

AUTHENTICATION OF GENUINE AND FAKE CERTIFICATES USING MACHINE LEARNING

ASYIQ SYAHMI BIN AMRAN

AUTHENTICATION OF GENUINE AND FAKE CERTIFICATES USING MACHINE LEARNING

by

ASYIQ SYAHMI BIN AMRAN

Thesis submitted in fulfilment of the requirements

For the Bachelors

Degree of Science (Honours) (Forensic Science)

FEBRUARY 2026

CERTIFICATE

This is to certify that the dissertation entitled

**“AUTHENTICATION OF GENUINE AND FAKE CERTIFICATES USING
MACHINE LEARNING”**

is the bona fide record of research work done by

ASYIQ SYAHMI BIN AMRAN

during the period of October 2025 to February 2026 under my supervision. I have read this dissertation and that is my opinion in it conforms to acceptable standards of scholarly presentation and is gully adequate, in scope and quality, as a dissertation to be submitted in partial fulfilment for the degree of Bachelor of Science (Honours) (Forensic Science).

Main Supervisor,

..  ..

Dr. Chang Kah Haw

Lecturer

School of Health Sciences

Universiti Sains Malaysia

Health Campus

16150 Kubang Kerian Kelantan,

Malaysia.

Date: 29/1/2026

DECLARATION

I hereby declare that this dissertation is my original work, with the exception of citations that are properly acknowledged. I also declare that it has not previously been or simultaneously submitted, in this entirety, for any degrees at Universiti Sains Malaysia or any other institution. I acknowledge that I was assisted by artificial intelligence tools in the preparation of this dissertation. I grant Universiti Sains Malaysia permission to use this dissertation for teaching, research or promotional purposes.

Asyiq Syāhmi Bin Amran

Date: 28 January 2026

ACKNOWLEDGEMENTS

First and foremost, I would like to extend my deepest gratitude to Allah S.W.T for granting me knowledge, strength, and ease throughout the process of completing this project.

I am sincerely grateful to everyone who has supported and guided me during this research journey, whether through physical assistance or heartfelt prayers. My utmost appreciation goes to my supervisor, Dr. Chang Kah Haw, whose generosity in sharing knowledge and patience in supervising me through the project completion. Without his support, this project might not have reached this final stage.

I would also like to thank my fellow research group members for their constructive feedback, insightful suggestions, and continuous encouragement, which greatly improved the quality of this work.

I am profoundly thankful to my beloved family, my parents, Mama and Ayah, as well as Aqeela and Adlyn, for their unwavering love, prayers and moral support. Their sacrifices in all kind of things, encouragement, and belief in me have been the foundation of my perseverance, I am forever indebted. My heartfelt gratitude also goes to my dearest friend that close to my heart, for the constant words of encouragement and emotional support that sustained me during challenging times.

Finally, I wish to acknowledge myself, for the dedication, resilience, and determination invested in completing this thesis.

TABLE OF CONTENTS

CERTIFICATE	II
DECLARATION.....	III
ACKNOWLEDGEMENTS.....	IV
TABLE OF CONTENTS.....	V
ABSTRACT	IX
CHAPTER 1 INTRODUCTION	1
1.1 Overview	1
1.2 Problem Statement	2
1.3 Aim & Objectives.....	3
1.3.1 Aim	3
1.3.2 Objectives	3
1.4 Significance of Study	3
CHAPTER 2 LITERATURE REVIEW	5
2.1 Introduction to Forensic Digital & Forensic Intelligence.....	5
2.2 Digital Evidence & Document Authentication	6
2.3 Traditional Approaches to Certificate Authentication	10
2.4 Machine Learning in Digital Forensics	11
2.5 Application of Random Forest Algorithm.....	14
2.6 Application of Support Vector Machine Algorithm.....	17
2.7 Comparison of Random Forest & Support Vector Machine Algorithms.....	20
CHAPTER 3 METHODOLOGY	22
3.1 Research Methodology	22
3.2 Sample Preparation.....	23
3.2.1 Scanning Original Certificates.....	23
3.2.2 Alteration of Original Certificates	24
3.3 Pre-Processing	27
3.4 Machine Learning Models.....	29
3.4.1 Random Forest.....	29
3.4.2 Support Vector Machine	32
3.5 Data Analysis	35
CHAPTER 4 RESULT & DISCUSSION	37
4.1 Analysis of Feature Variability in Genuine Samples	37
4.1.1 Impact of Scanning Resolution on GLCM Features.....	37
4.1.2 Impact of PDF-to-JPEG Conversion Software.....	41

