotis, G.; Bradley, D.D.C, 2003).

Polymer banknotes remain intact when exposed to water and maintain their physical integrity. The transparency of these banknotes results from their material composition, and they exhibit an exceptionally high level of water resistance, contributing significantly to their security features (Vásquez-Garay, F.; Carrillo-Varela, I.; Vidal, C.; Reyes-Contreras, P.; Faccini, M.; Mendonça, R.T., 2021).

Certain attributes hold particular significance in the crafting and manufacturing of polymer banknotes. The sheets undergo offset printing, a method that concurrently imparts colored inks to both sides of the sheet, ensuring the alignment of images on both faces of the banknote. This procedure forms the foundation for one of the primary security features of Australian banknotes, particularly in banknote authentication. When illuminated, diamond-shaped patterns are printed on each side of the banknote to produce an image depicting a seven-pointed star enclosed within a circle (Policy Pap. **2012,** Karnutsch, C.; Pflumm, C.; Heliotis, G.; Demello, J.C.; Bradley, D.D.C.; Wang, J.; Weimann, T.; Haug, V.; Gartner, C.A.; Lemmer, U, 2007, Chen, Y.; Herrnsdorf, J.; Guilhabert, B.J.E.; Kanibolotsky, A.L.; Mackintosh, A.R.; Wang, Y.; Pethrick, R.A.; Gu, E.; Turnbull, G.A.; Skabara, P.J.; et al. , 2011).

Subsequently, the distinctive serial number is imprinted on the banknotes using ultraviolet light-reactive ink. Protective coating is administered to the bill to enhance its longevity and maintain cleanliness. Additionally, fluorescent sections are introduced during this phase.

The banknotes undergo a final scrutiny to ensure there are no printing errors. Subsequently, they are meticulously packaged and readied for the invoicing process (Chen, Y.; Herrnsdorf, J.; Guilhabert, B.J.E.; Kanibolotsky, A.L.; Mackintosh, A.R.; Wang, Y.; Pethrick, R.A.; Gu, E.; Turnbull, G.A.;Skabara, P.J.; et al. ,2011).

The augmentation of security measures, coupled with polymer banknotes' ability to resist tampering with optical and variable inks, and the incorporation of a transparent layer of polymer film with a focus on 3D materials, has heightened security levels and effectively thwarted counterfeiting attempts on banknotes in circulation (Singh, N., 2008, Delori, F.C.;Webb, R.H.; Sliney, D.H.,2007).

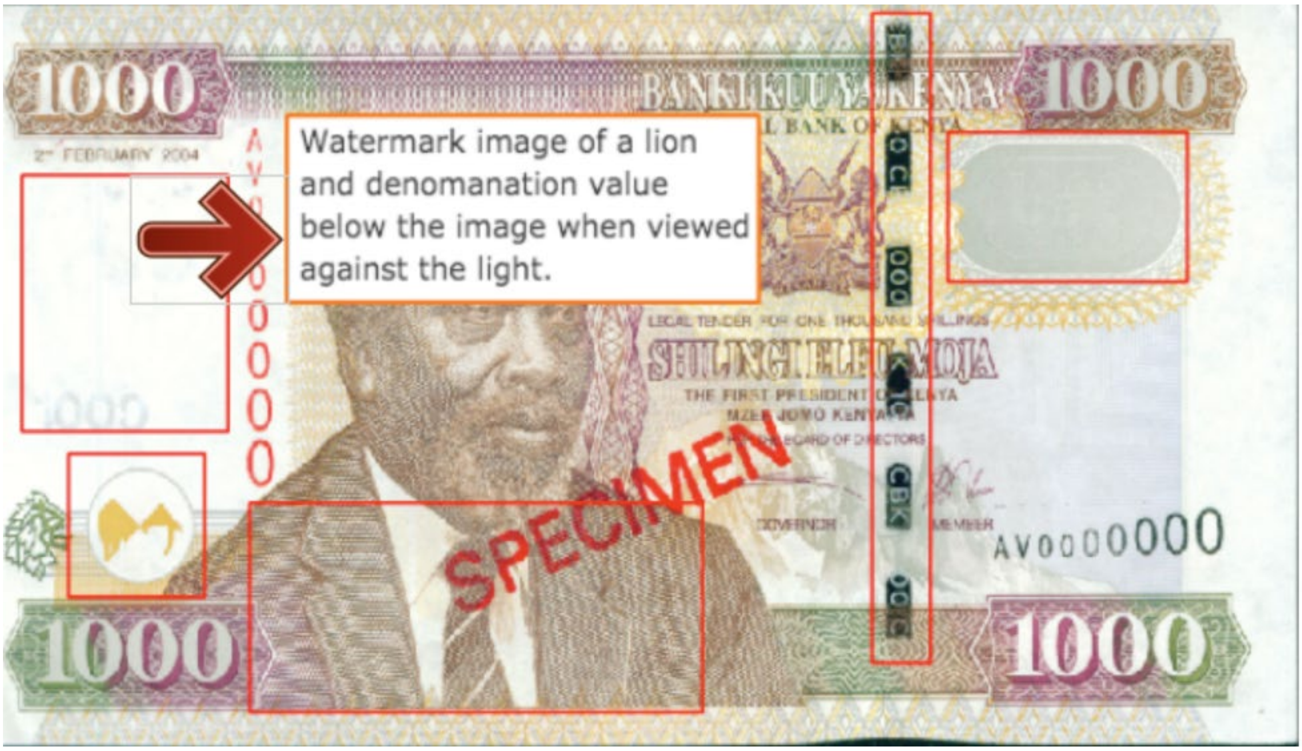
2.5 Theoretical Framework

2.5.0 Banknote security features

2.5.1 Watermarks

Take for instance, the $100 banknote in the United States, which features a watermark displaying the portrait of Benjamin Franklin positioned alongside his central portrait on the note. Watermarks are most effective when they are easily visible and identifiable upon examination, and it is recommended that they remain unobscured by any printing (Renesse, 2002). This type of watermark offers a high level of security and is endorsed by Interpol for use in banknotes (Renesse, 2002).

Moreover, multi-tone watermarks can introduce greater complexity, featuring variations in tone across different sections of the watermark, with some areas appearing darker or lighter than others. Multi-tone watermarks provide protection against scanning, copying, chemical alteration, mechanical tampering, and attempts at reproduction (Warner, 2005).



Watermark image of a lion and denomanation value below the image when viewed against the light.

Figure 2. Watermark on a banknote.

Banknotes, similar to the majority of secure documents, hinge on the substrate as the fundamental element ensuring security. In the realm of security paper, a watermark assumes a role as an exceedingly potent security feature. Put plainly, a watermark represents an image integrated into the paper during the paper manufacturing process by adjusting the thickness of the fibers, thereby affecting the paper's transparency (Warner, 2005). The watermark stands as a security attribute created in the paper production procedure, having earned a distinguished reputation for its unwavering and trustworthy utility, rendering it synonymous with security (Renesse, 2002). Acknowledged by the general public, the watermark serves as the central and most secure constituent. Thus, banknotes will continue the use of a multi-tone watermark to fight against counterfeiters.

2.5.2 Ultraviolet security

Another security element linked to the substrate pertains to the absence of optical brightening agents in the paper production process. Security paper must exhibit ultraviolet-dull (UV-dull) characteristics, signifying that the paper is devoid of optical brightening agents (Warner, 2005). This UV-dull paper enhances security for two key reasons. Firstly, it permits the application of fluorescent inks as a security feature. Secondly, it refrains from fluorescing under UV light, which is in contrast to counterfeits produced on typical, brightened colored paper (Warner, 2005). Consequently, the majority of security-printed documents employ uncoated substrates that lack brightening agents.

2.5.3 Security threads

Security threads and fibers constitute another aspect of security that involves the substrate. Much like watermarks, security threads and fibers are integrated into the security paper during the manufacturing process (Warner, 2005). Security fibers introduce visibly distinct colored fibers into the documents, serving as an overt security feature—meaning it can be easily detected with the naked eye. Additionally, these security fibers can be nearly invisible in color but fluoresce when exposed to UV light, simplifying the authentication process (Warner, 2005). Security fibers are often employed alongside watermarks and offer protection against color photocopying (Warner, 2005).

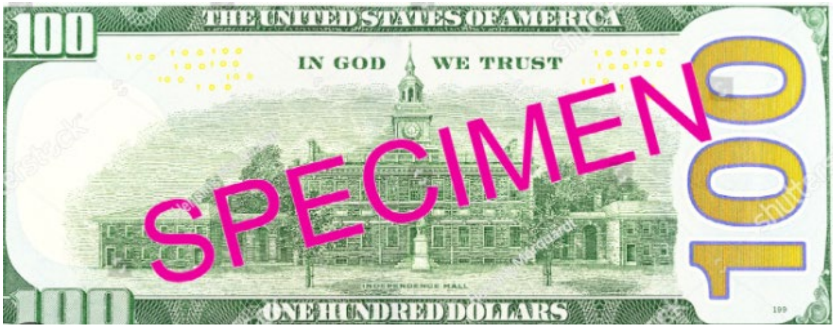


Figure 3. United States of America Banknote showing security threads.

2.5.4 Durability as a form of security

Banknotes are particularly unique because they are initially issued by a central bank and then circulate through various social and cultural settings. There is no fixed environment where a banknote must be kept, so its condition depends on cultural and social factors. Banknotes can be found in wallets, billfolds, pockets, or even in direct contact with the skin. They are exposed to various hazards as they are handled in diverse conditions, including banks, offices, ships, markets, and bars. Under all these circumstances, a banknote must maintain its value and not change in color or composition (Renesse, 2002).

Rudolf L. van Renesse, the author of "Optical Document Security," highlights that banknotes are distinctive documents due to the intricate handling they undergo regularly. Vigorous handling can weaken the structural integrity of banknotes, rendering them unusable within a relatively short timeframe. Consequently, some countries opt for polymer notes, which offer a sturdier substrate for their currency. Moreover, as time passes, the security features incorporated into banknotes may deteriorate, reaching a point where they are no longer discernible. For instance, exposure to certain chemicals may erode the fluorescent threads in a banknote, leading it to appear counterfeit. Therefore, it is essential for banknotes to exhibit durability to ensure that the security features integrated into their production endure throughout the entire lifespan of the banknote.

2.5.5 Inks for Banknote security

An important step in enhancing the security of banknotes concerns the pigments utilized for imaging. There exist two primary categories of ink associated with security printing: anti-duplication ink and anti-alteration ink. "Anti-duplication inks are formulated to thwart unauthorized copying or replication of documents" (Warner, 2005). These inks employ concealed security methods like UV fluorescence for authentication. On the other hand, "anti-alteration inks offer overt indications of tampering, including color changes when exposed to water or chemicals or damage to the background" (Warner, 2005).

Ultraviolet Inks (UV) find frequent use in the printing of U.S. banknotes. These inks are characterized by being "invisible to the human eye in standard lighting conditions" (Warner, 2005). The visibility of these inks necessitates illumination by UV radiation. For example, the U.S. $20 banknote incorporates a variant of UV ink known as invisible UV-fluorescent ink. These types of ink possess a unique property—they remain invisible in daylight but "exhibit different hues when exposed to UV light" (Warner, 2005). This ink introduces a concealed security feature, as it remains undetectable without the appropriate short-wave or long-wave UV illumination (Warner, 2005).

2.5.6 Color shifting

Color-shifting inks are exclusively employed in the production of U.S. banknotes and serve as an illustration of both anti-duplication and anti-alteration ink. These inks fall under the category of optically variable devices (OVDs) and are integrated into the $5, $10, $20, $50, and $100 banknotes. This sophisticated ink feature "prints the denomination numeral in the lower right-hand corner on the front of the banknote" (Warner, 2005). When the bill is tilted forwards or backwards, the ink undergoes an actual color transformation, shifting from black to green or copper to green, contingent upon the note's printing date (Warner, 2005). Another instance of this can be observed on the €5 (Euro) banknote, where a segment appears black at one angle and yellow at a different angle (Warner, 2005).

An Optically Variable Device (OVD) is a mechanism that modifies the visual characteristics of printed material in various ways. For instance, OVDs exhibit alterations in appearance to the viewer when there are changes in the viewing angle between the device and the observer, shifts in the angle between the device and the light source, rotations of the device, or modifications in the color temperature or dominant wavelength of the light source (Warner, 2005). It is entirely expected that OVDs have evolved into what can be described as "a fundamental component of document security applications" (Warner, 2005).

Numerous other security ink methods are presently not employed in banknote printing but could potentially be adopted in the future. A captivating instance is the utilization of electrochromic ink, a recent innovation from the Dow Chemical Company, USA (Warner, 2005). This unique ink possesses the capability to "alter its color in response to an electric current" (Warner, 2005). Presently, such ink is utilized for packaging purposes, yet it may emerge as a viable choice for verifying banknote authenticity in forthcoming developments.

2.6 Security printing of Banknotes

To facilitate security for banknotes, numerous security-printing methods are applied during the banknote printing process. (Warner,2005) identifies banknotes as sophisticated security end products (SEPs) and acknowledges that the greater the number of security features integrated into creating a high-tech secure document, the more challenging it becomes to counterfeit. Presently, there are more than forty techniques utilized for crafting high-tech security end products. Nonetheless, the most frequently employed methods in banknote production encompass security paper, security ink, lithography, intaglio, letterpress, optical variable devices, machine-readable elements, durability enhancements, anti-forgery measures, microprinting, and design enhancements.

When individuals handle banknotes, they often overlook the extensive technology and security measures concealed within the palm of their hand. It's easy to take these features for granted, but it's crucial to remember the rationale behind this heightened level of security: "One of the most widely used currencies is also the most counterfeited one—the U.S. dollar. No other currency is involved in as many seized counterfeits worldwide" (Renesse, 2002).

2.6.1 Lithography

Lithography is a widely adopted printing technique rooted in the principle that water and oil do not mix. In contemporary lithography, an image is transferred to a plate through a photochemical process. The plate accepts ink within the image regions while repelling ink in the non-image areas using a water-based fountain solution. Security printing employs lithography in a distinct manner compared to conventional lithography practices (Renesse, 2002). Security lithography entails the creation of images through the formation of line structures and the manipulation of colors along these lines. This approach achieves simulated 3-D effects, playing a crucial role in deterring counterfeit reproduction. Lithography enables the printing of a smoothly transitioning color along a single line, a technique known as "rainbowing." This is advantageous because it produces an intensified, multicolored effect that cannot be dissected into individual color components. Consequently, "Counterfeiters employing the camera [counterfeit] method must invest significant time in manually retouching the negatives to generate a satisfactory plate" (Renesse, 2002).

The brilliance of security printing through lithography lies in its meticulous registration of individually colored printings. This is accomplished by employing duplex or triplex patterns on the document's surface. The inclusion of multiple color patterns proves to be an exceptionally potent security measure because "if counterfeiters attempt to isolate these colors, they must ensure that the minute details are impeccably sharp to maintain pattern integrity and that they seamlessly align with each printing to achieve color consistency" (Renesse, 2002).

Another noteworthy security method enabled by lithography in currency printing is the see-through effect, contingent upon precise registration. Through lithography, it is "feasible to generate a composite image by printing elements on both sides of the document" (Renesse, 2002). Typically, this entails printing the outline of a shape on one side of the document and the solid shape on the other side. When the document is held up to the light, the solid shape seamlessly aligns with the outline shape on the opposite side.

2.6.2 Intaglio

The intaglio printing technique demands meticulous craftsmanship, involving the precise engraving of images onto the printing surface or plate. Once engraved, the plate is coated with ink and subjected to substantial pressure to transfer the image from the cylinder onto the substrate. This method is frequently employed in security printing, where it traditionally serves as the primary visual security feature on the document. Intaglio printing, akin to gravure printing in commercial terminology, necessitates the use of "thick paste inks with hand-engraved plates under high printing pressures" (Renesse, 2002). Additionally, intaglio security printing exhibits "distinctive variations in image depth and tonal range" (Renesse, 2002). Consequently, "The intaglio engraver consistently seeks out combinations of shading and tonal variations" (Renesse, 2002). This meticulous approach ensures that the portrait on a banknote remains highly recognizable and extremely challenging to counterfeit using photographic processes, as fine details are lost or solid areas fill in. Moreover, intaglio printing creates a three-dimensional textured print. This texture "can be employed to conceal a message that becomes legible only from a specific angle" (Renesse, 2002). The message becomes visible when the document is viewed towards the light at an oblique angle.

2.6.3 Letterpress

Letterpress, another extensively employed security technique in currency printing, has historical roots dating back to Johannes Gutenberg's invention of movable type. In this method, metal plates bearing raised images are inked and then pressed onto the substrate. It is a mandatory requirement in the United States for each banknote to feature a unique identification number, a task executed through the letterpress process (Renesse, 2002). Letterpress employs a numbering box that rotates with the press, enabling the automatic advancement and printing of the unit digit in the box. This technique's effectiveness lies in its ability to create and print any number in perfect alignment (Renesse, 2002). Counterfeiters face considerable challenges replicating these numbering patterns due to their non-commercial availability. Furthermore, this type of number security can be enhanced by utilizing special inks, including two-color inks, fluorescent inks, magnetic inks, or other specialized ink varieties (Renesse, 2002).

2.6.4 Micro printing

Microprinting is a widely employed security printing technique involving the printing of minuscule letters that are so tiny they are imperceptible without magnification (Warner, 2005). When viewed from a typical distance, these characters resemble extremely fine lines, but in reality, they contain legible information. Microprinting poses a formidable challenge for counterfeiters because attempting to reproduce this print accurately using only photocopiers is virtually impossible (Warner, 2005). Banknote printing frequently utilizes microprinting as part of its security measures. For instance, on the new $100 bill, microprinting is employed in two instances: "USA 100" appears within the lower left corner, and the words "United States of America" are spelled out on the lapel of Franklin's coat ("Paper Currency").

2.6.5 Fluorescent

Invisible fluorescent printing plays a role in machine reading technology. This technique involves printing an image using ink that contains a fluorescent pigment with similar optical properties to the ink vehicle. As a result, the image remains hidden and is only revealed under a UV light source. Counterfeiters are unaware of this hidden image unless exposed to UV lighting, enhancing security significantly.

2.7 Methodology Used in Previous Studies

2.7.0 Authentication of banknotes

2.7.1 Machine authenticating

In spite of the reduced reliance on physical currency due to the recent worldwide expansion of electronic financial transactions, real money transactions continue to hold significant importance in the global market (Kim & Turton, 2014). When engaging in such monetary transactions, the manual handling and counting of banknotes remains a common practice in daily life. However, the utilization of various automated machines has become imperative for large-scale and secure transactions. These devices are mandated to possess four critical functions: banknote recognition, counterfeit banknote detection, serial number recognition, and fitness classification. While prior studies have conducted limited investigations in the realms of banknote recognition and counterfeit banknote detection, these aspects remain of great significance. Counterfeit banknote detection typically revolves around techniques aimed at differentiating real currency from counterfeit bills. This validation process involves scrutinizing anti-counterfeiting features.