4.2 Support Vector Machine (SVM) Performance.....	44
4.2.1 Overall Performance Metrics for SVM	44
4.2.2 Confusion Matrix of SVM.....	46
4.3 Random Forest (RF) Performance	50
4.3.1 Overall Performance Using Random Forest.....	50
4.3.2 Confusion Matrix of Random Forest.....	52
4.4 Comparison of RF and SVM Model Performance	54
CHAPTER 5 CONCLUSION, LIMITATIONS AND FUTURE RECOMMENDATIONS.....	56
5.1 Conclusion.....	56
5.2 Limitations and Future Recommendations.....	57
REFERENCES.....	59

LIST OF TABLES

	PAGE
Table 3.1 : 9 Distinct Class Of Forgery Techniques Applied In This Study	26
Table 3.2: Summarized Library Of Random Forest Algorithm.....	32
Table 3.3 : Summarized Library Of Support Vector Machine Algorithm.....	34
Table 3.4: Brief Description Of The Metrics	36
Table 4.1: Kruskal-Wallis Test For The Relationship Between Different Scanning Resolution.....	39
Table 4.2 :Kruskal-Wallis Test For The Relationship Between Asm Value From Different Conversion Method.....	42
Table 4.3 : One-Way Anova Test For The Relationship Between The Glcm Features That Normally Distributed (Contract, Correlation, Idm And Entropy) Value From Different Conversion Method.....	43
Table 4.4 : Comprehensive Performance Metrics For Svm Classification.....	45
Table 4.5 : Overall Performance Metrics For The Rf Algorithm	50

LIST OF FIGURES

	PAGE
Figure 3.1: Flow Chart Of Methodology	22
Figure 3.2: Normal & 9 Distinct Forgery Techniques	27
Figure 4.1 : Confusion Matrix Of Binary Classification Performance Of The Support Vector Machine Algorithm.....	46
Figure 4.2: Confusion Matrix For The Multiclass Classification Of Support Vector Machine Algorithm.....	48
Figure 4.3: Confusion Matrix For The Multiclass Classification Of Random Forest Algorithm.....	52
Figure 4.4: Confusion Matrix For The Multiclass Classification Of Random Forest Algorithm.....	53

AUTHENTICATION OF GENUINE AND FAKE CERTIFICATES USING MACHINE LEARNING

ABSTRACT

The proliferation of fake academic certificates in Malaysia has poses a crucial threat to the integrity of higher education and the credibility of the national workforce. This study was aimed to differentiate genuine and fake academic certificates by analysing their visual textural features through machine learning-based algorithms. In this study, the original physical certificates were digitalised at four scanning resolutions (100 to 400 DPI) and systematically creating 180 fake samples using nine distinct alteration methods using Adobe® Photoshop® software. Textural information was then extracted using the Gray-Level Co-occurrence Matrix (GLCM) while statistical tests were conducted to investigate the influence of the four scanning resolution and effects of different three conversion methods. The results demonstrated that scanning resolution and conversion methods possessed influence in generating the scanned certificates. Both random forest (RF) and support vector machine (SVM) models were effective for binary classification. However, in the multiclass classification of specific forgery types, the RF model outperformed the SVM. Overall, the research underscored the critical role of scanning resolution in shaping textural feature quality and validated the effectiveness of machine learning algorithms in certificate authentication. By demonstrating the feasibility of automated and scalable detection systems, this study contributed to safeguarding institutional integrity and protecting the value of educational qualifications, offering a practical pathway toward strengthening trust in Malaysia's academic and professional landscape.

Keywords: Certificate authentication, machine learning, random forest, support vector machine, GLCM, digital forensics.

CHAPTER 1

INTRODUCTION

1.1 Overview

Certificates are highly significant documents, particularly when an individual seeks to demonstrate their skills and qualifications in a specific field. From primary education to higher levels of study, certificates of recognition play a vital role, not only in motivating individuals to celebrate their achievements, but also in serving as formal proof that a person is qualified for a particular program or discipline. Traditionally, certificates were issued in physical form, printed on durable paper. However, with the advancement of technology and modernization, certificates are now increasingly available in electronic formats. In many application processes, soft copies of certificates must be uploaded online, requiring original certificates to be scanned using appropriate devices or software.