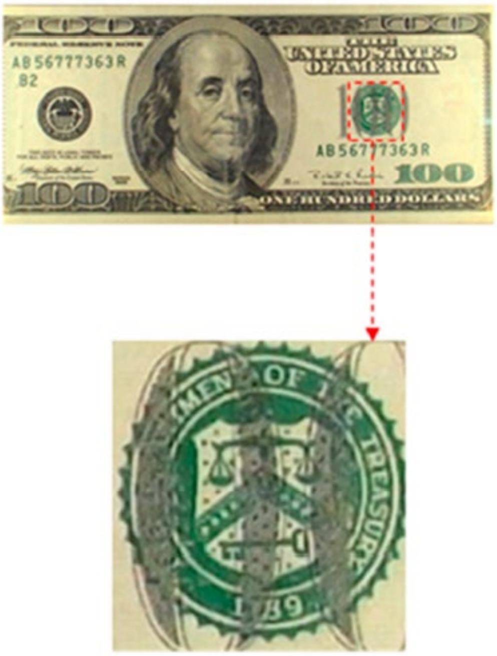


Figure 4. Genuine banknote.

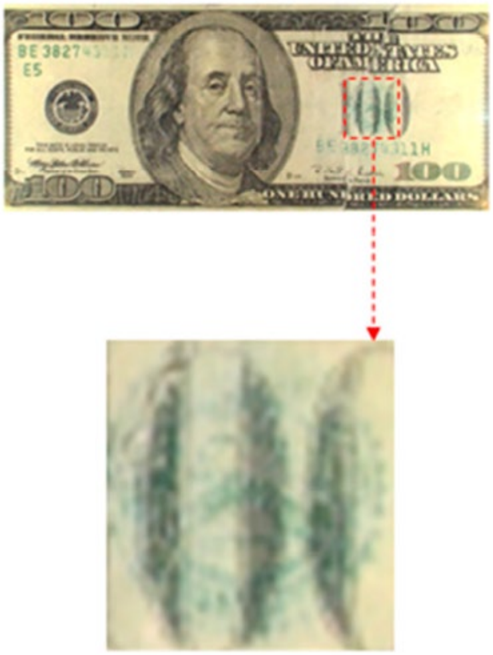


Figure 5. Fake banknote.

A banknote serial number is a unique alphanumerical identifier engraved on each banknote in the banknote production process. It contains the name of the issuing bank and serial information of each denomination (https://www.moneyfactory.gov/seriessntable.html, 2016). Given that each banknote possesses its distinct serial number, this feature can be harnessed for tracking its origin and path through circulation, thereby proving to be a valuable tool in the fight against counterfeit banknotes.

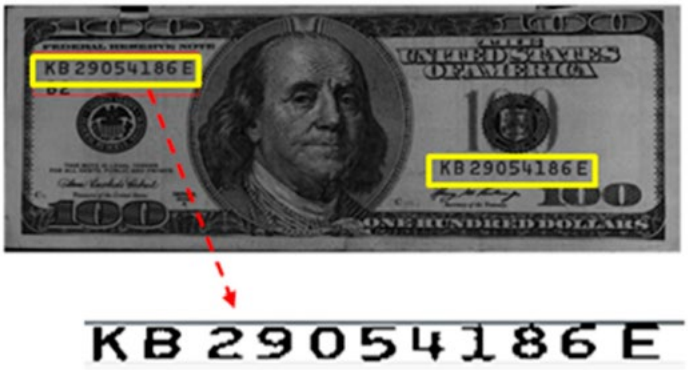


Figure 6. Example of serial number code (USD 100 bill).

Fitness classification of banknotes generally pertains to methods for categorizing banknotes based on their physical condition, which includes factors like soiling. Banknotes of the same denomination can exhibit various states of fitness or unfitness, encompassing issues like soiling and creases. These conditions are influenced by factors such as circulation frequency and environmental conditions. To ensure that banknotes in circulation are maintained in good condition, automated self-service terminals like ATMs must incorporate a fitness classification feature to segregate and retrieve unfit banknotes. This retrieval of unfit banknotes is crucial in preventing errors in banknote classification.

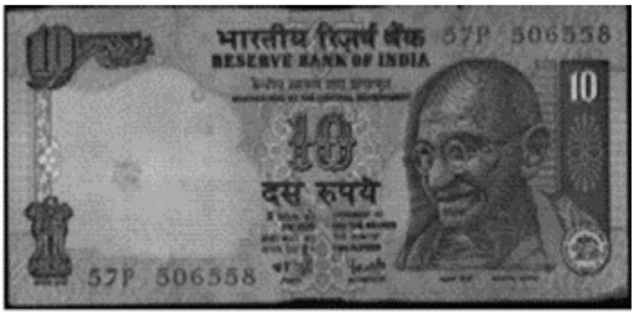


Figure 7. A fit banknote.

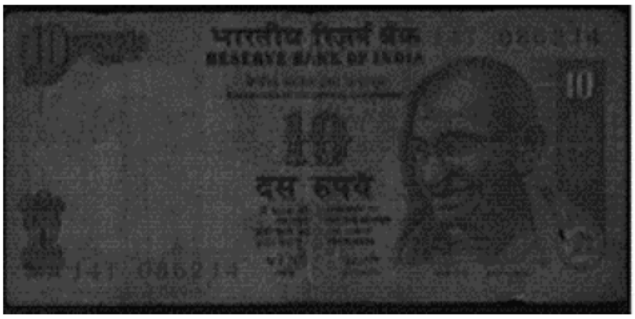


Figure 8. An unfit banknote.

A typical process flow of banknote recognition implemented in a self-service terminal.

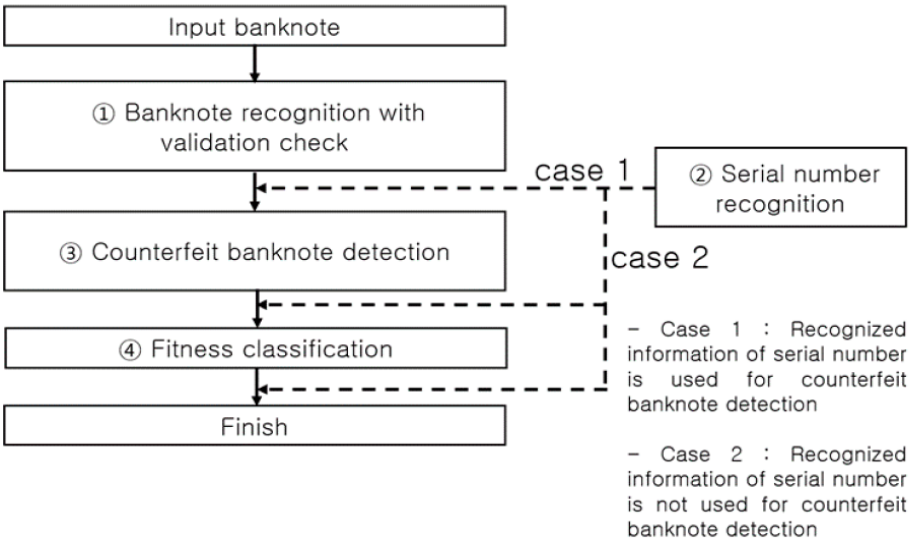

Input banknote
① Banknote recognition with validation check
case 1
② Serial number recognition
③ Counterfeit banknote detection
case 2
④ Fitness classification
Finish
– Case 1 : Recognized information of serial number is used for counterfeit banknote detection
– Case 2 : Recognized information of serial number is not used for counterfeit banknote detection

Figure 9. Banknote recognition process flow in an automated device.

Banknotes primarily serve as a means for people to engage in daily transactions for goods and services. These banknotes incorporate various security features that appeal to both touch and sight (Renesse, 2002). Machine reading, in this context, involves the utilization of machines to verify the authenticity of documents, comprising two primary categories. The first category encompasses teller-assisted features, which assist inspectors in validating documents. The second category involves automated features that facilitate the acceptance of a document. An example of the former is the use of fluorescence lighting, while the latter includes machine sorting systems. Discussion regarding automated machine sorting systems is highly restricted, as typically only the currency printer and central bank personnel possess knowledge of such features (Renesse, 2002).

Figure 10. Banknote authenticating machine.

The U.S. one-dollar bill employs a different teller-assisted feature related to magnetic detection. Magnetic ink, mixed with the black ink on the front of the bill, is used. Handheld devices are employed to detect the magnetic field when moved over the document's surface. This feature, known as magnetic detection, has been extended to include numbers, signatures, and intaglio elements on banknotes from other countries. It should be noted that magnetic detection is more effective with darker colors, making it less suitable for use with lighter hues. For instance, bright red ink does not produce a strong magnetic signal. Despite this limitation, magnetic ink remains an effective security measure against counterfeiting, with minor restrictions on its versatility (Renesse, 2002).

(Yoshida et al., 2007) proposed a currency detection technique using CMOS based scanner called Grid Scanner, which uses an infrared filter and captures image in infrared band. Then, micro-text printed area was captured as a gray scale image for reading the micro text printed on the currency image. The acquired image undergoes processing through either a microcontroller, namely the PIC-16F648A or the ATMega88 (AVR). Subsequently, the microcontroller employs an Optical Character Recognition (OCR) technique to ascertain the authenticity of the banknote. It does so by identifying the characters "B," "A," and "N" within the scanned image. When the image is well-captured, this counterfeit detection method achieves a 100% success rate, and the average processing time is approximately 250 milliseconds when utilizing the aforementioned microcontroller.

2.7.2 Human authentication

Banknotes are not primarily intended for use with automatic identification methods. Typically, the attributes of banknotes that are employed for identification using such methods have to be selected based on empirical factors. This implies that there is usually no straightforward algorithm to combine these attributes in order to ascertain the validity of the banknotes.

Previous studies have indicated the existence of two distinct cognitive systems that influence decision-making. One of these systems is characterized as rapid, automatic, and mostly operating at a non-conscious level. This particular processing mode is commonly referred to as System-1 or Type-1 processing (Frankish, 2010; Kahneman, 2010).

However, when investigating counterfeit detection through a cognitive experiment, assessing Type-1 processing may prove challenging. Specifically, asking participants whether a given banknote is genuine or counterfeit is likely to trigger higher levels of suspicion and caution. As a result, the authentication process would involve a slower, more deliberate, and conscious decision-making procedure, which is commonly referred to as Type-2 processing in the literature (Frankish, 2010; Kahneman, 2010).

Apart from the constraints related to perception, it's essential to emphasize the presence of the "prevalence effect." Visual search experiments entail perceptual activities that demand actively scanning the visual surroundings to locate a specific object or characteristic (the target) amid other objects or characteristics (the distractors). Typically, in the majority of visual search experiments, targets are presented in over 50% of the trials (Wolfe & van Wert, 2010).

Nonetheless, Wolfe and van Wert's research demonstrated that when targets were infrequent (1% prevalence), observers committed more than four times the number of "miss" errors compared to when targets were common (50% prevalence). The elevated rate of missing targets, particularly when they are rare, poses a substantial concern in significant everyday scenarios, such as medical or airport screening (Wolfe & Van Wert, 2010). Additionally, (Wolfe, Horowitz &Kenner 2005) revealed that if observers consistently fail to detect their target, they are more likely to miss it when it eventually appears. This prevalence effect certainly has implications for counterfeit detection as well, given that counterfeit incidents in everyday life are exceedingly rare (Rich et al., 2008).

The prevailing belief is that a presentation lasting just 200 ms should suffice for the detection of fundamental features. Given that the minimum duration for a saccadic eye movement is also around 200 ms, tasks of this nature can be accomplished in a single rapid glance (Healey & Enns, 2012). On the other hand, recognizing and distinguishing complex patterns seems to demand more time.

The process of accepting a banknote happens swiftly. An internal field study involving DNB cashiers (Zondervan, Heinen, & Heuvel, 2019) revealed that the majority of cashiers decide whether to accept a banknote, either explicitly or implicitly, without employing authenticating devices, all within a time frame of 3 seconds. Additionally, according to (Layne-Farrar, 2011), waiters typically take only 1-2 seconds to pick up money left on a table as a tip and place it in their pockets.

Performing the straightforward task of accepting a banknote and placing it in your wallet likely falls within that time frame. It's safe to assume that, during this period, the banknote is implicitly authenticated. Several national central banks within the Eurosystem, such as the Bank of Italy (2020) and the Bank of Finland (2020), emphasize on their websites that it takes only a few seconds to explicitly authenticate a banknote. To the best of our knowledge, no empirical evidence exists concerning the speed at which banknotes can be recognized as counterfeit or genuine.

As mentioned earlier, it is uncertain whether extending the exposure duration would enhance counterfeit detection. (Fei-Fei et al., 2007) found that observers require a presentation time of 500 ms to nearly perfectly categorize outdoor and indoor scenes. Additionally, a study conducted by (Greene, Botros, Beck, Fei-Fei, 2015) revealed that participants can provide an adequate description of typical real-world scenes after 506 ms. However, participants take longer to comprehend and even perceive unlikely visual scenarios (e.g., a press conference held underwater), indicating that our rapid scene-categorization abilities depend significantly on our prior experience with real-world environments (Greene et al., 2015).

If counterfeit banknotes can be readily distinguished from genuine ones due to prominent features (Theeuwes, 1992), then this discrimination should be a rapid process. Certainly, if identifying counterfeit banknotes relies on scrutinizing specific details, it is reasonable to anticipate that a longer exposure duration would lead to significant performance improvements. We set an upper limit of 10 seconds for the exposure duration, as previous research (Van der Horst, Eschelbach, Sieber, & Miedema, 2016) indicated that the detection hit rate does not notably increase beyond this 10-second threshold.

When individuals have access to both visual and haptic sensory information, there is a strong likelihood that these senses interact with each other, as suggested by (Wijntjes, 2009) and cited in (De De Heij, 2017) and explored in studies like (Kandula, Hofman & Dijkerman 2015).

An illustrative example of this interaction is the rubber-hand illusion, where observing a rubber hand being stroked while one's own hand, unseen, is stroked simultaneously, can lead to a sense of the rubber hand being associated with one's own body (Tsakiris & Haggard, 2005).

The idea that haptic perception is likely to play a significant role is also reinforced by the fact that it can provide valuable new information. For instance, when handling a banknote, individuals might only visually perceive one side of it, but they will invariably feel both sides.

Haptic perception usually entails engaging in active manual exploration. When individuals explore objects through touch, they often draw upon their prior experiences related to surface textures, object attributes like roughness, shape, weight, material properties, contours, and more, from their interactions with the external world. As outlined by Lederman and (Klatzky, 1987), haptic exploration encompasses six primary types:

Lateral motion- typically utilized for exploring textures, Pressure- which aids in assessing hardness, Static contact- used to gauge temperature, unsupported holding- employed to judge weight, Enclosure- which helps in estimating size and Contour tracking-used to determine the shape.

In the context of haptically evaluating counterfeit banknotes, we postulate that the most critical types of haptic exploration are lateral motion, which pertains to texture exploration, and pressure, which involves assessing the surface's hardness.

(Wijntjes, 2009) conducted research on the haptic examination of banknotes. This study revealed that when a cash handler receives a banknote, they typically engage in haptic exploration before depositing it into the cash register. Typically, a banknote is held between two fingers, with the index finger placed on the reverse side and the thumb on the front. Additionally, the middle finger or its side may provide assistance to the index finger by exerting counter-pressure to the thumb.

The picture on the left shows the bending of the paper, the picture in the middle shows planar movement of the thumb and the picture on the right shows the multiple contact areas. The cash handler thus perceives various banknote properties such as its structure and raised ink.

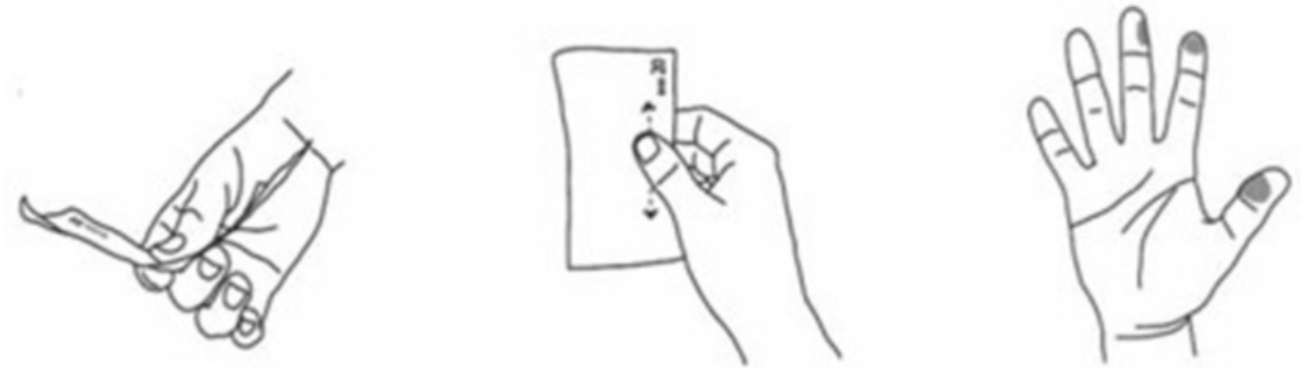


Figure 11. Human authentication of banknote by touch and feel.

In an internal study conducted by (Zondervan et al., 2019) on behalf of De Nederlandsche Bank, two undercover shoppers bought a product from 30 different stores and used artificially altered genuine banknotes for payment. The behavior of the cashiers when presented with these "suspicious" banknotes was evaluated. One noteworthy discovery was that around half of the shopkeepers authenticated banknotes by using their fingertips.

Previous research on haptic perception has demonstrated that humans can quickly recognize common objects, such as paper, through touch alone in just a few seconds (Lederman & Klatzky, 1993). Tactile information is processed even when individuals do not intentionally focus on it. According to (De Heij, 2017), several studies have revealed that individuals are prompted to perform an authenticity check on a banknote they have just received if they sense that "it felt different."

In alignment with this viewpoint, the European Central Bank (ECB) acknowledges the significance of the tactile aspects in detecting counterfeit banknotes. The tactile experience encompasses the texture of the banknote itself ("feel the banknote, it is crispy and firm") and the raised print elements ("feel the short, raised lines on the left and the right edges of the banknote. The main image and the large value numeral also feel thicker") (European Central Bank, 2013). The ink layer of a banknote typically has a height of approximately 60 µm, although this height may decrease with extensive use. As noted by (De Heij, 2017), the deterioration of banknotes can result from the relaxation of paper fibers and various forms of wear and tear, which may introduce wrinkles and contribute to a "tactile noise level."

A study conducted by Raymond (2017) was structured to facilitate perceptual testing and discrimination based exclusively on "intaglio" elements (raised print). In contrast to the current study, the banknotes used in this investigation were custom-made for the research. Participants were required to familiarize themselves with the fantasy notes, and the counterfeit notes were artificially created, rather than being taken from circulation as in the present study. Raymond and her team employed three soil levels and three variations of counterfeit banknotes, which mirrored what she described as typical characteristics of real counterfeits. The results demonstrated that the ability to detect counterfeit banknotes was effective across all soil levels, even when high-quality counterfeits were presented. Raymond's findings led to the conclusion that tactile information contributes to superior counterfeit detection compared to visual information, irrespective of the level of soiling.