Despite these advancements, there exists a darker side to the widespread use of electronic and scanned certificates. A number of individuals exploit this system by producing counterfeit certificates, either to boast of false achievements or to meet minimum requirements for certain opportunities. The proliferation of fake electronic certificates has become a growing concern, including during the university admissions and other institutional processes.

Screening and verifying electronic certificates are not a straightforward task. The challenge arises from the sheer volume of certificates submitted, often from applicants across the globe. Manual verification is time-consuming and prone to error, making it impractical for large-scale operations. Therefore, with the rapid development of machine learning technologies that continue to simplify human tasks, it is timely to explore their potential in this domain. Machine learning offers powerful capabilities to

detect subtle differences and patterns, enabling automated systems to distinguish between genuine and counterfeit certificates with greater efficiency and reliability.

1.2 Problem Statement

The proliferation of fake academic certificates in Malaysia has emerged as a crucial challenge to the integrity of higher education. Apart from that, it may also potentially provoke the credibility of the nation's workforce. Investigations conducted by professional screening agencies have revealed hundreds of fabricated certificates annually, with a significant proportion involving reputable local universities and, in some cases, non-existent foreign institutions. Such phenomenon not only deceives employers, but also results in the recruitment of unqualified individuals into critical professional roles such as medicine and finance (Ahmad, 2017). Hence, the investigation of the authentication of genuine and fake certificates shall be initiated.

Although the existing legislation including the Private Higher Educational Institutions Act 1996 (Act 555) provides penalties of up to RM200,000 in fines or two years of imprisonment, the enforcement remains limited, with few formal complaints lodged despite widespread reports of falsified qualifications (Bernama, 2025). Furthermore, while centralised verification initiatives such as the Graduate Reference Hub for Employment and Training have been introduced, these systems are not yet comprehensive or universally adopted. This leaves significant gaps in real-time authentication and employer accessibility. The persistence of fake certificates, despite legal provisions and verification platforms, highlights a research gap which is the need for more robust and technology-driven solutions that can provide reliable, scalable and immediate certificate validation (Sardar, 2025).

1.3 Aim & Objectives

1.3.1 Aim

The aim of this research is to differentiate the genuine and fake academic certificates through their visual features using machine learning-based algorithm.

1.3.2 Objectives

The objectives of this study are:

- i. To examine the effects of scanning resolution on the quality of genuine certificates.
- ii. To develop machine learning models for the classification of genuine or fake certificates.
- iii. To classify the different alteration methods in certificate forgery through a developed machine learning model.

1.4 Significance of Study

The authentication of academic certificates is an essential process to verify an individual's qualifications. This is because these types of documents serve as proof of educational acknowledgement and professional credibility. However, the increasing prevalence of counterfeit certificates has become a national issue, with fraudulent documents being used to gain admission to pursue further their education. The current traditional verification methods, which often utilise the manual and physical inspection. Apart from that, institutional cross-checking is also practised and had presented notable disadvantages. These methods are not only time-consuming but also

susceptible to human error and bias. In addition, in many cases, they lack the scalability required to address the growing number of fraudulent attempts. The findings of this study can serve as a foundation to initiate a machine-learning model for differentiating genuine and fake certificates.

In recent years, the application of machine learning algorithm techniques has gained popularity in forensic and document authentication studies. It offers new avenues for improving classification accuracy and reliability. Nevertheless, many existing approaches either depend heavily on complex proprietary systems or require extensive technical expertise, which limits their accessibility and reproducibility. Therefore, this study which explored the potential of machine learning algorithms in the classification and authentication of academic certificates. By incorporating methodological rigor such as feature selection, class balancing, and hyperparameter tuning, this research seeks to enhance the robustness and reproducibility of certificate authentication procedures.