In addition to intaglio, the physical composition or material of the banknote proves to be valuable for authentication purposes. According to a 2013 cash survey conducted by the Bank of Spain (Pérez, Guinea, & Negueruela, 2014), this was the security feature most frequently examined by both the general public and retailers. A study carried out by (Summers, Irwin, Brady, 2008) focused on distinguishing between ten different types of plain paper based on brief contact within a few seconds. Summers concluded that two key perceptual attributes, namely roughness and stiffness, were employed to differentiate the paper types. Nevertheless, similar to raised ink, a drawback associated with these factors is their substantial transformation throughout the lifespan of the banknote.

(Verma et al., 2011) introduced a method for Indian Currency Recognition based on Texture Analysis. Their system is built upon the inherent characteristics of the currency itself. They harnessed texture as the intrinsic feature for identifying Indian currency and assessed how well these features distinguished between different denominations. To extract these texture features from the currency images they captured, they employed a tool called Mazda. Initially, they acquired scanned images of the front side of currency notes in three denominations: Rs. 10, 100, and 500. These images were loaded into the Mazda texture analysis system, and texture features were extracted from five Regions of Interest (ROIs) chosen based on domain knowledge, aiming to maximize the discriminatory texture features. Subsequently, the texture features for each class of images underwent reduction using Mazda's built-in Fisher discriminate analysis. Features were ranked according to their discrimination percentage for three class comparisons: 10 vs. 100, 10 vs. 500, and 100 vs. 500.

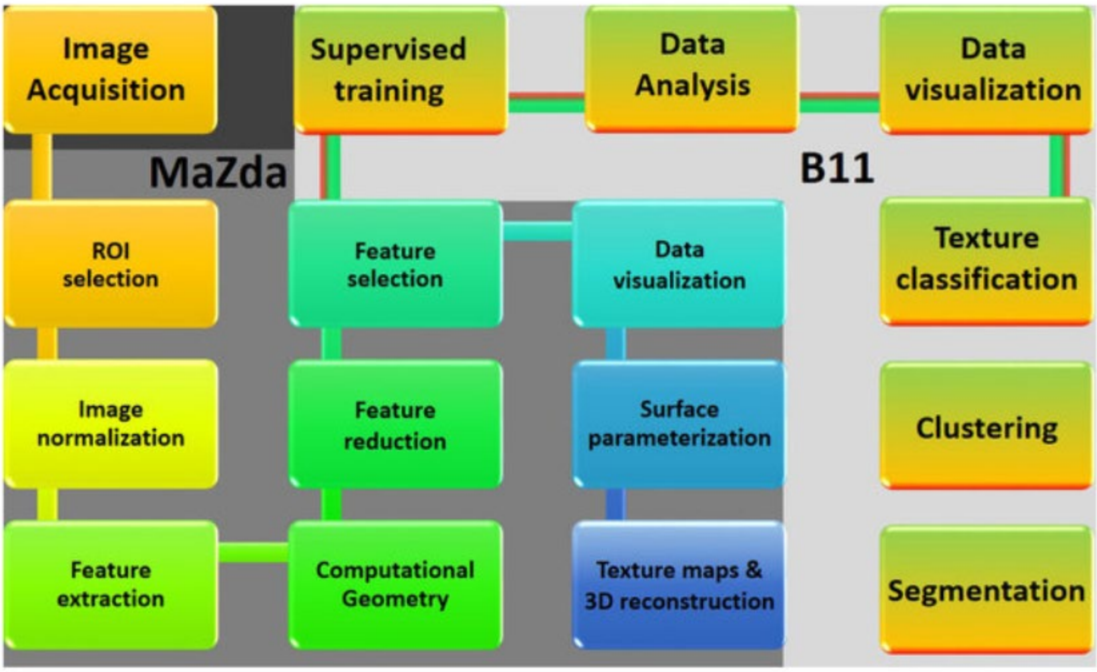


Figure 12. Mazda texture analysis system.

Texture analysis heavily depends on the quality of the captured images. Poor lighting conditions, blurriness, or low resolution can affect the accuracy of texture-based recognition.

2.7.3 Hyperspectral Authentication

Hyperspectral imaging (HSI) is a non-invasive measurement technique (paty et al., 1988), that records the intensity levels across consecutive spectral bands spanning a wide spectral range, generating a comprehensive spectrum for every spatial location (Kumar et al., 2013). HSI is characterized by its ability to provide imaging data with spectroscopic details across a minimum of 100-200 wavelength bands (Liu et al., 2011). The wealth of spectral information acquired through HSI enables its application in classification and quantification (Kumar et al., 2013), setting it apart as a substantial advantage compared to other imaging methods that capture just a single or a limited number of wavelength bands.

HSI gives a collection of intensity-related values stored in a three-dimensional spatial-spatial-spectral domain, known as a datacube. Each value in the datacube represents the recorded intensity of a specific spectral band belonging to a particular spatial position in a two-dimensional imaged area.

The spectral characteristics of the features on the genuine polymer banknotes can be acquired using HSI to build spectral libraries, which can potentially be used to authenticate polymer notes. However, this is not widely reported and has become one of the latest thrust research area in forensic identification.

Nonetheless, there is a limited number of studies that have employed hyperspectral imaging (HSI) for tasks such as verifying the authenticity of artworks, detecting document forgery, identifying counterfeit currency, authenticating images, and validating holograms. An example of an artwork authentication method utilizing HSI is pigment identification (Rosi, F.; Grazia, C.; Fontana, R.; Gabrieli, F.; Buemi, L.P.; Pampaloni, E.; Romani, A.; Stringari, C.; Miliani, C. Disclosing Jackson, 1947).

(S. Baek, et al., 2018) carried out a classification task involving 20 different denominations of currency, such as the EU Euro, Indian Rupee, and US Dollar, utilizing low-resolution multispectral images. They employed a contact image sensor (CIS) to capture images using six distinct wavelengths that covered the RGB to IR channels. The algorithm initially separated obvious counterfeit banknotes through a global classification process and then examined the security features of the remaining banknotes using local feature classification. They applied the same samples to the method detailed in the study conducted by Kang and his team, and subsequently conducted comparisons. The outcome demonstrated a classification accuracy of 99.89% (27,484 out of 27,764) (S. Baek et al., 2018), whereas the approach proposed by (Kang et al., 2017) achieved a classification accuracy of 98.66% (27,392 out of 27,764).

In the case of counterfeit currency detection using hyperspectral imaging (HSI), a spectral database of genuine banknotes is created. Subsequently, this database is compared to the hyperspectral characteristics of banknotes under scrutiny (Lim, H.-T.; Murukeshan, V.M., 2017).

In the context of image authentication, hyperspectral imaging (HSI) distinguishes the specific film brand used to capture the image by analyzing the hyperspectral signature unique to each type of film (Tournié, A.; Carré, P.; Andraud, C. Boust, C.; Lavédrine, B., 2017).

Consequently, the merging of two images captured on different films becomes readily detectable. Regarding hologram authentication, hyperspectral imaging (HSI) can capture the hyperspectral fingerprints of the hologram's reflections from various incident angles. These fingerprints can subsequently be compared to the hologram under scrutiny (Sumriddetchkajorn, S.; Intaravanne, Y., 2008).

In a manner reminiscent of the spectral library established in the study conducted by (Polak et al., Casini, 2016) compiled a reference database for red lake pigment utilizing HSI (Hyperspectral Imaging). They faithfully recreated cochineal and brazilwood paints through a historically accurate process, capturing them with the HSI device working in the Visual-NIR (VNIR) spectrum. For the sake of comparison with the prevailing method of that era, they generated a reference database for the same pigments using fiber optic reflectance spectroscopy (FORS). Upon subsequent comparison, it was evident that the data obtained via HSI proved to be accurate and closely aligned with the results from FORS. It's worth noting, however, that the researchers did not provide exact numerical data.

In a separate study, (Daniel et al., 2011) employed HSI (Hyperspectral Imaging) for the purpose of identifying materials and mapping paintings within the Museum of Zaragoza. To assess the analytical performance of various HSI systems, the researchers evaluated two systems, one utilizing a "pushbroom" and the other a "mirror-scanning" approach. Both systems operated under identical parameters, capturing spectral data within the VNIR range. The data was subsequently processed using a spectral angle mapper (SAM). The researchers concluded that while HSI proved to be suitable for the analysis of artworks, the need for a new algorithm was recognized to address specific interpretation challenges.

Similarly, (Deborah et al., 2015) endeavored to tackle the issue of crack detection in paintings by employing spectral processing, which was presented in a comprehensive or vector-based approach. This approach was pursued as other methods available at the time of the study either processed the information in a limited manner or involved extensive data reduction. Consequently, they devised a multivariate top-hat transformation known as spectral convergence mathematical morphology (SCMM) and conducted an experiment to compare its effectiveness with two established methods, specifically grayscale top-hat on a distance map (DM) and marginal top-hat (Marg.). The outcomes indicated that while SCMM demonstrated robustness in detecting cracks, it did not exhibit significant improvement compared to the existing approaches.

(Wang et al., 2021) introduced a fusion method that relies on HSI (Hyperspectral Imaging) features for the purpose of distinguishing counterfeit modern Chinese paintings from genuine ones. They employed an HSI camera operating within the 400–900 nm range to scan and differentiate between real and counterfeit Chinese paintings. Subsequently, spectral features were extracted using singular spectrum analysis (SSA), while spatial features were extracted through a combination of principal component analysis (PCA) and convolutional neural network (CNN). The extracted features were then subjected to classification using a Support Vector Machine (SVM). As a result, the proposed method achieved an accuracy rate of 84.6%, averaging results from ten tests that involved the classification of random 2500 samples out of a total of 5000 samples.

(C.S. Silva et al. 2014) investigated the utilization of HSI in the near-infrared range (HSI-NIR) for the forensic analysis of document forgery. In order to assess its precision, they conducted experiments involving three distinct types of simulated forgeries: line crossing, text obfuscation, and text addition. The sample images they prepared were subjected to mapping with a spectral resolution of 6.3 nm and a spatial resolution of 10 meters, all within the selected range of 928–2524 nm.

For data processing, the team employed Principal Component Analysis (PCA) and Multivariate Curve Resolution-Alternating Least Squares (MCR-ALS) in the cases of text obfuscation and text addition. In the instance of line crossing, they utilized MCR-ALS and Partial Least Squares-Discriminant Analysis (PLS-DA). The results of the experiment revealed accuracy rates of 43%, 82%, and 85% for detecting forgeries involving text obfuscation, text addition, and line crossing, respectively.

In a research conducted by (J.F. Pereira, et al., 2017) Hyperspectral Imaging (HSI) was applied across both the Near-Infrared (NIR) and Middle Infrared (MIR) ranges. They utilized a total of 16 different pens as samples and applied Principal Component Analysis (PCA) and Projection Pursuit (PP) as their data processing methods. Accuracy was assessed by comparing the numbers written with different pens on both white paper and bank check paper, each with 2 cm straight lines drawn by each pen.

The results of this evaluation indicated that when using HSI-MIR along with PP and PCA, it achieved an accuracy of 97.5% (73 out of 75) and 87.5% (60 out of 75), respectively. Conversely, when employing HSI-NIR, the accuracy rate was notably lower, reaching 83.3% (5 out of 6) with PP and 76.7% (21 out of 36) with PCA.When HSI-MIR was used in combination with HSI-NIR, both methods collectively achieved an accuracy of 90%. Consequently, they reached the conclusion that this final configuration was the most practical and effective.

(Z. Khan et al., 2013) showcased the application of Hyperspectral Imaging (HSI) in detecting mismatching inks in handwritten notes. Instead of pre-selecting a specific band, they developed an innovative technique called Joint Sparse Band Selection (JSBS) to aid in the selection of the most informative band for forgery detection. Additionally, they developed a dedicated end-to-end camera-based HSI system tailored for document mapping. In this study, samples were not artificially generated but were rather acquired from a database of handwritten notes. When all bands were included, the algorithm achieved detection accuracies of 75.4% and 74.7% for blue and black inks, respectively. However, the utilization of JSBS led to significantly improved accuracies, reaching 86.7% and 89% for blue and black inks, respectively.

Furthermore, (Khan, et al., 2013) presented another study in which they introduced a deep learning approach for detecting ink mismatches in Hyperspectral (HS) document images. They employed deep learning techniques to reshape HS images into formats suitable for Convolutional Neural Networks (CNN) and subsequently used CNN for classification. This novel method yielded impressive detection accuracies of 98.2% and 88% for blue and black ink, respectively.

(Luo et al., 2015) made an effort to overcome the primary constraints in detecting ink mismatches, which typically necessitated prior information about the number of inks to be discriminated and the uniformity in their relative proportions within the examined image. To tackle these limitations, they employed anomaly detection in combination with unsupervised clustering and subsequently subjected it to testing. This innovative approach resulted in a detection accuracy of 89.0% for blue ink and 82.3% for black ink, respectively.

(A.R. Martins, et al., 2019) proposed that determining the chronological sequence of overlapped lines presented a recurring challenge in the forensic examination of documents. To offer a straightforward analysis protocol for this issue, they employed the hyperspectral mode of the VSC6000 for mapping. Their sample encompassed a total of 49 overlapping lines drawn on white paper using 7 different brands of blue ballpoint pens, and they chose bands within the range of 400 to 1000 nm. They conducted the analysis using HYPER-Tools and applied univariate analysis (UA) along with Multivariate Curve Resolution-Alternating Least Squares (MCR-ALS) for processing. This developed protocol succeeded in determining the chronological sequence of 31 out of the 49 overlapped lines, achieving an accuracy rate of 63%.

(Kang, et al. 2016) introduced a system for identifying counterfeit banknotes by utilizing multispectral images within the visual (VIS) and IR spectrum. They partitioned the banknotes into multiple sections and extracted features from each section to expedite data processing.

After data processing, they employed a Gaussian Maximum Likelihood (ML) classifier for classification. The results of their experiment were remarkable, achieving an accuracy rate of 99.97%, correctly classifying 8546 out of 8549 banknotes.

(J.M. del Hoyo-Meléndez, et al., 1932-1934) endeavored to authenticate outdated banknotes employing various techniques. In the context of HSI, they set up a SPECIM HS system operating in a pushbroom configuration, capturing 776 spectral bands within a range of 400–100 nm. The acquired images were subsequently subjected to dark current correction and normalization using a white reference. Envi 5.0 software was employed for data processing. The HSI analysis revealed the use of different types of papers for printing the banknotes, exhibiting clear spectral differentiation in two suspicious banknotes. It is important to note that the study did not assess detection accuracy.

2.8 Focused Security features for authentication

Transactions involving cash at a point-of-sale are typically conducted with speed and automation (van der Horst & Matthijsen, 2013). Individuals often do not allow themselves ample time or may experience discomfort when carefully inspecting a banknote (De Heij, 2017). To ensure the proper authentication of a banknote, an effective approach involves focusing on its security features. Attentional orientation can occur through both bottom-up and top-down processes. Bottom-up attention is typically triggered automatically based on scene characteristics and the salience of the stimulus (Theeuwes et al., 2003). However, it's worth noting that the capture of attention can be controlled through inhibitory mechanisms designed to suppress salient stimuli (Luck et al., 2021).

Top-down attention, which is believed to be responsible for such inhibition, is typically engaged deliberately in accordance with one's tasks and objectives (Egeth, Yantis, 1997). Nevertheless, the top-down authentication of banknotes might be hindered by the handler's previously mentioned lack of knowledge. Hence, it would be ideal if security features could naturally and rapidly capture attention through a bottom-up process (Theeuwes, 2019).

It's important to highlight that there has been a notable increase in the circulation of simplified counterfeit banknotes lacking replicated security features (Deutsche Bundesbank, 2020). This suggests that if attention could be swiftly and momentarily directed to the specific areas on a banknote, it might enhance counterfeit detection. This underscores the significance of guiding the attention of banknote users toward the security features.

It's not unexpected that the concept of saliency is familiar to security feature developers of banknotes. For example, technologies like nano-optic displays offer dynamic effects such as movement, 3D depth, and a variety of colors. While extensive research indicates that attention can be directed effectively using conspicuous visual cues (Theeuwes, 2010), it's essential to acknowledge a potential limitation. It is a well-established fact that the most eye-catching elements in a visual display tend to capture attention initially, regardless of their relevance or irrelevance (Wang, Theeuwes, 2020).

Consequently, when the prominent element coincides with the location of the security feature, as exemplified by a pink frame surrounding the banknote's emerald number, there arises a question: Would attention be primarily drawn to the pink frame or the emerald number itself? In the former scenario, the conspicuous element serves as a general guide for attention (e.g., directing it to the right quadrant of the banknote), yet it might interfere at a more detailed level (e.g., focusing attention on the pink frame rather than the content within the frame). The selection of the color pink (a desaturated red) for the frame was based on its high saliency. (Drelie Gelasca et al., 2005) conducted an experiment in which participants were asked to rank 12 colors according to their saliency.

The colors that received significantly more attention were red, yellow, green, and pink, while those with lower saliency appeared to be light blue, maroon, violet, and dark green. Furthermore, in a color-based experiment where two groups were tasked with identifying desaturated targets among saturated and white distractors, it was observed that pink and peach targets exhibited an advantage in terms of reaction times compared to green, blue, and purple targets (Kuzmova et al., 2008).

However, it's important to note that there is currently no scientific information available regarding the effectiveness of enhancing the saliency of security features. Additionally, one should consider the possibility that by increasing the saliency of one security feature, attention might be drawn away from other security features. Therefore, achieving an optimal balance of saliency across various features poses a challenge, especially considering that these features vary in terms of shape and size.

2.8.1 Machine learning and artificial intelligence authentication

In their research, (Chi-Yuan Yeh, Wen-Pin Su, Shie-Jue Lee, 2011) introduced a system for recognizing counterfeit banknotes, which is founded on multiple-kernel support vector machines. They developed a support vector machine (SVM) with the aim of reducing false positive rates. Through experiments conducted with Taiwanese banknotes, their proposed approach demonstrated superior performance compared to single-kernel SVMs, standard SVMs employing SDP, and multiple-SVM classifiers.

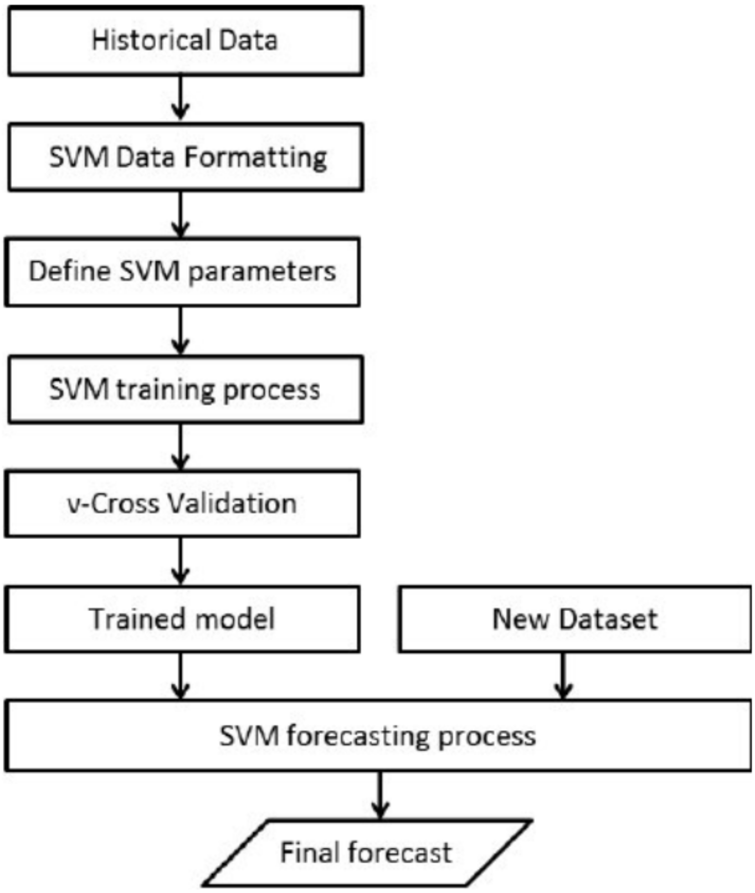


Figure 13. Basic SVM flowchart .