The study also emphasises the broader significance of integrating open-source tools and reproducible workflows into forensic document examination. The findings are expected to provide new insights into the comparative performance of machine learning algorithms, thereby contributing to the academic literature in forensic science. Furthermore, the methodological approaches discussed in this study highlight the potential for scalable and automated systems that can be deployed by educational institutions and professional bodies to safeguard against certificate forgery. Ultimately, this research underscores the role of artificial intelligence in strengthening institutional integrity, ensuring fairness in academic recognition, and protecting the credibility of educational qualifications.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction to Forensic Digital & Forensic Intelligence

Digital forensics is defined as the application of investigation and analysis techniques to gather and preserve evidence from computing devices in a manner suitable for presentation in a court of law (Shah Khan et al., 2025). It is fundamentally a branch of forensic science dedicated to examining digital evidence to extract useful insights for solving cybercrimes, typically aiming to establish what occurred, when it occurred, and the identity of the perpetrator (Helal et al., 2024). The core process involves identifying, acquiring, preserving, analysing, and presenting digital evidence to support investigative activities (Hamed, 2025).

The scope of digital forensics has broadened significantly, moving from its initial focus on standalone computer systems to encompass virtually any device containing a digital processor or storage medium (Vala & Vekariya, 2024). Modern DF encompasses several specialized sub-domains, tailored to different environments and data types (Shah Khan et al., 2025). These branches include disk forensics, which targets storage media like hard drives and flash drives; network forensics, which monitors and analyses volatile computer network traffic for intrusion detection; mobile device forensics, focused on data extraction from smartphones and tablets, (Hamed, 2025) and cloud forensics, necessitated by the growing reliance on third-party cloud computing environments (Hamed, 2025). Other specialised areas include memory forensics, database forensics and multimedia forensics such as analysing audio, video, and image files (Vala & Vekariya, 2024). Meanwhile, forensic intelligence (FI), is the strategic utilisation of forensic data, such as fingerprints, DNA profiles and ballistic information, integrated into a cross-referenced and indexed dataset (Delgado et al.,

2021). Its principal role is to function as an intermediary, bridging the technical analysis conducted by the forensic scientist, who maintains unbiased objectivity with the investigative needs of law enforcement (Delgado et al., 2021). The scope of FI involves embedding an intelligence analyst within the forensic services operation to transform the complex scientific outcomes into actionable intelligence for police investigators. By integrating forensic data early in the investigative cycle with other relevant datasets, FI facilitates a holistic approach for case resolution. This enables law enforcement agencies to identify crime patterns, link seemingly disparate crime scenes and develop proactive strategies to disrupt criminal activities (Delgado et al., 2021).

2.2 Digital Evidence & Document Authentication

The authentication of digital evidence is a cornerstone of modern criminal proceedings, serving to establish the genuine origin and integrity of electronic information from its creation until its presentation in court (Shyshenko, 2025). Unlike traditional physical or paper evidence, digital data exists in a virtual environment where it is highly susceptible to modification, erasure, or transformation during copying and processing. This inherent volatility means that digital traces can often be edited without leaving visible signs of tampering, rendering metadata erasure and file manipulation significant technical risks (Shyshenko, 2025). Consequently, the scientific nature of electronic evidence necessitates a rigorous authentication process to confirm that the data is exactly what it is presented to be and has not been falsified or tampered with. Without such verification, courts may view electronic materials, such as unconfirmed screenshots or files lacking a technical protocol, with substantial doubt regarding their reliability and procedural value.

To ensure the legitimacy of forensic evidence, authentication requires a combination of strict legal adherence and specialised technical expertise. Evidence must be obtained through lawful procedures, such as a signed and dated warrant from a competent authority, and subsequently verified by computer science or information technology experts (Moussa, 2021). These specialists conduct forensic examinations to detect traces of editing, verify the authenticity of data sources, and determine the precise time and geographical parameters of creation. While some jurisdictions currently lack a unified mechanism for this verification, international standards such as ISO/IEC 27037:2012 advocate for the use of digital hash identifiers and secure protocols to maintain the immutability of the original data structure. Ultimately, the criminal judge relies on these expert assessments to form a conviction, as the complexity of digital structures demands scientific logic to confirm that the evidence remains intact and unquestionable throughout the investigative chain (Moussa, 2021) .