(Lanckriet et al., 2004) employed a technique that involves the linear combination of matrices to amalgamate multiple kernels. They integrated this approach with Support Vector Machines (SVMs) and transformed the problem into a Semi-Definite Programming (SDP) problem. SDP, being a convex optimization problem, offers a global optimum solution and can be efficiently resolved using the interior-point method. Other effective algorithms for multiple-kernel learning have also been proposed, including those by (Bach et al., 2004; Sonnenburg et al., 2008; and Rakotomamonjy et al., 2014). These methods address large-scale problems by iteratively utilizing the Sequential Minimal Optimization (SMO) algorithm to update Lagrange multipliers and kernel weights. However, it's important to note that while these approaches are faster than SDP, they can sometimes be susceptible to becoming trapped in local minima.

(Takeda et al., 1999) introduced a method that optimizes masks using genetic algorithms (GA) and neural networks to detect counterfeit banknotes. (Frosini et al., 1996) utilized neural networks to create a system for recognizing and verifying paper currency. (He et al., 2004) introduced one-class classifiers for counterfeit banknote recognition, where each banknote is subdivided into segments, and an individual classifier is developed for each segment. These classifiers are subsequently combined to make the final decision. To further enhance their approach, a genetic algorithm (GA) is employed to determine optimal values for parameters m and n. Nevertheless, it's worth noting that this GA-based method is considerably time-consuming. (Ionescu & Ralescu, 2005) also proposed one-class classifiers for counterfeit banknote recognition. In their approach, specific regions are identified for each banknote, and each of these regions is divided into segments. Furthermore, they use fuzzy Hamming distance to gauge the similarity between banknotes.

A currency recognition method was proposed by (Chang et al., 2007) using Support Vector Machine (SVM). In this study, watermark, hidden fluorescent fibers and color-changing ink were used as features of the banknote. These features were captured using separate hardware i.e., digital camera and sensors; and were used in collection of required information. The watermark was captured using digital camera; while fluorescent fiber features were extracted by applying spectral analysis on reflected signal of low-cost ultraviolet sensors. Then, color-changing ink was captured using an optoelectronic device. After capturing these features, Support Vector Machine (SVM) was used for classification.

Support vector machines (SVMs) have proven to be a valuable tool in addressing classification problems, as demonstrated in prior studies. Nevertheless, it is essential for the user to predefine the kernel function and its associated hyperparameters. Inappropriately selected kernel functions or hyperparameters can result in a considerable decrease in performance. Consequently, the task of identifying appropriate kernel functions and hyperparameters is a critical concern when employing SVMs.

2.8.2 Authentication using RBF

Sarfraz introduced the utilization of a radial basis function (RBF) neural network to recognize banknote currency, with a specific emphasis on Saudi Arabia's currency. Following the extraction of features and the classification process, the model demonstrated a level of accuracy that can be considered reasonable. An enhanced feed-forward neural network, guided by a mixed-margin principle, demonstrated superior flexibility and accuracy with a reduced requirement for training samples. This margin-based feed-forward neural network was applied to banknote data and achieved notably higher accuracy when compared to conventional methods like ANN, SVM, and AdaBoost algorithms.

According to (Sargano *et al.,* 2014*)*, they claim to be the first to conduct recognition for Pakistani banknotes. Ten different currency papers totally 175 banknotes were used. Essential features are extracted from the notes, which are passed as input for training a three-level feed-forward back-propagation neural network. Accurate detection was achieved after experimentations. The feature vectors are extracted from gray-level histogram shape descriptors and banknote image texture.

The feed-forward neural network is responsible for categorizing the feature vectors, resulting in an impressive accuracy rate of 98.6% when compared to other approaches like the pattern recognition feed-forward neural network (PRFNN), cascade forward neural network (CNN), and AdaBoost. (Kumar & Dudyala, 2015) conducted a comprehensive series of experiments focused on authenticating banknotes, employing various machine learning algorithms. In this particular context, various learning algorithms were put to use, including the probabilistic neural network (PNN), MLP, RBF, decision tree, and naïve Bayes. The results highlight the noteworthy performance of MLP and decision tree algorithms in accurately classifying banknote data for dependable predictions. To further bolster the identification of counterfeit banknotes, multispectral images of these notes are obtained by employing specially designed multispectral sensors intended for use in ATMs.

(Gai et al., 2013) delved into this topic by introducing a novel approach for feature extraction, harnessing the advantages of the quaternion wavelet transform (QWT). QWT produces one shift-invariant magnitude and three phases, rooted in quaternion algebra. To extract the statistical characteristics of QWT, the generalized Gaussian density was employed. Subsequently, the back propagation neural network was employed to classify the resulting extracted features. They also put forward a gene expression programming ensemble for the purpose of classifying banknote data. Their primary focus was an exhaustive analysis of various security features present on Indian banknotes. Their experimentation involved 1000 banknote samples, comprising 500 genuine and 500 counterfeit notes. The authors utilized k-means, NN, and SVM for the classification of banknotes.

The colour and texture features for classifying banknotes came to the fold in the work of (Garcia-Lamont *et al.,*2013*)*. With the colour feature modelled under RGB, texture feature on the other hand is modeled with binary patterns methods. For classification, the linear vector quantization (LVQ) networks are used and a non-parametric test based on *G* statistic is performed. High recognition accuracy rate is obtained by the LVQ classifier. A comprehensive review was conducted in the areas of the recognition and detection of banknotes. The review targets four keys research components namely; banknote recognition, counterfeit banknote detection, serial number recognition, and fitness classification with the application of various sensors. In-depth discussions and analysis of the different recognition methods, feature extractions techniques, and modes of algorithmic classification were reported.

2.8.3 Authentication via 2D infrared

(Spagnolo et al., 2010) proposed a method for currency verification based on security features of the banknote. These features include fiber structure and position of metallic color fiber which can only be observed under ultraviolet light. In this regard, banknotes were passed through the ultraviolet light to show the position of metallic color fiber and microscope was used to detect the metallic color fiber and digitized the captured images. The Central bank database was accessed for templates of the currency with a secure connection, then template from the bank and the one obtained with this process were matched with exclusive-OR, and results were generated.

(Spagnolo et al., 2010) also introduced another method for currency verification in addition to the one based on security features of the banknotes. In this technique they have used 2D barcode which can only be read using infrared light; this code was verified from the bank database.

2.8.4 Authentication using Classification

In their 2015 study (Gogoi et al.), it was suggested that Indian banknotes can be categorized by leveraging a set of distinctive and non-discriminatory attributes, which include characteristics such as color, dimensions, and, most notably, the Identification Mark unique to each denomination, as specified in the RBI guidelines. To commence the process, the system extracts the prevailing color and the aspect ratio of the currency note. Following this, it proceeds with segmenting the area of the note containing the distinct identification Mark. Subsequently, feature extraction is conducted on these segmented images using Fourier Descriptors. Given that each banknote possesses a unique shape due to its identification Mark, the classification of these shapes is executed with the aid of an Artificial Neural Network. Upon completing the feature extraction, the denominations are identified based on the developed algorithm. Notably, the proposed system demonstrated a remarkable success rate of 97% while necessitating only 2.52 seconds for processing.

2.8.5 Mobile app authentication

Mobile banking, as a channel, delivers consumers added convenience, instant accessibility, and a wider array of options. (Vyas, 2016) and (Rao et al., 2007) advocate for a broader perspective on mobile banking by banks, beyond its role as a mere extension of online banking. Instead, they suggest recognizing mobility as a robust and captivating standalone delivery channel. This approach empowers banks to offer end-users new advantages, such as immediate access and greater control over their personal finances. According to (Vyas, 2016), banks are targeting individuals who do not use online banking and may lack regular access to desktop Internet but are likely to own mobile devices.

The prototype system, detailed in "Smartphone Recognition of U.S. Banknote Denominations for the Visually Impaired" (Grijalva et al., 2010), was designed to assist visually impaired individuals in Ecuador in identifying the largest denomination of U.S. banknotes in circulation. The initial step involves digitally processing an image captured by a mobile phone camera to isolate a specific region of interest within that image. Subsequently, a recognition stage is applied to this Region of Interest, utilizing the Face Recognition using Eigenfaces method, which, in turn, relies on the mathematical technique called Principal Component Analysis (PCA). The paper concludes by presenting the results of tests conducted on the system, which was implemented on two mobile phones.

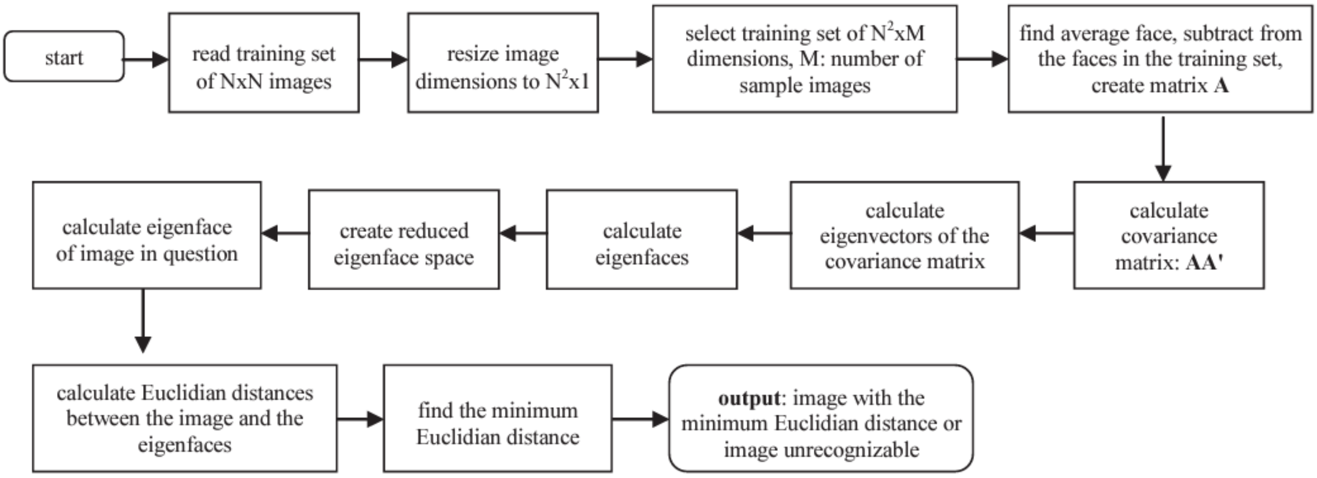

start
read training set of NxN images
resize image dimensions to N²x1
select training set of N²xM dimensions, M: number of sample images
find average face, subtract from the faces in the training set, create matrix A
calculate covariance matrix: AA'
calculate eigenvectors of the covariance matrix
calculate eigenfaces
create reduced eigenface space
calculate eigenface of image in question
calculate Euclidian distances between the image and the eigenfaces
find the minimum Euclidian distance
output: image with the minimum Euclidian distance or image unrecognizable

Figure 14. Eigenfaces method flow chart.

One of the key limitations of the system described in this paper is that the background of the image containing the object to be identified (i.e., the banknote) must have strong contrast with that object. Another constraint is that the lighting conditions across the image must be uniform.

(Paisios et al., 2012) introduced a mobile currency recognition system that employed the SIFT method for identifying partial images. They assessed the system using a constrained sample set that included varying conditions, such as folded, incomplete, or different orientations and rotations. The outcomes revealed that the nearest neighbor algorithm yielded an accuracy of 75%, while the nearest to the second-nearest neighbor ratio algorithm achieved a higher accuracy rate of 93.83%.

(Toytman & Thambidurai, 2011) introduced a banknote recognition system designed for Android, incorporating enhanced Speedup Robust Features (SIFT). This algorithm effectively addressed challenges related to varying illumination conditions, scale, and rotation. It displayed a notable tolerance to clutter, occlusion, and wrinkling of banknotes. The approach was assessed and yielded favorable results concerning clutter and variations in illumination. However, it did not resolve the issue of detecting folded banknotes. It's important to note that the paper did not furnish details regarding the algorithm's accuracy.

2.9 Blockchain in finance

Originally conceived as a distributed ledger system for managing bitcoin transactions, blockchain technology has its roots in the realm of financial technology (FinTech). While, for a period, it was somewhat eclipsed by the Bitcoin phenomenon, recent years have witnessed a significant shift in attention towards blockchain as an autonomous and foundational technology within the FinTech landscape (Du, Pan, Dorothy, Leidner, & Yinga, 2019).

Scholars and industry experts have come to recognize that the influence of blockchain extends far beyond the confines of bitcoin and even transcends the boundaries of the financial sector, catalyzing transformative effects across a wide spectrum of industries (Ølnes, Ubacht, & Janssen, 2017). Indeed, blockchain stands out as one of the most promising and advanced technologies in the broader FinTech domain (Du et al., 2019). While its initial purpose was to serve as a decentralized ledger for monitoring bitcoin transactions, the potential of blockchain transcends this limited scope, promising to revolutionize various operational aspects of businesses, both within the financial sector and across diverse commercial domains (Kshetri, 2018; Underwood, 2016).

At its core, a blockchain comprises a sequence of data blocks, each designed to document transactions. Every block contains a cryptographic hash of the preceding block, a timestamp, and transaction data (Du et al., 2019).

While blockchain technology has assumed a pivotal role in fostering financial innovations and serving as the fundamental driving force behind the FinTech revolution, its primary application has largely centered around the realm of payments. Advances in technology and evolving business processes, coupled with the ever-growing consumer demands, have instigated the transformation and development of payment instruments and systems. The fundamental aim of any payment system remains the facilitation of secure and intelligent transactions (Ali, Barrdear, Clews, & Southgate, 2014; Kshetri, 2018).

Cryptocurrencies make use of decentralized peer-to-peer (P2P) networks, encryption methods, cryptographic techniques, and a public key infrastructure (PKI) in which pairs of public and private keys are employed to ensure the secure transfer of data (Abramova & Böhme, 2016). Another compelling application of blockchain technology is its role as an autonomous, self-governing, and self-regulating infrastructure, specifically designed to enable the functioning of distributed autonomous organizations (Beck, Czepluch, Lollike, & Malone, 2016; Chapron, 2017; Peters & Panayi, 2015; Wörner, von Bomhard, Schreier, and Bilgeri et al., 2016).

In this alternative system, data and actions can be executed without the necessity of routing them through a central authority, thereby obviating the need for such an intermediary. As a consequence, transactions become irreversible, and the associated transaction costs are lowered. Notably, the reliance on trusted governments, private enterprises, mediators, and counterparties is eliminated in this paradigm, as trust is now vested in the protocols and the underlying infrastructure (Karafiloski & Mishev, 2017).

In this emerging field, there is a noticeable dearth of substantial academic research and publications, despite the profound potential of this technology (Yli-Huumo et al., 2016). According to Elsevier's Scopus database, the keyword 'blockchain' yields a meager 331 documents as of March 5, 2018. Intriguingly, the majority of these articles, about three-quarters, were authored in 2016. Furthermore, a mere 2.5 percent of these articles emphasize finance or business-related themes, underscoring the pressing need for additional research in this domain (Yli-Huumo et al., 2016).

The inherent decentralization of these payment systems and platforms presents several significant challenges (Lindman et al., 2017). These challenges encompass issues like ensuring privacy and trust within a platform-mediated network and identifying ways to mitigate associated risks and obstacles. To achieve more advantageous, trustworthy, and efficient services for consumers, it is imperative to gain a deeper comprehension of these challenges and the corresponding benefits (Lindman et al., 2017).

This literature review explores the evolution and significance of methods used to verify the authenticity of currency. It discusses the historical context of banknote authentication and the pivotal role played by advanced technologies, particularly machine learning and blockchain, in this field. Additionally, the review underscores the crucial importance of secure and intelligent payment systems in contemporary finance. It emphasizes the need for further research in this domain, pinpointing challenges related to decentralized payment systems, trust, privacy, and risk mitigation. Overall, the literature review highlights the critical role of banknote authentication in the financial sector and its broader implications for the industry.

In conclusion, research on authenticating banknotes is instrumental in preserving the integrity of financial systems, adapting to technological advancements, enhancing security and privacy, and promoting economic stability. This research is not only relevant within the financial sector but also holds broader implications for various industries, underlining its continued importance in our increasingly digitized and interconnected world.

CHAPTER THREE

3.0 Introduction

In the pursuit of ensuring the security and integrity of financial systems, the authentication of banknotes emerges as a critical undertaking. This methodology chapter delineates the systematic and rigorous approach undertaken to authenticate banknotes, a process vital for safeguarding economies against the threats posed by counterfeit currency. Our aim is to identify and extract relevant features from the banknote images, such as variance, skewness, kurtosis and entropy, employed as statistical measures to characterize and analyze various aspects of the banknote images. These features will be useful in the development of image processing and analysis techniques, and therefore in distinguishing genuine banknotes from counterfeit ones.

3.1 Research Design

(Cooper & Schlinder, 2001) define research design as the outline for data collection, measurement and analysis. A research design shows the general plan of how the researcher intends to go about answering the research questions. (Saunders, Lewis & Thornhill, 2007). This study used descriptive study and a survey was conducted with the aim of establishing the relationship between firm characteristics and income diversification in Kenya.

This study is going to incorporate a mixed research method, which combines both qualitative and quantitative approaches. This will offer a comprehensive and nuanced understanding of the research question or problem. The integration of both methods will give a chance to capitalize on the strengths of each approach, addressing the limitations inherent in using only one. While quantitative methods provide numerical data, statistical analyses, and generalizable patterns, qualitative methods offer in-depth insights into the context, motivations, and meanings behind the observed phenomena. By employing a mixed research method, we can triangulate findings, ensuring greater validity and reliability. This approach enables a more holistic exploration of complex research questions, facilitating a deeper comprehension of the studied phenomena. Additionally, the combination of qualitative and quantitative data allows for a more robust interpretation and validation of results, leading to richer conclusions and, ultimately, a more comprehensive contribution to the existing body of knowledge in the field.

3.0.1 System Development Methodology

The Agile methodology stands out as particularly suitable for developing a banknote authentication system utilizing the Random Forest algorithm due to its inherent flexibility, adaptability, and iterative nature. In the realm of machine learning, especially with evolving datasets and potential variations in counterfeit strategies, an Agile approach allows for continuous refinement and enhancement of the authentication model. The iterative development cycles enable quick adaptations to emerging requirements and changes in the financial landscape, ensuring that the system remains responsive to real-world scenarios. The collaborative nature of Agile methodologies, fostering regular communication and collaboration among cross-functional teams, including data scientists and developers, aligns seamlessly with the dynamic demands of developing and fine-tuning a Random Forest-based authentication system. This iterative and collaborative approach empowers the team to address challenges, incorporate feedback, and deliver a robust and adaptive banknote authentication system that meets the evolving needs of the financial sector.