The proliferation of digital document exchange has necessitated the development of robust forensic authentication to counter the growing efficacy of powerful image-altering software and sophisticated digital printers (Shinde et al., 2022). Digital image forensics serves as a scientific field dedicated to identifying, analysing and interpreting quantitative proof regarding the authenticity and source of electronic files. Forensic investigators primarily target three distinct forms of tampering, namely the addition of new text, the alteration of existing content, and the erasure of information intended to be concealed (Boonkrong, 2025). Such illegal manipulations are frequently observed in the falsification of real estate agreements, travel documents and academic credentials, where individuals attempt to gain unlawful employment or bypass security measures. Consequently, document forensics is

essential across various criminal investigations to establish the scientific logic and determine whether a piece of evidence is genuine or fabricated.

Authenticating these documents involves both active and passive detection techniques, ranging from traditional digital watermarking and signatures to blind analysis of binary information without prior knowledge (Shinde et al., 2022). Modern methodologies frequently utilise image processing techniques such as the convolutional neural network (CNN) and discrete cosine transform (DCT) to extract identifying features and detect inconsistencies in character texture or ink response. A CNN is a deep feed-forward multi-layered hierarchical network inspired by the biological receptive field mechanism (Li et al., 2020). As a representative algorithm in deep learning, it achieves "end-to-end" learning by automatically transforming raw data into high-level feature representations through multiple layers of transformation (Li et al., 2020).

The standard architecture consists of an input layer, alternate layers of convolution and pooling, as well as one or more fully connected layers followed by an output layer (Zhao et al., 2024). Convolution layers are pivotal for feature extraction, while pooling layers are used to reduce data redundancy and parameters while maintaining useful information. These networks possess distinctive advantages such as local connections, weight sharing and dimensionality reduction, which allow for more efficient training compared to traditional fully connected networks (Li et al., 2020). CNNs have enabled significant breakthroughs in computer vision, including face recognition, autonomous vehicles and intelligent medical treatment. Beyond two-dimensional images, they are also applied to one-dimensional data for functions such as signal identification and time-series prediction (Li et al., 2020).

Meanwhile, the DCT is a mathematical transformation that decomposes an input signal into a weighted sum of basis cosine sequences (Oleiwi et al., 2021). It is a cornerstone of digital image processing, primarily valued for its exceptional energy compaction property, which allows it to remove redundancy between neighbouring pixels (Oleiwi et al., 2021). The function enables DCT to compact the energy of a signal into small indexed frequencies, making it highly technically powerful for image compression standards like JPEG. Because each DCT coefficient can be processed independently due to its de-correlated properties, it is extensively used in systems requiring high accuracy, such as health diagnoses and information security. In digital image forensics, DCT is specifically applied to detect and localise copy-move forgeries by evaluating overlapping pixel blocks to identify duplicated regions (Shehin & Sankar, 2024). To address its high computational complexity, researchers have developed fast DCT (FDCT) algorithms that significantly reduce processing time for practical network applications (Oleiwi et al., 2021).

Furthermore, cryptographic hash functions are increasingly employed to ensure data integrity through the properties of one-way computation and collision resistance, allowing verifiers to detect unauthorised modification by comparing resultant hash values against stored originals. Despite these advancements, significant challenges persist in the field, including high computational complexity, the difficulty of processing low-quality or noisy images, and the necessity of accessing original document references for certain verification protocols to be effective (Shinde et al., 2022).

2.3 Traditional Approaches to Certificate Authentication

Historically, the authentication of documents was primarily centred on the examination of handwriting, a practice dating back to the Roman Empire where expert testimony was first utilised. Early methodologies relied heavily on witness testimony, circumstantial evidence, and the insights of "recognition witnesses". Individuals who were personally acquainted with the alleged author's script and could provide evidence based on that familiarity (Devlin et al., 2024). The traditional approach evolved through the 20th century as judges and juries often conducted their own manual comparisons in conjunction with testimony, eventually leading to the emergence of the formalised expert witness roles recognised today (Devlin et al., 2024).

The technical framework for traditional authentication was significantly broadened by pioneers, namely Albert S. Osborn, who expanded investigative parameters beyond handwriting to include the analysis of typewriting, ink and paper. Such traditional mandate involves the scientific identification of alterations, deletions, substitutions and the detection of counterfeits through rigorous visual inspections (Devlin et al., 2024). Common practices include examining documents under white light and ultraviolet (UV) light to assess physical characteristics, such as printing methods, serial numbers, and the presence of embedded security features like watermarks or microprinting. These "simpler" traditional examinations are often sufficient, as only a small number of fraudulent documents require highly sensitive or resource-intensive instrumental techniques for detection.

In a procedural sense, traditional certificate authentication operates predominantly within a judicial paradigm, focusing on case-by-case resolutions to provide evidence for legal proceedings. This approach is characterised as being largely reactive, as its primary objective is to establish whether a document is genuine or

fraudulent to facilitate action against a specific individual holder. Consequently, traditional methods tend to focus on establishing the source or authenticity of a single item, often underutilising the broader information contained within the traces once a document has been identified as a forgery (Devlin et al., 2024).

2.4 Machine Learning in Digital Forensics

The integration of machine learning into forensic science represents a transformative shift, providing a branch of data science capable of improving the speed, efficiency and reliability of complex decision-making (Richmond, 2020). Forensic applications of these technologies are remarkably diverse, spanning digital forensics, biometric identification, forensic pathology, chemometrics and crime scene analysis (Kassem & Lodhi, 2024). Within the digital realm, machine learning systems are utilised to filter evidence from vast media repositories, perform visual analyses of satellite data to detect settlement destruction, and conduct textual analyses of judicial reporting datasets. Furthermore, specialised frameworks such as IoTdots have been developed to scan application source code for forensic information, while tools like VERITAS automatically collect and extract evidence from the heterogeneous and distributed environments of the Internet of Things (Tageldin & Venter, 2023) .

IoTdots and VERITAS are advanced analytical frameworks designed to enhance security, accountability and transparency within smart environments and digital media, respectively. IoTdots serves as a digital forensic framework for smart settings, comprising the IoTdots-Modifier which automatically inserts tracing logs into the source code of smart applications at compile time, as well as the IoTdots-Analyser which utilises machine learning and data processing to extract forensic

evidence from device activities (Babun et al., 2018). In contrast, VERITAS is a framework dedicated to verifying the "realness" of images. It specifically analyses small and low-resolution files by identifying AI-generated content and providing human-readable explanations through artifact localisation and semantic reasoning (Srivastava et al., 2025). While IoT Dots focuses on identifying security policy violations and holding individuals or applications accountable within a physical IoT ecosystem, VERITAS seeks to improve trust in digital platforms by using vision-language models to describe the specific synthetic anomalies that justify an image's classification as artificial (Babun et al., 2018).

Beyond data management, machine learning facilitates highly technical forensic tasks that previously relied on manual and subjective expertise. In biometric identification, algorithms have revolutionised facial recognition, fingerprint analysis, and voice verification by surpassing the accuracy and speed of traditional human-led methods (Kassem & Lodhi, 2024). Forensic pathology has also seen significant advancements through the use of Natural Language Processing for autopsy reporting and the implementation of virtual autopsies, which utilise imaging technologies like Magnetic Resonance Imaging (MRI) and Computed Tomography (CT) scans to create non-invasive 3D reconstructions. Additionally, machine learning is employed in the automated interpretation of complex DNA profiles, such as degraded or mixed samples, through probabilistic genotyping software. These systems assist investigators in handling "low template" DNA that would otherwise be difficult to interpret through traditional manual deconvolution (Richmond, 2020).

The primary advantage of machine learning in forensics lies in its sophisticated pattern recognition capabilities, which allow systems to learn from historical data to predict future criminal behaviour or identify the source of evidence (Tageldin &

Venter, 2023). For instance, supervised learning models are trained on labelled datasets to recognise the unique minutiae points of fingerprints or the specific inflections in a human voice. In crime scene reconstruction, algorithms analyse the size and distribution of bloodstain patterns or the microscopic markings on bullet casings to match firearms with high precision. Moreover, these technologies enable predictive policing by identifying crime hotspots and potential criminal trajectories, such as forecasting the flight pathways of compromised drones. This ability to disaggregate complex tasks into intelligible sub-tasks through neural networks mimics human logic while operating at a scale that is fundamentally inaccessible to human investigators (Richmond, 2020).