3.0.2 Stages of development in Agile methodology

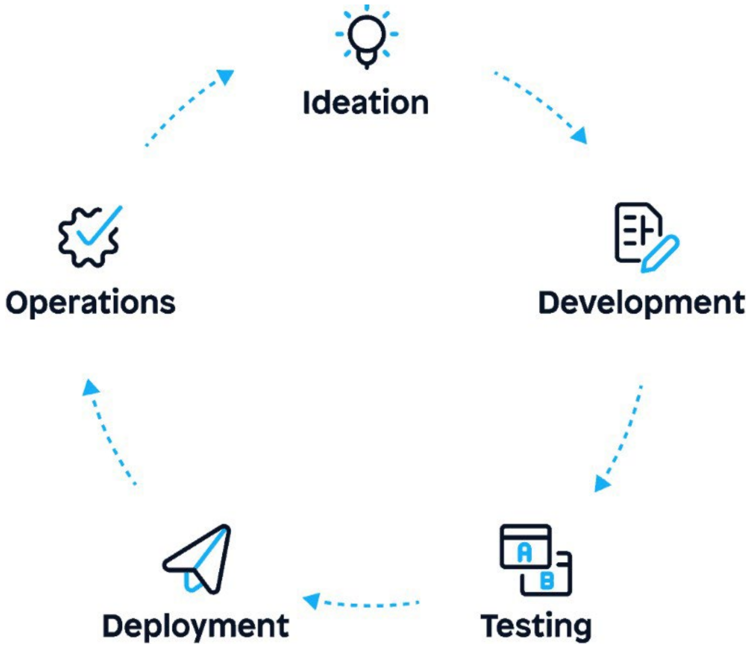


Figure 15. Agile methodology cycle.

Stage 1: Ideation

This is the stage where stakeholders, the business team, developers, and future app users formulate the purpose and goals of the system.

Stage 2: Development

The development phase includes all related production tasks in the SDLC, such as design, architecting, and coding. Developing the first iteration of a software product is often the longest stage of the Agile application development lifecycle.

Stage 3: Testing

Before release, the app has to go through a quality assurance check. The Agile team tests the app to ensure full functionality by, Checking that the code is clean, Addressing bugs/errors and Performing trial runs.

Stage 4: Deployment

Once the app is ready for release, the Agile team deploys it to the cloud or an on-premise server.

Stage 5: Operations

Ongoing maintenance helps squash bugs and maintain functionality. As users engage with the app, there will be opportunities to collect feedback and make improvements to release in future iterations.

3.2 Participants or Sample

(Cooper & Schindler, 2001) define a population as the total collection of elements which the researcher would like to make some interpretations. Machine learning algorithms learn from the dataset. Statistical algorithms are used behind the scenes to make a machine learning model learn from the data. Therefore, to identify whether a banknote is real or not, we needed a dataset of real as well as fake bank notes along with their different features. Luckily, we found such dataset at UCI Machine Learning repository, which is a repository of freely available datasets.

Data were extracted from images that were taken from genuine and forged banknote-like specimens. For digitization, an industrial camera usually used for print inspection was used. The final images have 400x 400 pixels. Due to the object lens and distance to the investigated object gray-scale pictures with a resolution of about 660 dpi were gained. Wavelet Transform tool were used to extract features from images.

The dataset contains 1372 records. Our dataset will focus on four features: variance, skewness, curtosis and entropy, while the class category refers to whether or not the banknote is real or not.

3.3 Data Collection

A data collection instrument is a method used for collecting data from the target population. A research instrument ensures that the right data is collected from the right population (Kothari, 2004). Research instrument refers to tools for data collection and can be through questionnaire, interview, survey or observation or obtaining data from credible secondary sources. The research instrument for this study is through obtaining data from secondary sources. This choice is informed by the fact that they help the researcher access objectivity of the data (Adedokun, 2003). The source of our data will be **UCI Machine Learning repository.**

3.4 Data Analysis

Data analysis is the process of inspecting, cleaning, transforming, and modeling data to extract meaningful information, draw conclusions, and support decision-making. It involves the use of various techniques, methods, and tools to uncover patterns, trends, relationships, and insights within a dataset. The goal of data analysis is to convert raw data into actionable knowledge, allowing individuals, organizations, or researchers to make informed decisions and predictions.

In this study statistical analysis is the preferred method for data analysis because it enhances the credibility and reliability of findings, facilitating evidence-based decision-making and contributing to the advancement of knowledge and understanding in various fields.

Jupyter Notebook will be used in this study. It is an open-source interactive web application that allows users to create and share documents that contain live code, equations, visualizations, and narrative text. It is widely used in data science, scientific research, machine learning, and education due to its flexibility and ease of use. Anaconda is another tool that will be used in this study. It is a distribution of the Python and R programming languages for scientific computing, that simplifies package management and deployment. The distribution includes data-science packages suitable for Windows, Linux, and macOS.

3.5 Ethical Considerations

3.5.1 Informed Consent

To make sure Participants are provided with a clear and comprehensive explanation of the purpose of the research. They need to understand how their involvement contributes to the project's goals, including the development of banknote authentication technology.

Participants must willingly agree to take part in the research without any coercion or undue influence. They should be informed that they have the right to withdraw from the study at any point without facing negative consequences.

3.5.2 Privacy

The study will clearly outline the type of data that will be collected. To ensure that the collection methods are minimally invasive and necessary for the research objectives.

Also implement robust security measures to protect the collected data. This includes encryption, access controls, and secure storage protocols to safeguard against unauthorized access.

3.5.3 Confidentiality

To clearly define how the collected data will be handled throughout the research process. Establish protocols for data access, sharing, and disposal to ensure that information remains confidential and is not misused.

3.5.4 Debriefing

To provide participants with a thorough debriefing at the conclusion of the study. This includes explaining the outcomes of the research, addressing any misconceptions, and ensuring that participants are informed about the use of the data they contributed.

3.5.5 Ethical Review

Depending on the nature and scope of the research, seek approval from an ethical review board. This ensures that the research design and procedures comply with ethical standards and guidelines.

3.5.6 Accessibility and Inclusivity

Ensure that all communication, including consent forms and debriefing materials, is presented in a language that is easily understandable by the participants. Additionally, consider the needs of participants with different abilities to ensure inclusivity.

3.6 Data Presentation

In machine learning, presenting data involves preparing and formatting the data in a way that is suitable for training models and extracting meaningful patterns. Some of the ways of presenting data used in this study are:

3.6.1 Data Preprocessing

We will utilize Scikit-learn library from python. It provides tools for handling missing values, converting data types, and other preprocessing tasks. It offers methods for scaling features, such as standardization or normalization, to ensure that features are on a similar scale.

3.6.2 Data Splitting

Scikit-learn library will provide Scikit-learn's train_test_split function which simplifies the process of splitting datasets into training and testing sets, a crucial step in evaluating model performance.

3.6.3 Feature Extraction

Scikit-learn includes methods for dimensionality reduction, such as Principal Component Analysis (PCA), which helps in reducing the number of features while preserving the most important information.

3.6.4 Statistical Data Visualization

The Seaborn library from python is utilized in this study. It simplifies the process of creating complex statistical visualizations by providing functions that work directly with data frames. It can generate a variety of plots, including scatter plots, line plots, bar plots, and more.

3.6.5 Pair Plots

Seaborn's pairplot function will be utilized and enables the creation of a matrix of scatterplots for a dataset with multiple variables. This is useful for quickly examining relationships between different pairs of variables.

3.6.6 Customizable Color Palettes

Seaborn allows users to easily customize color palettes to suit their preferences or match the requirements of a specific visualization.

3.6.7 Array Creation

NumPy will provide a powerful array object that allows for the creation of arrays with various dimensions. These arrays can be used to represent vectors, matrices, or higher-dimensional tensors.

3.6.8 Line Plots

Matplotlib a python library will be used for creating line plots, which are useful for visualizing trends in data over a continuous variable, such as time.

3.6.9 Scatter Plots

Scatter plots in Matplotlib are useful for visualizing the relationship between two continuous variables and identifying patterns or outliers.

The methodology chapter in a banknote authentication project utilizing machine learning is of paramount importance as it delineates the systematic approach employed to achieve the project's objectives. It provides a transparent and reproducible account of key aspects such as data collection, preprocessing, feature selection, model development, and ethical considerations, ensuring the validity and reliability of the research findings. This chapter not only guides the execution of the project but also allows for the benchmarking and comparison of methodologies, fostering transparency and accountability in the development of machine learning models for banknote authentication. Additionally, the methodology chapter serves as a valuable resource for future research, enabling continuous learning, improvement, and the responsible deployment of technology in the field of financial security.

CHAPTER FOUR

4.0 System Analysis

4.1 Data Collection

4.1.0 Online Repositories and Archives

The study explored online repositories and archives that host datasets, research papers, and technical reports related to banknote authentication. Platforms like Kaggle, UCI Machine Learning Repository, and government archives may provide valuable datasets and research materials.

4.1.1 Industry Reports and White Papers

The study also utilized industry reports and white papers published by organizations specializing in security, currency, or machine learning applications. These reports may provide market trends, technological advancements, and case studies related to banknote authentication.

4.1.2 Online Forums and Communities

Participate in online forums and communities dedicated to machine learning, data science, or financial technology. Discussions in these platforms may point to recent developments, shared resources, and practical insights into banknote authentication.

4.1.3 Academic Theses and Dissertations

We explored academic theses and dissertations on topics related to machine learning and banknote authentication. University repositories and databases often house comprehensive research conducted by graduate students.

4.1.4 Official Reports and Publications

Another useful source was official reports and publications from financial institutions, central banks, and government agencies responsible for currency production. These documents contain insights into the security features of banknotes and the challenges addressed by existing authentication systems.

4.2 User requirements for the system

4.2.1 Accuracy and Reliability

The system should achieve a high level of accuracy and reliability in authenticating banknotes to minimize false positives and negatives. Users typically expect the machine learning model to correctly identify genuine banknotes and detect counterfeit ones with a high degree of accuracy.

4.2.2 Real-time Processing

The system should process authentication requests in real-time. Users often require quick and efficient authentication to streamline processes such as cash handling in banks or retail environments.

4.2.3 Adaptability to Currency Variations

The system should be adaptable to different currencies and denominations. Users may need the authentication system to handle various types of banknotes, each with its unique security features.

4.2.4 User-Friendly Interface

The user interface should be intuitive and user-friendly. Users, especially those who may not have a technical background, should be able to interact with the authentication system easily.

4.2.5 Integration with Existing Systems

The system should seamlessly integrate with existing banking or financial systems.Users may want the authentication system to work as part of a broader financial infrastructure, ensuring smooth integration with existing processes.

4.2.6 Scalability

The system should be scalable to handle varying volumes of banknote authentication requests.

As user demands change, the system should be able to scale its processing capabilities accordingly.

4.2.7 Security and Privacy

The system should adhere to high standards of security and data privacy. Users expect that sensitive information related to banknotes and authentication processes is securely handled and that the system complies with privacy regulations.

4.2.8 Training and Support

The system should come with comprehensive training materials and support resources.

Users should have access to training programs and support channels to ensure effective use of the authentication system.

4.3 Business needs of the system

4.3.1 Enhanced Security

Improve the overall security of financial transactions and cash handling processes. Businesses, especially those in the financial sector, require robust authentication systems to protect against counterfeit banknotes, enhancing the integrity of financial transactions.

4.3.2 Risk Mitigation

Mitigate the risks associated with counterfeit banknotes and fraudulent activities. A machine learning-based authentication system helps businesses minimize the financial and reputational risks associated with accepting counterfeit currency.

4.3.3 Operational Efficiency

Streamline and optimize operational processes related to banknote handling and authentication.

Efficiency gains in authentication processes contribute to faster and more streamlined operations, reducing manual efforts and transaction processing times.

4.3.4 Customer Trust and Satisfaction

Build and maintain trust with customers by ensuring the authenticity of banknotes. Providing customers with confidence that the business employs state-of-the-art technology to authenticate banknotes contributes to overall customer satisfaction and trust.

4.3.5 Brand Protection

Protect the brand reputation by ensuring the integrity of financial transactions. Implementing advanced authentication methods demonstrates a commitment to security and professionalism, positively impacting the business's brand image.

4.4 Feasibility Analysis

4.4.1 Technical

4.4.1.1Data Availability and Quality

Availability of a sufficient and high-quality dataset for training and testing the machine learning model. Assess the accessibility of diverse and representative data that includes genuine and counterfeit banknotes. The quality of the dataset significantly impacts the model's ability to generalize to real-world scenarios.

4.4.1.2 Algorithm Selection

Identification of machine learning algorithms suitable for banknote authentication.

Evaluate different machine learning algorithms (e.g., Random Forest, support vector machines, Logistic regression) to determine the most suitable approach for the specific characteristics of banknote authentication, considering factors like feature complexity and interpretability.

4.4.1.3 Feature Extraction and Selection

Feasibility of extracting relevant features from banknote images and selecting the most discriminative ones. Determine the feasibility of extracting features (such as variance, skew, curtosis, entropy) from banknote images and selecting those that contribute most to the authentication task.

4.4.1.4 Model Training and Optimization

Ability to train and optimize machine learning models efficiently. Assess the computational resources required for model training, hyperparameter tuning, and optimization. Consider parallel processing or cloud-based solutions for scalability.

4.4.1.5 Real-time Processing

Ability to process banknote authentication requests in real-time. Evaluate the computational efficiency of the machine learning model to ensure that authentication can be performed within the required time constraints, especially in scenarios where real-time processing is essential.

4.4.1.6 Integration with Existing Systems

Compatibility with existing banking or financial systems. Evaluate the ease of integrating the banknote authentication system with existing infrastructure, ensuring interoperability and minimal disruptions to current processes.

4.4.1.7 Scalability

Scalability to handle varying volumes of banknote authentication requests. Considerations: Assess whether the system can scale efficiently to accommodate increased transaction volumes without compromising performance or accuracy.

4.4.2 Operational

4.4.2.1 User Acceptance

Willingness of end-users to accept and adopt the machine learning-based authentication system. Conduct user surveys, interviews, or pilot programs to gauge the acceptance of the system among individuals who will interact with it regularly. Address any concerns or resistance through effective communication and training.

4.4.2.2 Training Requirements

Feasibility of providing necessary training to users for operating and understanding the banknote authentication system. Assess the level of training required for end-users to effectively use the system. Develop training programs and materials to ensure users are proficient in utilizing the system.

4.4.2.3 Integration with Workflows

Integration of the authentication system with existing operational workflows. Evaluate how seamlessly the machine learning system can be integrated into current business processes without causing disruptions. Minimize the impact on daily operations.

4.4.2.4 User Interface Design

Design of a user-friendly interface for interacting with the authentication system.

Ensure that the user interface is intuitive, easy to navigate, and requires minimal training for users to understand and operate effectively.

4.4.2.5 Accessibility and Availability

Availability and accessibility of the authentication system to users. Confirm that the system is available and accessible when needed. Assess potential downtime, maintenance schedules, and measures in place to ensure continuous availability.

4.4.2.6 Operational Impact

Assessment of the impact on current operations. Evaluate how the introduction of the authentication system will impact daily routines and tasks. Minimize disruptions and plan for a smooth transition to the new system.

4.4.3 Economic feasibility of the system

4.4.3.1 Cost-Benefit Analysis

Conduct a comprehensive cost-benefit analysis to evaluate the economic viability of the project. Compare the initial and ongoing costs of implementing the machine learning-based authentication system against the expected benefits, including cost savings from reduced counterfeit acceptance and potential revenue gains.

4.4.3.2 Initial Investment

Assess the initial investment required for developing and deploying the authentication system.

Consider costs related to software development, hardware acquisition, data acquisition, training, and any other initial investment needed for the project.

4.4.3.3 Operational Costs

Estimate the ongoing operational costs associated with maintaining and using the authentication system. Include costs for system maintenance, regular updates, training, support, and any additional operational expenses. Evaluate whether these costs align with the benefits derived from the system.

4.4.3.4 Savings from Counterfeit Prevention

Evaluate the potential savings resulting from preventing the acceptance of counterfeit banknotes. Estimate the financial impact of reducing losses incurred due to counterfeit currency, including direct financial losses and potential damage to the organization's reputation.

4.4.3.7 Return on Investment (ROI)

Determine the expected return on investment over a specific period. Calculate the ratio of the net benefits (savings and additional revenue) to the total costs. A positive ROI indicates economic feasibility.

4.4.3.6 Cost of Downtime and System Errors

Assess the economic impact of system downtime and errors. Consider the potential financial losses resulting from disruptions to operations, user dissatisfaction, and potential penalties. Implement measures to minimize downtime and errors.

4.4.3.7 Market Demand and Competitiveness

Evaluate the market demand for a secure banknote authentication system and the competitiveness of the proposed solution. Assess whether the solution meets a genuine market need and how it compares to existing alternatives. Consider the potential for gaining a competitive advantage.

4.4.4 Scheduling feasibility of the system

4.4.4.1 Project Timeline

Define a realistic and achievable project timeline. Break down the project into phases, specifying key milestones, and allocate time for each stage, including data collection, model development, testing, and deployment.

4.4.4.2 Development Time

Estimate the time required for developing the machine learning model and authentication system. Assess the complexity of the model, the availability of skilled personnel, and the time needed for data preprocessing, feature engineering, and algorithm selection.

4.4.4.3 Data Collection and Preparation

Determine the time required for collecting and preparing the dataset for training and testing. Evaluate the availability of relevant and representative data. Consider any potential challenges in obtaining the required data and the time needed for cleaning and preprocessing.

4.4.4.4 Training Time

Estimate the time needed for training the machine learning model. Consider the computational resources available for model training, the size of the dataset, and the complexity of the chosen algorithm.

4.4.4.5 Testing and Validation

Allocate time for thorough testing and validation of the authentication system.

Plan for comprehensive testing, including unit testing, integration testing, and validation against real-world scenarios. Ensure that sufficient time is allotted for debugging and refining the model.

4.4.4.6 User Training

Determine the time needed for training end-users to interact with the authentication system.

Develop training materials and sessions to familiarize users with the system interface and functionality. Plan for ongoing support and training as needed.

4.4.4.7 Integration with Existing Systems

Allocate time for integrating the authentication system with existing operational workflows.

Coordinate with relevant stakeholders to ensure smooth integration, minimizing disruptions to current processes. Plan for any necessary system adjustments during the integration phase.

4.4.4.8 Deployment Time

Estimate the time required for deploying the authentication system in the production environment. Plan for a phased deployment approach if necessary, ensuring that the system is gradually introduced to minimize disruptions.

4.4.5 Software Requirement Specification

4.4.5.1 Functional requirements

4.4.5.1.1 Banknote Image Input

The system should be able to accept digital images of banknotes as input for the authentication process. Users should be able to submit images of banknotes captured through cameras, scanners, or other imaging devices.

4.4.5.1.2 Data Preprocessing

The system should perform preprocessing on input images to enhance their quality and extract relevant features. Preprocessing steps may include image normalization, resizing, noise reduction, and other techniques to prepare images for analysis.