In addition to pattern recognition, machine learning provides critical advantages for anomaly detection, particularly in safeguarding smart environments against sophisticated cyber threats (Richmond, 2020). AI systems involve massive volumes of network logs to detect unusual outbound traffic or unauthorised access requests that indicate a data breach. Intelligent intrusion detection systems utilise machine-to-machine frameworks to discover simple and complex attacks early in the data transmission process, which is essential for protecting resource-constrained IoT devices. By automating the prioritisation of suspicious file artefacts and identifying data-scavenging attacks via blockchain-assisted shared audit frameworks, these technologies significantly reduce the workload on human analysts (Kassem & Lodhi, 2024). Ultimately, while challenges such as algorithmic opacity and bias remain, the use of machine learning enhances the pursuit of justice by providing more objective, data-driven insights into the root causes of digital and physical crimes (Kassem & Lodhi, 2024).

2.5 Application of Random Forest Algorithm

The Random Forest (RF) algorithm represents a robust and versatile cornerstone of modern machine learning, serving as an ensemble model extensively utilised for both classification and forecasting tasks (Salman et al., 2024). At its core, it operates as a collection of tree-structured classifiers, where each individual tree is generated based on random vectors that are independently and identically distributed (Fei et al., 2022). By aggregating the outcomes of numerous decision trees, the model goes beyond the limitations of a single predictive path, culminating in a result that is significantly more accurate and stable than its constituent parts (Salman et al., 2024). This approach has earned substantial recognition in the field of data mining due to its high accuracy and its supervised learning capabilities (Salman et al., 2024).

The architectural elegance of a RF model is found in its training mechanism, primarily through a technique known as bootstrap aggregation or "bagging" (Salman et al., 2024). During the process, the model constructs a multitude of decision trees. Each trained on a unique, randomly chosen subset of the original training data. By incorporating such randomness, the algorithm effectively "decorrelates" the individual trees, which mitigates the risk of overfitting and allows the model to generalise far better to novel and unseen data. While the number of trees is a critical parameter often set to values such as 100 or 500, the model remains remarkably resilient and does not require overly complex parameter modulation to achieve high precision (Salman et al., 2024).

One of the most profound features of the RF is its innate ability to perform feature selection and evaluate variable importance (Salman et al., 2024). Using embedded methods such as the Gini index or out-of-bag (OOB) error rates, the algorithm can quantitatively rank the contribution of each feature during the training

process (Fei et al., 2022). Unlike some alternative models that might struggle with high-dimensional data, a RF chooses the optimal split at each node from a random subset of predictors, ensuring that even variables with lesser impacts are evaluated fairly. This allows researchers to manage thousands of input variables without the premature need for data deletion, effectively identifying crucial characteristics within complex datasets (Salman et al., 2024).

The prediction process in a Random Forest varies slightly depending on whether the task is categorical or continuous in nature. For classification, the model employs a "majority-voting" procedure where each tree casts a single vote for its predicted class, and the class with the most votes become the final output (Salman et al., 2024). Conversely, for regression tasks, the algorithm averages the individual predictions of all trees to derive a final value. This collective decision-making process functions, even if one tree makes an error, ensures that the final prediction remains reliable and less susceptible to the biases of a single viewpoint (Salman et al., 2024).

The strengths of the RF are particularly evident in its handling of massive and complex databases. It is widely regarded as one of the most efficient techniques in machine learning because it can process large amounts of data while maintaining a relatively fast training speed. In comparative studies, RF often demonstrates higher accuracy and better stability than traditional models like support vector machines (SVM) or artificial neural networks (ANN), especially in land-cover and species classification (Fei et al., 2022). Its ability in providing a built-in estimate of generalisation error further enhances its utility for production managers and scientific researchers alike.

Beyond speed, the model excels at overcoming common data-related challenges, such as imbalanced datasets and missing values. RF provides internal algorithms to impute missing data based on proximity matrices, ensuring that the integrity of the analysis is maintained even when information is incomplete (Salman et al., 2024). Furthermore, it is notably immune to outliers and distributive errors that might otherwise impact parametric models, as outliers generally do not influence the fundamental division of data within the trees. This durability makes it a preferred choice for noisy and real-world data across various industries (Salman et al., 2024).