4.4.5.1.3 Feature Extraction

Implement algorithms for extracting key features from banknote images. Features here include kurtosis, variance, skewness and entropy.

4.4.5.1.4 Machine Learning Model

Develop and integrate a machine learning model for banknote authentication. Implement a classification model, such as supervised machine capable of learning and making predictions based on the extracted features.

4.4.5.1.5 Training Mechanism

Provide a mechanism for training the machine learning model. Users should be able to train the model with labeled datasets to enhance its ability to distinguish between genuine and counterfeit banknotes.

4.4.5.1.6 Real-time Processing

The system should process authentication requests in real-time. Ensure that the authentication process is efficient and can be seamlessly integrated into real-world scenarios where quick decisions are necessary.

4.4.6 Non-functional requirements

4.4.6.1 Performance

The system should provide fast and efficient banknote authentication. Define performance metrics, such as response time and throughput, to ensure timely and effective authentication processing.

4.4.6.2 Scalability

Ensure that the system is scalable to handle varying volumes of authentication requests.Design the system architecture to accommodate growth in the number of users and transaction volumes.

4.4.6.3 Reliability

The system should demonstrate high reliability in making accurate authentication decisions.

Define reliability metrics, including the system's mean time between failures (MTBF) and mean time to recovery (MTTR).

4.4.6.4 Availability

The system should be highly available to users when needed. Specify availability targets, such as a percentage of uptime, to ensure continuous access to the authentication services.

4.4.6.5 Security

Implement robust security measures to protect against unauthorized access and ensure data integrity. Define security protocols, encryption standards, access controls, and measures to prevent tampering or attacks on the system.

4.4.6.6.Accuracy

The machine learning model should demonstrate high accuracy in authenticating banknotes.

Specify the acceptable level of accuracy, including false positive and false negative rates, to ensure reliable authentication.

4.4.6.7 Usability

The user interface should be intuitive and user-friendly. Assess the ease of use for end-users, providing a clear and straightforward interface for submitting banknote images and interpreting authentication results.

4.4.6.8 Maintainability

The system should be designed for ease of maintenance and updates. Implement modular and well-documented code, allowing for seamless updates, bug fixes, and enhancements to the system.

CHAPTER FIVE

5.0 System Design

5.1 Introduction

This chapter unfolds the intricacies of architecting a robust and effective solution for the reliable verification of banknote authenticity. Building upon the foundation laid during the requirements analysis phase, we delve into the systematic planning and structuring of our system. From the definition of system components to the identification of key processes, data flows, and external entities, our design endeavors to encapsulate a holistic view of the envisioned solution. Emphasizing clarity and coherence, the System Design chapter serves as a blueprint for the subsequent stages of implementation, testing, and deployment. As we navigate through the intricate decisions surrounding algorithm selection, data handling, and user interface design, this chapter aims to provide a comprehensive understanding of the design principles shaping our innovative banknote authentication system.

5.2 Dataflow Design

Design flow diagram of currency recognition system.

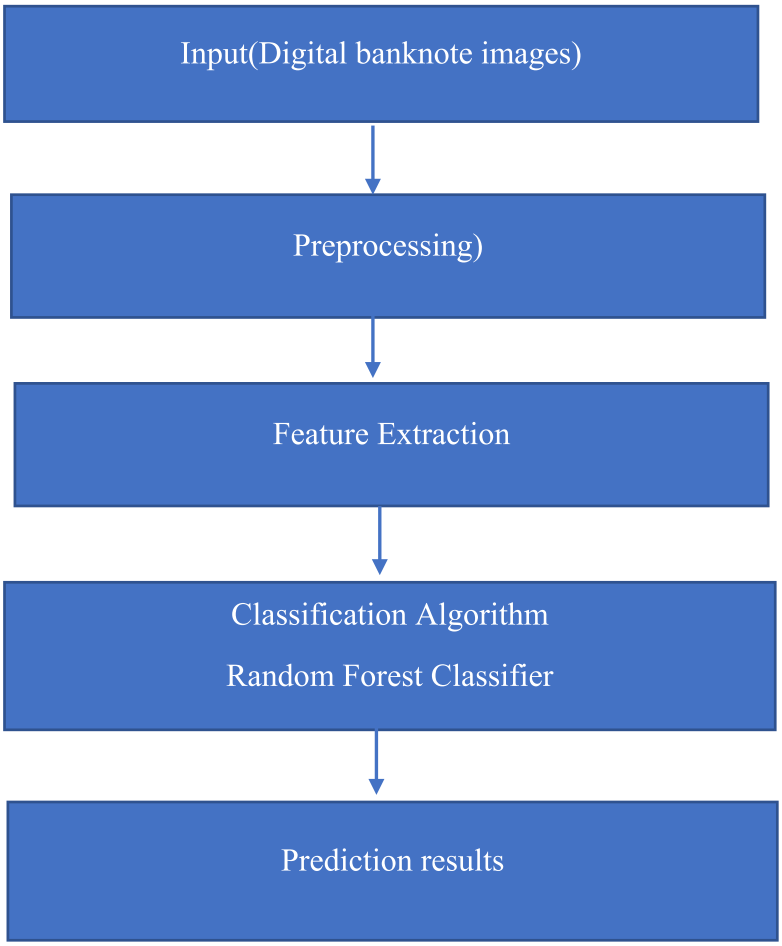


Figure 15. Design flow diagram .

Banknote image acquisition – The dataset is input into the system.

Image preprocessing - The images are preprocessed by splitting the dataset into training set and test set. This is done to improve the accuracy of the machine learning model.

Target Features - our dataset is already cleaned so the target features are skewness, curtosis, variance and entropy.

Machine learning classification - The selected features are input to a machine learning model to classify the banknote as genuine or counterfeit.

Classification result output - The classification result is output to the user.

5.3 Random Forest Classifier architecture

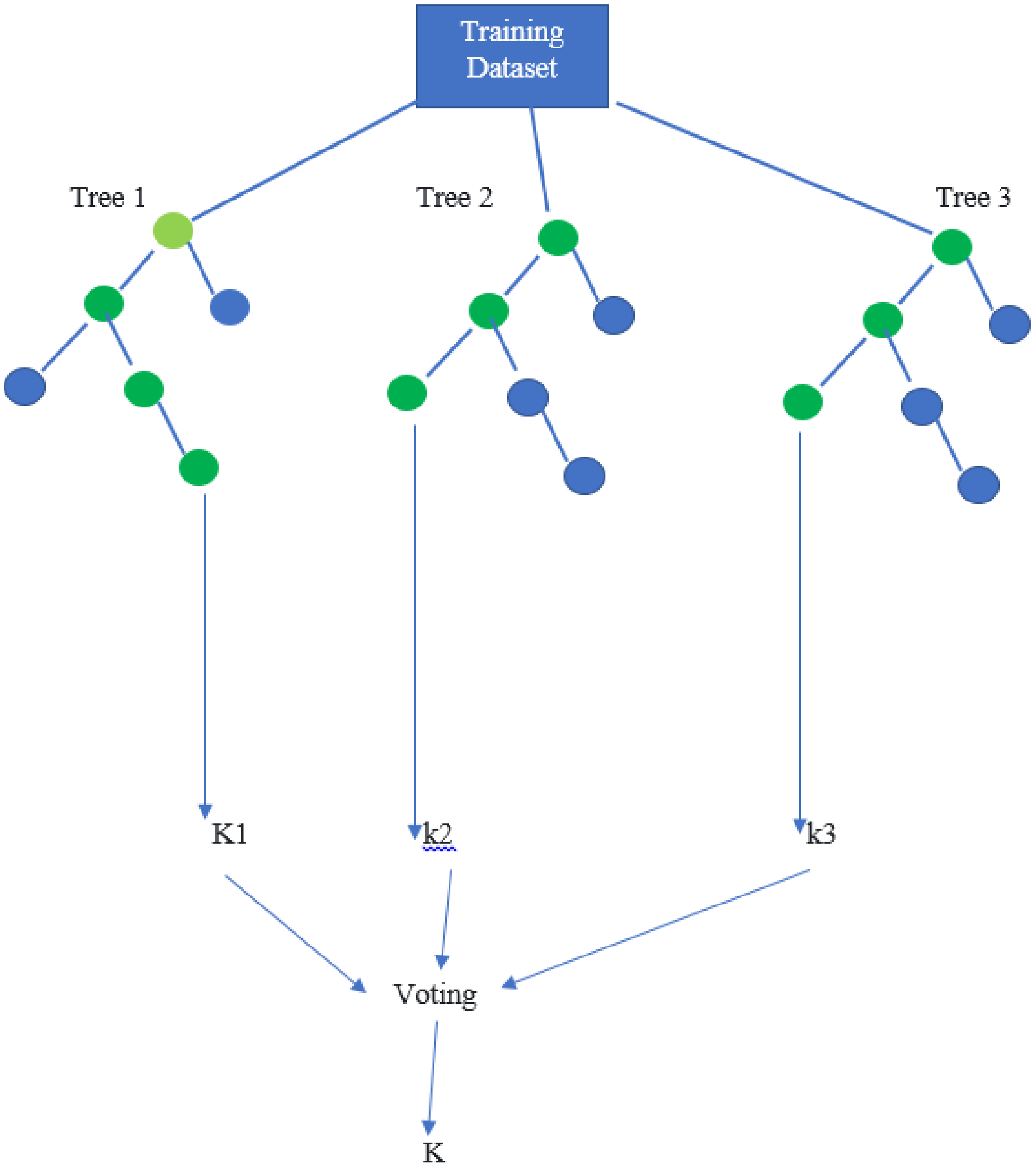


Figure 16. Random Forest Classifier architecture.

Bagging, also known as Bootstrap Aggregation, serves as the ensemble technique in the Random Forest algorithm. Here are the steps involved in Bagging:

Selection of Subset - Bagging starts by choosing a random sample, or subset, from the three it has created from the entire training dataset.

Bootstrap Sampling - Each model is then created from these samples, called Bootstrap Samples, which are taken from the original data with replacement. This process is known as row sampling.

Bootstrapping - The step of row sampling with replacement is referred to as bootstrapping.

Independent Model Training - Each model is trained independently on its corresponding Bootstrap Sample. This training process generates results for each model.

Majority Voting - The final output is determined by combining the results of all models through majority voting. The most commonly predicted outcome among the models is selected.

Aggregation – The final step, which involves combining all the results and generating the final output based on majority voting.

5.4 Random Forest Classifier process

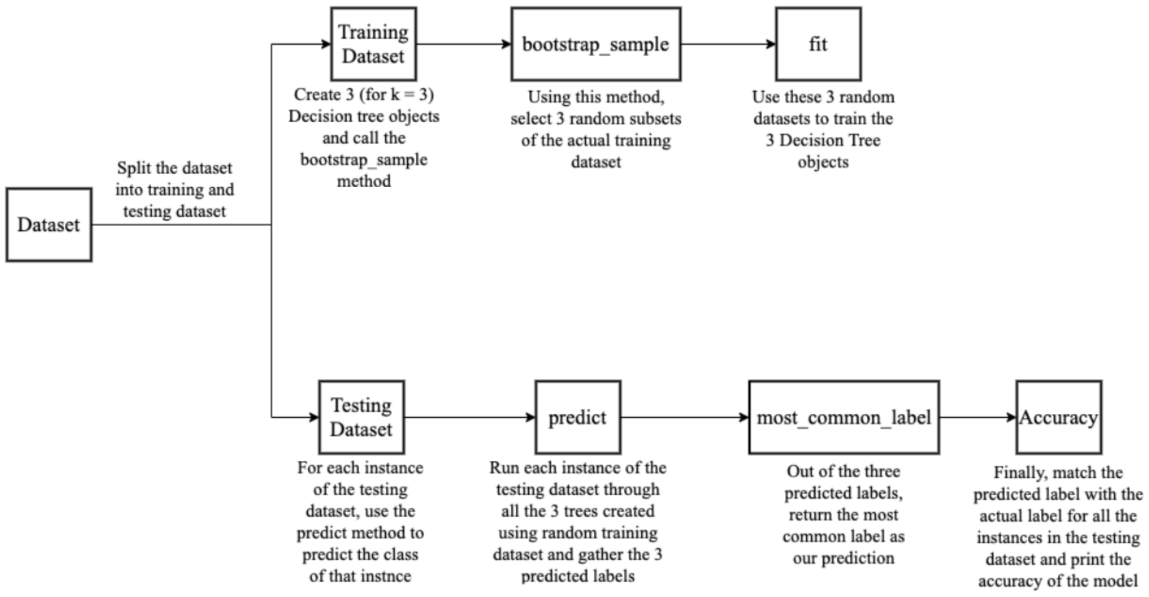

Dataset
Split the dataset into training and testing dataset
Training Dataset
Create 3 (for k = 3) Decision tree objects and call the bootstrap_sample method
bootstrap_sample
Using this method, select 3 random subsets of the actual training dataset
fit
Use these 3 random datasets to train the 3 Decision Tree objects
Testing Dataset
For each instance of the testing dataset, use the predict method to predict the class of that instnce
predict
Run each instance of the testing dataset through all the 3 trees created using random training dataset and gather the 3 predicted labels
most_common_label
Out of the three predicted labels, return the most common label as our prediction
Accuracy
Finally, match the predicted label with the actual label for all the instances in the testing dataset and print the accuracy of the model

Figure 17. Random Forest Classifier process.

1) Split the dataset into training and testing dataset.
2) Create 3 Decision tree objects and call the bootstrap_sample method.
3) Using this method, select 3 random subsets of the actual training dataset.
4) Use these 3 random datasets to train the 3 Decision Tree objects.
5) For each instance of the testing dataset, use the predict method to predict the class of that instance.

6) Run each instance of the testing dataset through all the 3 trees created using the random training dataset and gather the 3 predicted labels.
7) Out of the three predicted labels, return the most common label as our prediction.
8) Finally, match the predicted label with the actual label for all the instances in the testing dataset and print the accuracy of the model.

In conclusion, the system design phase of our banknote authentication system, leveraging the Random Forest algorithm, has resulted in a robust and effective solution for discerning the authenticity of banknotes. The chosen algorithm, Random Forest, proved to be a judicious selection, demonstrating its prowess in handling intricate patterns within the banknote data. Through careful consideration of key design elements such as data preprocessing, feature selection, and model training, we have achieved a system that excels in accuracy and reliability. Our validation efforts underscored the model's proficiency, consistently yielding high-performance metrics. Additionally, the scalability and efficiency of the system were thoroughly examined, ensuring its capability to handle diverse datasets and computational demands. The user experience and interface design considerations were integral, contributing to an accessible and intuitive system. This system design chapter lays the foundation for subsequent stages, emphasizing the significance of our approach in achieving the objectives set forth for the banknote authentication system.

CHAPTER SIX

6.0 System Implementation

6.1 Introduction

This chapter marks a pivotal phase in the development of our banknote authentication system, centered around the Random Forest algorithm. Building upon the comprehensive design laid out in previous chapters, this section delves into the practical realization of our envisioned solution. Herein, we navigate through the technological landscape, outlining the tools, languages, and frameworks chosen for the implementation. The intricate process of data preprocessing takes center stage, ensuring the seamless preparation of our banknote dataset for the rigorous training of the Random Forest model. As we integrate features and orchestrate the model training, we pay meticulous attention to the design and development of a user-friendly interface, a crucial facet enhancing the accessibility and usability of our system. The System Implementation chapter unfolds the intricate details of translating design concepts into a tangible, functioning system, laying the groundwork for comprehensive testing, validation, and eventual deployment in real-world scenarios.

6.2 Programming Language and Coding Tools

6.2.1 Python

Python's suitability for machine learning is unparalleled, owing to its versatility, extensive libraries, and vibrant community support. Python serves as the lingua franca for machine learning practitioners, providing a seamless environment for algorithm development, data manipulation, and model deployment. Frameworks like Scikit-Learn, TensorFlow, and PyTorch empower developers with user-friendly tools for building and training machine learning models, while libraries like NumPy and Pandas facilitate efficient data handling and preprocessing. Python's clear syntax and readability accelerate the development cycle, and its interactive environments, such as Jupyter Notebooks, offer an ideal space for exploration and experimentation. The language's adaptability extends to web development, enabling the creation of user interfaces and APIs for seamless integration of machine learning models into broader applications. Python's rich ecosystem, encompassing visualization tools like Matplotlib and community-driven knowledge sharing, further solidify its position as the language of choice for machine learning practitioners and researchers alike.

6.2.2 Jupyter notebook

Jupyter Notebook is a versatile and interactive computational environment that allows users to create and share documents containing live code, equations, visualizations, and narrative text. Named after the core programming languages it supports—Julia, Python, and R—Jupyter provides an open-source platform that fosters a seamless integration of code execution and data analysis. Its web-based interface facilitates the creation of documents, known as notebooks, where users can write and execute code in a modular and interactive fashion. Jupyter Notebooks support a wide array of programming languages, making them a popular choice for various scientific and data-driven tasks. The live code cells enable users to see the immediate results of their code, promoting an iterative and exploratory approach to data analysis, research, and education. Additionally, Jupyter Notebooks have become an invaluable tool for sharing reproducible research, collaborative projects, and educational materials, making them a cornerstone in the toolkit of data scientists, researchers, and educators.

6.2.3 Anaconda

Anaconda is a comprehensive open-source distribution and platform designed for simplifying and streamlining the process of data science and machine learning. Developed by Anaconda, Inc., this distribution includes a wide array of popular programming languages and libraries such as Python, R, and Jupyter, along with pre-installed data science and machine learning packages. Anaconda's strength lies in its ability to manage software dependencies efficiently through its package management system, making it easier for users to install, update, and maintain the diverse set of tools needed for data analysis and scientific computing. It also provides a user-friendly graphical interface, Anaconda Navigator, and a command-line interface for managing environments. Anaconda supports the creation of isolated environments, allowing users to work on different projects with distinct dependencies. With its emphasis on accessibility, reproducibility, and ease of use, Anaconda has become a preferred choice for individuals and organizations engaged in data science, scientific research, and machine learning.

6.3 Machine learning frameworks

6.3.1 Pandas

Pandas is an open-source data manipulation and analysis library for the Python programming language. Pandas provides high-performance, easy-to-use data structures and data analysis tools. The two primary data structures in Pandas are Series and DataFrame. A Series is a one-dimensional array with labeled indices, while a DataFrame is a two-dimensional table with rows and columns, similar to a spreadsheet. Pandas excels in handling heterogeneous and labeled data, making it a powerful tool for tasks such as data cleaning, exploration, and transformation. It offers a rich set of functions for indexing, slicing, aggregating, and merging data, making it a go-to library for data manipulation in various domains, including data science, finance, and research. The combination of its flexibility, functionality, and integration with other Python libraries has contributed to the widespread adoption of Pandas in the data science and analytics communities.

6.3.2 Numpy

NumPy, short for Numerical Python, is a fundamental open-source library for numerical computing in Python. It provides support for large, multi-dimensional arrays and matrices, along with a collection of mathematical functions to operate on these arrays efficiently. NumPy is a cornerstone in the Python scientific computing ecosystem and serves as the foundation for many other libraries and frameworks. Its primary data structure is the NumPy array, a homogeneous N-dimensional array that can store elements of the same data type. NumPy arrays are efficient for numerical operations, taking advantage of low-level optimizations and providing a convenient interface for mathematical computations. NumPy also offers tools for linear algebra, Fourier analysis, random number generation, and more. Its versatility and performance make NumPy an essential library for scientific computing, data analysis, and machine learning applications in Python.

6.3.3 Seaborn

Seaborn is a statistical data visualization library in Python that is built on top of Matplotlib. It provides a high-level interface for creating attractive and informative statistical graphics. Seaborn is particularly designed for visualizing complex datasets with minimal code, making it a popular choice for data scientists and analysts. It comes with several built-in themes and color palettes that enhance the aesthetics of plots, and it also provides functions for visualizing relationships in data through scatter plots, line plots, bar plots, and more. Seaborn excels in the creation of statistical graphics such as box plots, violin plots, and pair plots, which can reveal patterns and distributions in the data. Additionally, it seamlessly integrates with Pandas DataFrames, making it easy to work with structured data.

6.3.4 Testing

Software testing can be stated as the process of verifying and validating whether a software or application is bug-free, meets the technical requirements as guided by its design and development, and meets the user requirements effectively and efficiently by handling all the exceptional and boundary cases. The process of software testing aims not only at finding faults in the existing software but also at finding measures to improve the software in terms of efficiency, accuracy, and usability.

6.4 The Software Testing Technique

6.4.1 White-Box Testing

White box technique of testing was used to test this system. It is where the tester is aware of the internal workings of the product, has access to its source code, and is conducted by making sure that all internal operations are performed according to the specifications is known as white box testing.

6.4.2 Levels of software testing

6.4.2.1 Unit Testing

Unit testing was used to test each individual module. The purpose was to validate that each unit of the software performed as designed.

6.4.2.2 Integration Testing

Integration testing was used to test the software by combining individual units and testing them as a group. The purpose of this level of testing was to expose faults in the interaction between integrated units.

6.4.2.3 System Testing

System testing is a level of the software testing process where a complete, integrated system/software is tested. The purpose of this test was to evaluate the system's compliance with the specified requirements.

6.4.2.4 Acceptance Testing

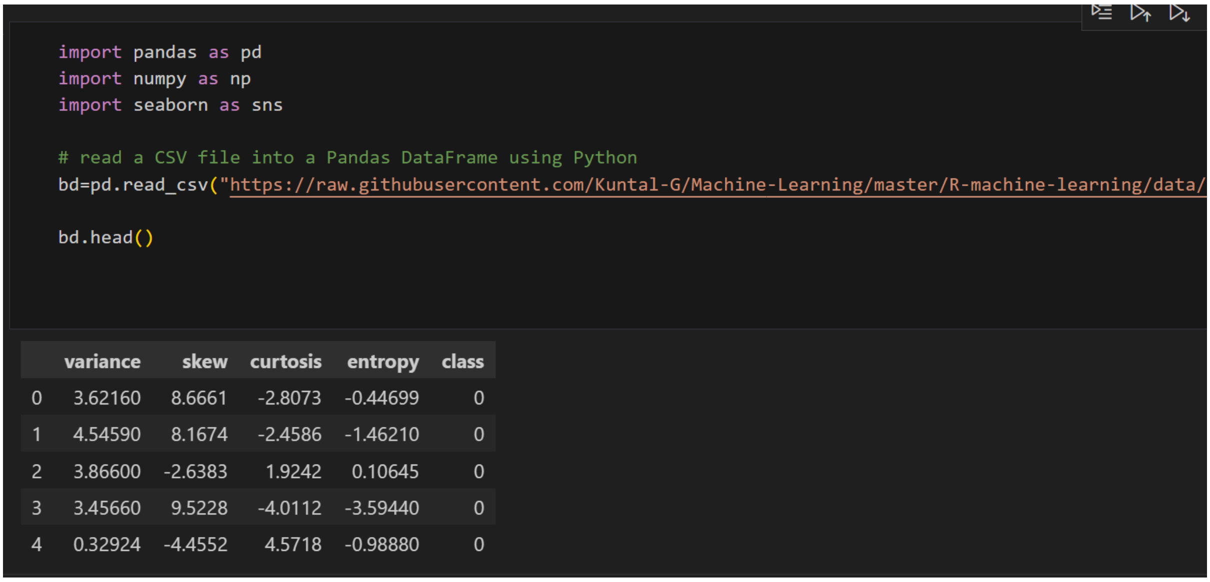
Acceptance testing is a level of the software testing process where a system is tested for acceptability by the users. The purpose of this test was to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.

6.4.2.5 System Interface Design

Jupyter Notebook which is a versatile and interactive web-based application that revolutionizes the way code is written, executed, and shared was used for this particular study. It provided the perfect environment to develop and output results. It's organization into cells, allows users to create documents that seamlessly integrate live code bringing a positive user experience.

6.4.3 Screenshots of the system

Step 1. Importing libraries

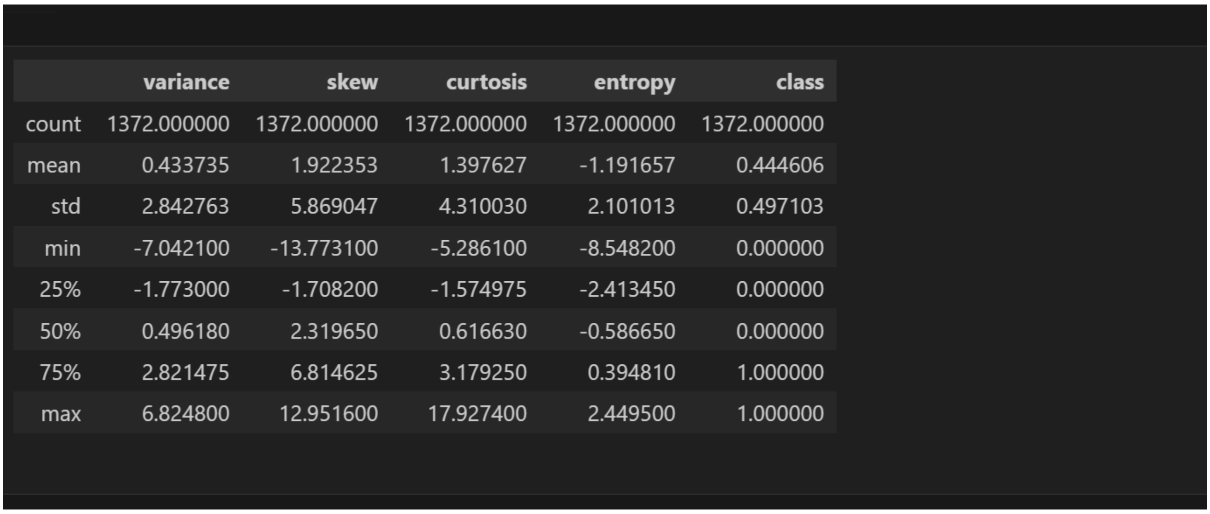


```
import pandas as pd
import numpy as np
import seaborn as sns

# read a CSV file into a Pandas DataFrame using Python
bd=pd.read_csv("https://raw.githubusercontent.com/Kuntal-G/Machine-Learning/master/R-machine-learning/data/

bd.head()
```

	variance	skew	curtosis	entropy	class
0	3.62160	8.6661	-2.8073	-0.44699	0
1	4.54590	8.1674	-2.4586	-1.46210	0
2	3.86600	-2.6383	1.9242	0.10645	0
3	3.45660	9.5228	-4.0112	-3.59440	0
4	0.32924	-4.4552	4.5718	-0.98880	0

Figure 18. Importing libraries

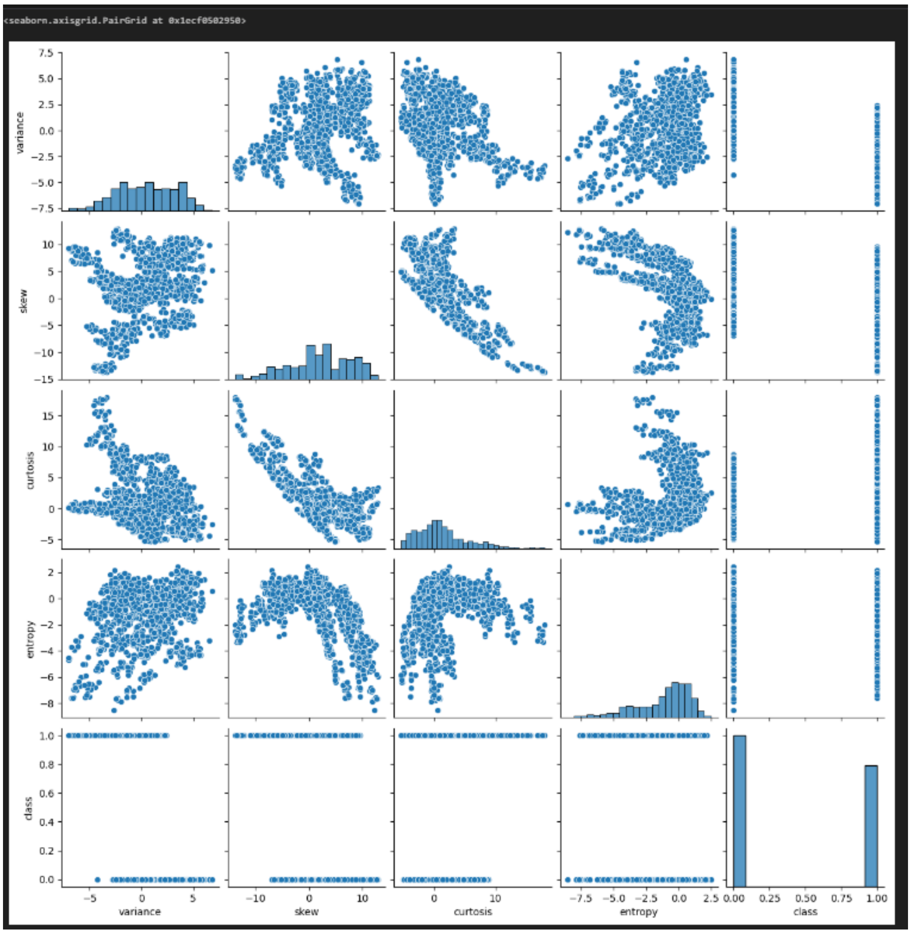
Step 2. Displaying dataset attributes



	variance	skew	curtosis	entropy	class
count	1372.000000	1372.000000	1372.000000	1372.000000	1372.000000
mean	0.433735	1.922353	1.397627	-1.191657	0.444606
std	2.842763	5.869047	4.310030	2.101013	0.497103
min	-7.042100	-13.773100	-5.286100	-8.548200	0.000000
25%	-1.773000	-1.708200	-1.574975	-2.413450	0.000000
50%	0.496180	2.319650	0.616630	-0.586650	0.000000
75%	2.821475	6.814625	3.179250	0.394810	1.000000
max	6.824800	12.951600	17.927400	2.449500	1.000000

Figure 19. Dataset attributes.

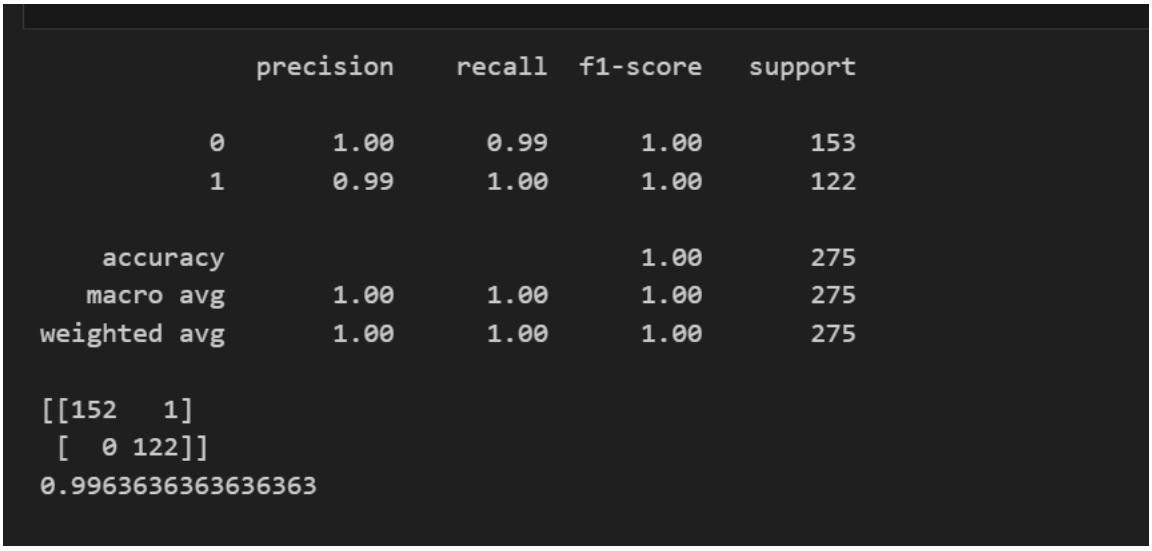
Step 3. Displaying dataset features relationship



```
<seaborn.axisgrid.PairGrid at 0x1ecf0502950>
```

Figure 20. Displaying dataset features relationship.

Step 4. Output prediction



```
              precision    recall  f1-score   support

           0       1.00      0.99      1.00       153
           1       0.99      1.00      1.00       122

    accuracy                           1.00       275
   macro avg       1.00      1.00      1.00       275
weighted avg       1.00      1.00      1.00       275

[[152   1]
 [  0 122]]
0.9963636363636363
```

Figure 21. . Output prediction.

In conclusion, the implementation of a banknote authentication system using machine learning represents a significant stride towards enhancing security measures in financial transactions. Through the utilization of advanced algorithms, such as the Random Forest classifier, this system demonstrates an effective means of distinguishing between genuine and counterfeit banknotes based on distinctive features. The rigorous testing phases, including model testing and system testing, ensure the system's accuracy, robustness, and reliability in real-world scenarios. The incorporation of machine learning not only fortifies the authentication process but also allows for adaptability to evolving counterfeit strategies. As technology continues to evolve, the banknote authentication system serves as a testament to the synergy between machine learning capabilities and the imperative need for secure financial transactions. This system stands poised at the forefront of technological advancements, promising a future where financial integrity is safeguarded through the continuous innovation and refinement of machine learning techniques.

CHAPTER SEVEN

7.0 Conclusion and Recommendations

7.1 Conclusion

This study was conducted with the aim of coming up with a system that could positively authenticate banknotes and classify them as real or fake. We compared three different algorithms to determine which amongst them was the most suitable for solving classification problem. We used Random Forest Algorithm, Logistic regression and Support Vector Machine which are ideal for supervised learning. Suitability is measured by accuracy, recall, f1 score values. The result shows that Random forest at 99.6% accuracy outperforms both Logistic Regression at 98.5% and Support Vector Machine 97.45% after hyper parameter tuning. This results proved that Random forest algorithm was best suited for the purpose of determining whether a banknote was authentic or not.

7.2 Future Scope

The future of a banknote authentication system using machine learning is poised for significant advancements and expanded capabilities. Further improvement will involve integration of a user interface and also it’s usage on ATMs. As technology continues to evolve, the integration of more sophisticated machine learning algorithms and techniques holds promise for further enhancing the system's accuracy and robustness. Future iterations may explore the incorporation of deep learning models, leveraging neural networks to discern intricate patterns and features in banknote data. Additionally, there is potential for the integration of real-time data streams and advanced sensors, allowing the system to adapt dynamically to emerging counterfeit strategies. Collaboration with blockchain technology could also be explored to enhance the security and traceability of authenticated banknotes. Furthermore, advancements in edge computing may enable the deployment of decentralized authentication systems, reducing reliance on centralized servers and bolstering the system's resilience. The future of banknote authentication through machine learning envisions a landscape where innovation and adaptability continuously fortify the security of financial transactions, ensuring the integrity of currency in the face of evolving challenges.

References

1. Davies, G. (2016). A History of Money: From Ancient Times to the Present Day. 4th.
2. Nakamura, C. (2010). The security printing practices of banknotes.
3. Markowitz, M. (2018). Bad Money–Ancient Counterfeiters and Their Fake Coins.
4. Warner, R., & Adams, R. M. (2005). Introduction to security printing, PIA.
5. Levenson, T. (2010). Benjamin Franklin's Greatest Invention.
6. Von Glahn, R. (2006). Re-examining the Authenticity of Song Paper Money Specimens. *Journal of Song-Yuan Studies*, (36), 79-106.
7. R. L. van Renesse, R. L. van Renesse, Ed., “Hidden and scrambled images: A review”, in Proc. SPIE , Apr. 2002, vol. 4677, OpticalSecurity and Counterfeit Deterrence Techniques IV, pp. 333–348.
8. Spencer, C. Paying with Polymer: Developing Canada’s New Bank Notes, Bank of Canada Review, Spring. 2011, pp. 37–45.
9. Available online: https://www.bankofcanada.ca/wp-content/uploads/2011/06/spencer.pdf (accessed on 7 February 2023).
10. Han, T.-H.; Lee, Y.; Choi, M.-R.; Woo, S.; Bae, S.-H.; Hong, B.H.; Ahn, J.-H.; Lee, T.-W. Extremely efficient flexible organic light-emitting diodes with modified graphene anode. Nat. Photon **2012**, 6, 105–110. [CrossRef]
11. White, M.S.; Kaltenbrunner, M.; Głowacki, E.D.; Gutnichenko, K.; Kettlgruber, G.; Graz, I.; Aazou, S.; Ulbricht, C.; Egbe, D.A.M.; Miron, M.C.; et al. Ultrathin, highly flexible and stretchable PLEDs. Nat. Photon **2013**, 7, 811–816. [CrossRef]
12. Kaltenbrunner, M.; Sekitani, T.; Reeder, J.; Yokota, T.; Kuribara, K.; Tokuhara, T.; Drack, M.; Schwödiauer, R.; Graz, I.; Bauer-Gogonea, S.; et al. An ultra-lightweight design for imperceptible plastic electronics. Nature **2013**, 499, 458–463. [CrossRef]
13. International Monetary Fund Bosnia and Herzegovina: Financial Sector Assessment Program-Detailed Assessment of Observance of the CPMI-IOSCO Principles for Financial Market Infrastructures. IMF Staff. Ctry. Rep. **2015**, 15, 1. [CrossRef]
14. Xia, R.; Heliotis, G.; Bradley, D.D.C. Fluorene-based polymer gain media for solid-state laser emission across the full visible spectrum. Appl. Phys. Lett. **2003**, 82, 3599–3601. [CrossRef]
15. Vásquez-Garay, F.; Carrillo-Varela, I.; Vidal, C.; Reyes-Contreras, P.; Faccini, M.; Mendonça, R.T. A Review on the Lignin Biopolymer and Its Integration in the Elaboration of Sustainable Materials. Sustainability **2021**, 13, 2697. [CrossRef]

16. International Monetary Fund Report to the Executive Boards of the IMF and the World Bank on the New CPSS-IOSCO Principles for Financial Market Infrastructures. Policy Pap. **2012**, 2012. [CrossRef]
17. Karnutsch, C.; Pflumm, C.; Heliotis, G.; Demello, J.C.; Bradley, D.D.C.; Wang, J.; Weimann, T.; Haug, V.; Gartner, C.A.; Lemmer, U. Improved organic semiconductor lasers based on a mixed-order distributed feedback resonator design. Appl. Phys. Lett. **2007**, 90, 131104. [CrossRef]
18. Chen, Y.; Herrnsdorf, J.; Guilhabert, B.J.E.; Kanibolotsky, A.L.; Mackintosh, A.R.; Wang, Y.; Pethrick, R.A.; Gu, E.; Turnbull, G.A.; Skabara, P.J.; et al. Laser action in a surface-structured free-standing membrane based on a _-conjugated polymer-composite. Org. Electron. **2011**, 12, 62–69. [CrossRef].
19. 30. Singh, N. Polymer Banknotes—A Viable Alternative to Paper Banknotes. Asia Pac. Bus. Rev. **2008**, 4, 42–50. [CrossRef]
20. 31. Delori, F.C.;Webb, R.H.; Sliney, D.H. Maximum permissible exposures for ocular safety (ANSI 2000), with emphasis on ophthalmic devices. J. Opt. Soc. Am. A **2007**, 24, 1250–1265. [CrossRef]
21. Solomon, D.; Spurling, T. The Plastic Banknote: From Concept to Reality; CSIRO Publishing: Melbourne, VIC, Australia, 2014. Available online https://www.publish.csiro.au/book/6490 (accessed on 7 February 2023).
22. Rogers, J.A.; Someya, T.; Huang, Y. Materials and Mechanics for Stretchable Electronics. Science **2010**, 327, 1603–1607. [CrossRef] [PubMed]
23. Nanto, D. K., & Perl, R. F. (2009). *North Korean counterfeiting of US currency*. Washington, DC: Congressional Research Service.
24. Available online: https://www.royaldutchkusters.com/blog/the-five-pros-and-cons-of-polymer-banknotes (accessed on 8 February 2023).
25. R. L. van Renesse, R. L. van Renesse, Ed., "Hidden and scrambled images: A review", in Proc. SPIE , Apr. 2002, vol. 4677, OpticalSecurity and Counterfeit Deterrence Techniques IV, pp. 333–348.
26. Frankish, K. (2010). Dual-process and dual-system theories of reasoning. *Philosophy Compass*, *5*(10), 914-926.
27. Morewedge, C. K., & Kahneman, D. (2010). Associative processes in intuitive judgment. *Trends in cognitive sciences*, *14*(10), 435-440.
28. Wolfe, J. M., & Van Wert, M. J. (2010). Varying target prevalence reveals two dissociable decision criteria in visual search. *Current biology*, *20*(2), 121-124.

29. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.csc2.ncsu.edu/faculty/healey/download/tvcg.11.pdf

30. Wijntjes, M.W.A., Volcic, R., Pont, S.C. *et al.* Haptic perception disambiguates visual perception of 3D shape. *Exp Brain Res* **193**, 639–644 (2009). https://doi.org/10.1007/s00221-009-1713-9
31. Kandula, M., Hofman, D., & Dijkerman, H. C. (2015). Visuo-tactile interactions are dependent on the predictive value of the visual stimulus. Neuropsychologia, 70, 358e366.
32. Pérez, M., Guinea, S., & Negueruela, J. D. (2014). The Banco de España's cash survey. *Billetaria*, *16*, 6-9.
33. Tsakiris, M., & Haggard, P. (2005). Experimenting with the acting self. *Cognitive Neuropsychology*, *22*(3-4), 387-407.
34. Klatzky, R. L., Lederman, S. J., & Reed, C. (1987). There's more to touch than meets the eye: The salience of object attributes for haptics with and without vision. *Journal of experimental psychology: general*, *116*(4), 356.
35. Snell, J., & Theeuwes, J. (2020). Finding counterfeited banknotes: the roles of vision and touch. *Cognitive Research*, *5*(1).
36. Lederman, S. J., & Klatzky, R. L. (1993). Extracting object properties through haptic exploration. *Acta psychologica*, *84*(1), 29-40.
37. Summers, I. R., Irwin, R. J., & Brady, A. C. (2008). Haptic discrimination of paper. *Human Haptic Perception: Basics and Applications*, 525-535.
38. *Proceedings 25* (pp. 293-308). Springer Berlin Heidelberg.
39. Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008). Good variants of HB+ are hard to find. In *Financial Cryptography and Data Security: 12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008. Revised Selected Papers 12* (pp. 156-170). Springer Berlin Heidelberg.
40. Brands, S., & Chaum, D. (1993, May). Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 344-359). Berlin, Heidelberg: Springer Berlin Heidelberg.

41. Rosi, F., Miliani, C., Delaney, J., Dooley, K., Stringari, L., Subelyte, G., & Buemi, L. P. (2020). Jackson Pollock's Drip Paintings: Tracing the Introduction of Alkyds Through Non-invasive Analysis of Mid-1940s Paintings.
42. Baek, S., Choi, E., Baek, Y., & Lee, C. (2018). Detection of counterfeit banknotes using multispectral images. *Digital Signal Processing*, *78*, 294-304.
43. Pham, T. D., Kim, K. W., Kang, J. S., & Park, K. R. (2017). Banknote recognition based on optimization of discriminative regions by genetic algorithm with one-dimensional visible-light line sensor. *Pattern Recognition*, *72*, 27-43.
44. Lim, H. T., & Murukeshan, V. M. (2017). Hyperspectral imaging of polymer banknotes for building and analysis of spectral library. *Optics and Lasers in Engineering*, *98*, 168-175.
45. Tournié, A., Carré, P., Andraud, C., Boust, C., & Lavédrine, B. (2017). Identification of chromogenic colour photographic print brand by fiber optical reflectance spectroscopy and statistical analysis. *Journal of Cultural Heritage*, *26*, 28-35.
46. Sumriddetchkajorn, S., & Intaravanne, Y. (2008). Hyperspectral imaging-based credit card verifier structure with adaptive learning. *Applied optics*, *47*(35), 6594-6600.
47. Polak, A., Kelman, T., Murray, P., Marshall, S., Stothard, D. J. M., Eastaugh, N., & Eastaugh, F. (2016). Use of infrared hyperspectral imaging as an aid for paint identification. *Journal of Spectral Imaging*, *5*.
48. Kanaev, A. V., Daniel, B. J., Neumann, J. G., Kim, A. M., & Lee, K. R. (2011). Object level HSI-LIDAR data fusion for automated detection of difficult targets. *Optics express*, *19*(21), 20916-20929.
49. Deborah, H., Richard, N., & Hardeberg, J. Y. (2015, August). Hyperspectral crack detection in paintings. In *2015 Colour and Visual Computing Symposium (CVCS)* (pp. 1-6). IEEE.
50. Tian, X., Zhang, W., Chen, Y., Wang, Z., & Ma, J. (2021). Hyperfusion: A computational approach for hyperspectral, multispectral, and panchromatic image fusion. *IEEE Transactions on Geoscience and Remote Sensing*, *60*, 1-16.
51. Grabowski, B., Masarczyk, W., Głomb, P., & Mendys, A. (2018). Automatic pigment identification from hyperspectral data. *Journal of Cultural Heritage*, *31*, 1-12.
52. Silva, C. S., Pimentel, M. F., Honorato, R. S., Pasquini, C., Prats-Montalbán, J. M., & Ferrer, A. (2014). Near infrared hyperspectral imaging for forensic analysis of document forgery. *Analyst*, *139*(20), 5176-5184.

53. Pereira, J. F. Q., Silva, C. S., Braz, A., Pimentel, M. F., Honorato, R. S., Pasquini, C., & Wentzell, P. D. (2017). Projection pursuit and PCA associated with near and middle infrared hyperspectral images to investigate forensic cases of fraudulent documents. *Microchemical Journal*, *130*, 412-419.
54. Khan, Z., Shafait, F., & Mian, A. (2013, August). Hyperspectral imaging for ink mismatch detection. In *2013 12th International Conference on Document Analysis and Recognition* (pp. 877-881). IEEE.
55. Luo, Z., Shafait, F., & Mian, A. (2015, August). Localized forgery detection in hyperspectral document images. In *2015 13th International Conference on Document Analysis and Recognition (ICDAR)* (pp. 496-500). IEEE.
56. Martins, A. R., Dourado, C. S., Talhavini, M., Braz, A., & Braga, J. W. B. (2019). Determination of chronological order of crossed lines of ballpoint pens by hyperspectral image in the visible region and multivariate analysis. *Forensic science international*, *296*, 91-100.
57. Kang, K., & Lee, C. (2016, July). Fake banknote detection using multispectral images. In *2016 7th International Conference on Information, Intelligence, Systems & Applications (IISA)* (pp. 1-3). IEEE.
58. Correia, R. M., Domingos, E., Tosato, F., Aquino, L. F. M., Fontes, A. M., Cao, V. M., ... & Romao, W. (2018). Banknote analysis by portable near infrared spectroscopy. *Forensic Chemistry*, *8*, 57-63.
59. Vila, A., Ferrer, N., Mantecon, J., Breton, D., & Garcia, J. F. (2006). Development of a fast and non-destructive procedure for characterizing and distinguishing original and fake euro notes. *Analytica Chimica Acta*, *559*(2), 257-263.
60. Lim, H. T., & Murukeshan, V. M. (2017). Hyperspectral imaging of polymer banknotes for building and analysis of spectral library. *Optics and Lasers in Engineering*, *98*, 168-175.
61. Prime, E. L., & Solomon, D. H. (2010). Australia's plastic banknotes: fighting counterfeit currency. *Angew. Chem. Int. Ed*, *49*(22), 3726-3736.
62. Yeh, C. Y., Su, W. P., & Lee, S. J. (2011). Employing multiple-kernel support vector machines for counterfeit banknote recognition. *Applied Soft Computing*, *11*(1), 1439-1447.
63. Egeth, H. E., & Yantis, S. (1997). Visual attention: Control, representation, and time course. *Annual review of psychology*, *48*(1), 269-297.

64. Drelie Gelasca, E., Tomasic, D., & Ebrahimi, T. (2005). Which colors best catch your eyes: a subjective study of color saliency. In *Fisrt International Workshop on Video Processing and Quality Metrics for Consumer Electronics, Scottsdale, Arizona, USA* (No. CONF).

65. Wolfe, J., Alvarez, G., Rosenholtz, R., Oliva, A., Torralba, A., Kuzmova, Y., & Uhlenhuth, M. (2008). Search for arbitrary objects in natural scenes is remarkably efficient. *Journal of Vision*, *8*(6), 1103-1103.

66. Lau, J. S. H., & Huang, L. (2010). The prevalence effect is determined by past experience, not future prospects. *Vision research*, *50*(15), 1469-1474.

67. Godwin, H. J., Menneer, T., Riggs, C. A., Taunton, D., Cave, K. R., & Donnel, N. (2016). Understanding the contribution of target repetition and target expectation to the emergence of the prevalence effect in visual search. *Psychonomic Bulletin & Review*, *23*, 809-816.

68. Nocum, D. J., Brennan, P. C., Huang, R. T., & Reed, W. M. (2013). The effect of abnormality-prevalence expectation on naïve observer performance and visual search. *Radiography*, *19*(3), 196-199.

69. Barnes, S. J., & Corbitt, B. (2003). Mobile banking: concept and potential. *International journal of mobile communications*, *1*(3), 273-288.

70. Vyas, G., Gaur, L., & Singh, G. (2016, March). Evolution of payments bank and impact from M-PESA: A case of mobile banking services in India. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (pp. 1-4).

71. Rao, S., & Troshani, I. (2007). A conceptual framework and propositions for the acceptance of mobile services. *Journal of theoretical and applied electronic commerce research*, *2*(2), 61-73.

72. Mas, I., & Kumar, K. (2008). Banking on mobiles: why, how, for whom?. *CGAP Focus note*, (48).

73. Bamoriya, P. S., & Singh, P. (2011). Issues & challenges in mobile banking In India: A customers' perspective. *Research Journal of finance and accounting*, *2*(2), 112-120.

74. Banzal, S. (2010). Mobile banking & M–commerce and related issues. *Retrieved On*.

75. Bach, F. R., Lanckriet, G. R., & Jordan, M. I. (2004, July). Multiple kernel learning, conic duality, and the SMO algorithm. In *Proceedings of the twenty-first international conference on Machine learning* (p. 6).

76. Bach, F. R., Lanckriet, G. R., & Jordan, M. I. (2004, July). Multiple kernel learning, conic duality, and the SMO algorithm. In *Proceedings of the twenty-first international conference on Machine learning* (p. 6).
77. Franc, V., & Sonnenburg, S. (2008, July). Optimized cutting plane algorithm for support vector machines. In *Proceedings of the 25th international conference on Machine learning* (pp. 320-327).
78. Rakotomamonjy, A., & Chanda, S. (2014). ℓp-norm multiple kernel learning with low-rank kernels. *Neurocomputing*, *143*, 68-79.
79. Bi, J., Zhang, T., & Bennett, K. P. (2004, August). Column-generation boosting methods for mixture of kernels. In *Proceedings of the tenth ACM SIGKD*
80. Takeda, F., Nishikage, T., & Omatu, S. (1999). Banknote recognition by means of optimized masks, neural networks and genetic algorithms. *Engineering Applications of Artificial Intelligence*, *12*(2), 175-184.
81. Frosini, A., Gori, M., & Priami, P. (1996). A neural network-based model for paper currency recognition and verification. *IEEE transactions on neural networks*, *7*(6), 1482-1490.
82. He, C., Girolami, M., & Ross, G. (2004). Employing optimized combinations of one-class classifiers for automated currency validation. *Pattern Recognition*, *37*(6), 1085-1096.
83. Ionescu, M., & Ralescu, A. (2005, May). Fuzzy hamming distance based banknote validator. In *The 14th IEEE International Conference on Fuzzy Systems, 2005. FUZZ'05.* (pp. 300-305). IEEE.
84. Chang, C. C., Yu, T. X., & Yen, H. Y. (2007, December). Paper currency verification with support vector machines. In *2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System* (pp. 860-865). IEEE.
85. Chang, C. C., Yu, T. X., & Yen, H. Y. (2007, December). Paper currency verification with support vector machines. In *2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System* (pp. 860-865). IEEE.
86. Sarfraz, M. (2015). An intelligent paper currency recognition system. *Procedia Computer Science*, *65*, 538-545.
87. Gogoi, M., Ali, S. E., & Mukherjee, S. (2015, February). Automatic Indian currency denomination recognition system based on artificial neural network. In *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 553-558). IEEE

88. Grijalva, F., Rodriguez, J. C., Larco, J., & Orozco, L. (2010, September). Smartphone recognition of the US banknotes' denomination, for visually impaired people. In *2010 IEEE ANDESCON* (pp. 1-6). IEEE.
89. Verma, K., Singh, B. K., & Agarwal, A. (2011, December). Indian currency recognition based on texture analysis. In *2011 Nirma University International Conference on Engineering* (pp. 1-5). IEEE.
90. Sarfraza, M. An intelligent system for paper currency recognition.
91. Sargano, A. B., Sarfraz, M., & Haq, N. (2014). An intelligent system for paper currency recognition with robust features. *Journal of Intelligent & Fuzzy Systems*, *27*(4), 1905-1913.
92. Kumar, C., & Dudyala, A. K. (2015, March). Bank note authentication using decision tree rules and machine learning techniques. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 310-314). IEEE.
93. Gai, S., Yang, G., & Wan, M. (2013). Employing quaternion wavelet transform for banknote classification. *Neurocomputing*, *118*, 171-178.
94. Kim, E., & Turton, T. (2014). The next generation banknote project. *RBA Bulletin, March*, 1-11.

95. García-Lamont, F., Cervantes, J., López, A., & Rodríguez, L. (2013). Classification of Mexican paper currency denomination by extracting their discriminative colors. In *Advances in Soft Computing and Its Applications: 12th Mexican International Conference on Artificial Intelligence, MICAI 2013, Mexico City, Mexico, November 24-30, 2013, Proceedings, Part II 12* (pp. 403-412). Springer Berlin Heidelberg.
96. Yoshida, K., Kamruzzaman, M., Jewel, F. A., & Sajal, R. F. (2007, December). Design and implementation of a machine vision based but low cost stand alone system for real time counterfeit Bangladeshi bank notes detection. In *2007 10th international conference on computer and information technology* (pp. 1-5). IEEE.
97. Zeggeye, J. F., & Assabie, Y. (2016). Automatic recognition and counterfeit detection of Ethiopian paper currency. *International Journal of Image, Graphics and Signal Processing*, *8*(2), 28.
98. Giuseppe Schirripa Spagnolo *et al* 2010 *Meas. Sci. Technol.* **21** 107002
99. Paisios, N. (2012). *Mobile accessibility tools for the visually impaired* (Doctoral dissertation, New York University).

100. Toytman, I., & Thambidurai, J. (2011). Banknote recognition on Android platform. *unpublished. Available at: http://www. stanford. edu/class/ee368/Project_11/Reports/Toytman_Thambidurai_Coin_counting_with_Android. pdf.*

101. Sawant, K., & More, C. (2016). Currency recognition using image processing and minimum distance classifier technique. *International Journal of Advanced Engineering Research and Science*, *3*(9), 236826.

102. Rahman, U. U., Sargano, A. B., & Bajwa, U. I. (2017). Android-based verification system for banknotes. *Journal of Imaging*, *3*(4), 54.

103. Kumar, G. R., & Nagamani, K. (2018). Banknote authentication system utilizing deep neural network with PCA and LDA machine learning techniques. *International Journal of Recent Scientific Research*, *9*(12), 30036-30038.

104. Haider, I., Yang, H. J., Lee, G. S., & Kim, S. H. (2023). Robust Human Face Emotion Classification Using Triplet-Loss-Based Deep CNN Features and SVM. *Sensors*, *23*(10), 4770.

105. Doush, I. A., & Sahar, A. B. (2017). Currency recognition using a smartphone: Comparison between color SIFT and gray scale SIFT algorithms. *Journal of King Saud University-Computer and Information Sciences*, *29*(4), 484-492.

106. Yousry, A., Taha, M., & Selim, M. M. (2018). Currency Recognition System for Blind people using ORB Algorithm. *Int. Arab. J. e Technol.*, *5*(1), 34-40.

107. Du, W. D., Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. *The Journal of Strategic Information Systems*, *28*(1), 50-65.

108. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government information quarterly*, *34*(3), 355-364.

109. Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17.

110. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of information management*, *39*, 80-89.

111. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3.

112. Abramova, S., & Böhme, R. (2016). Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study.

113. Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions. In *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016* (pp. 1-14). Springer Publishing Company.

114. Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *arXiv preprint arXiv:1508.04364*.

115. Wörner, D., Von Bomhard, T., Schreier, Y. P., & Bilgeri, D. (2016). The bitcoin ecosystem: Disruption beyond financial services?.

116. Karafiloski, E., & Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017-17th International Conference on Smart Technologies* (pp. 763-768). IEEE.

117. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

118. Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and risks of Blockchain Technologies–a research agenda.

119. Blumberg, B., Cooper, D., & Schindler, P. (2014). *EBOOK: Business research methods*. McGraw Hill.

120. Saunders, M., Lewis, P. H. I. L. I. P., & Thornhill, A. D. R. I. A. N. (2007). Research methods. *Business Students 4th edition Pearson Education Limited, England*, *6*(3), 1-268.

121. Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

122. Adedokun, O. A. (2003). The rights of migrant workers and members of their families: Nigeria. *International migration and multicultural policies section*.