In the context of binary classification, the suitability of Random Forest has been proven in highly sensitive fields such as cybersecurity (Li et al., 2021). Li et al. recognize that while X.509 certificates were designed to protect users, they were increasingly exploited by attackers in phishing websites and malware communications. To address this, they designed a system called Verification for Extraction (VFE), which systematically analysed certificates, extracted detailed features such as issuer information, chain validation and cryptographic attributes, and then applied machine learning models. This includes Random Forest, Support Vector Machine, ensemble methods, and deep learning. All algorithms were used to classify certificates as authentic or malicious. Their experiments demonstrated that the ensemble learning model was highly stable, while SVM achieved the highest accuracy at 98.2%, proving that machine learning could reliably distinguish fraudulent certificates from legitimate ones.

Machine learning algorithm could be exceptionally well-suited for multi-classification tasks, even where the relationships between categories are complex. In agricultural remote sensing, RF algorithm has been used to map various crops like cotton, rice and fruit trees with high precision when integrating spectral and texture

features (Fei et al., 2022). Similarly, in archaeological research, RF has effectively distinguished between different types of lithic use-wear traces, such as those from butchering, wood or shell contact, based on two-dimensional image texture analysis. By providing a bridge between qualitative description and quantitative data, RF enables a more standardised and objective understanding of diverse and multi-layered phenomena (Sferrazza, 2023).

2.6 Application of Support Vector Machine Algorithm

Support Vector Machine (SVM) represents a robust category of supervised machine learning algorithms, primarily utilised for classification and regression tasks (Liu et al., 2021). Introduced by Cortes and Vapnik in 1995 for binary classification, the algorithm operates by identifying a discriminant hyperplane that effectively separates data points into distinct categories (Dakhaz & Adnan, 2021). The fundamental goal is to locate the specific hyperplane that maintains the maximum margin or distance between the classes, as a larger margin typically ensures superior generalisation and accuracy when processing unseen data. To handle complex datasets where classes cannot be linearly separated in their original state, SVMs employ various kernel functions, such as polynomial or radial basis functions (Abdullah & Abdulazeez, 2021). These functions project the training data into a higher-dimensional feature space, making it significantly easier to define a linear separator. The selection of an appropriate kernel is vital, as the density of kernel directly influences the smoothness and overall performance of the resulting classifier (Dakhaz & Adnan, 2021).

The versatility of SVMs has led to their widespread application across numerous professional domains, notably in medical diagnostics and digital security.

In the healthcare sector, SVM classifiers contribute to the rapid and reliable identification of diseases, such as detecting cancer cells in medical imaging or identifying cataracts in fundus images. Simultaneously, the algorithm is pivotal in the realm of information security, where it is used to develop intrusion detection systems that track and prevent network attacks by distinguishing between normal and abnormal traffic patterns (Dakhaz & Adnan, 2021).

Beyond medicine and security, SVMs serve essential functions in document verification and specialised research (Sferrazza, 2023). They are highly effective in detecting document forgeries by analysing RGB colour channels and texture descriptors to differentiate between genuine and manipulated text (Gornale et al., 2022). The methodology employed by Gornale et al. (2022) to detect document forgery centres on a sophisticated integration of RGB colour channel analysis, texture descriptors, and multi-class support vector machine (MC-SVM) model. The process begins with a pre-processing stage where the input colour images, which may be either handwritten or printed, are resized to a standard 100 x 100 pixels to facilitate uniform analysis (Gornale et al., 2022). To identify minute local variations and discrepancies caused by forgery operations like insertion or copy-pasting, the system decomposes each image into its constituent red (R), green (G) and blue (B) colour components. The channel separation was critical because the intensity of inks could be non-uniform and affected by external factors like pen pressure or paper quality, which could be more easily scrutinised when viewed through individual colour layers (Gornale et al., 2022).

One of the most significant advantages of SVMs is their ability to achieve high classification accuracy, often reaching state-of-the-art levels in fields like face and character recognition (Liu et.al, 2020). Unlike many other machine learning methods, SVMs generalised remarkably well even when provided with minimal training data

and are inherently robust against the problem of overfitting. Additionally, they were exceptionally capable of solving non-linear and high-dimensional problems, offering a shorter prediction time once the global optimal solution was established (Dakhaz & Adnan, 2021).

However, the implementation of SVMs is not without its challenges, particularly regarding computational resources and model selection. As the size of the database increases, the time and space complexity of the algorithm tends to grow linearly, which can be taxing when processing large-scale data. Furthermore, the performance of the model is heavily dependent on the user's ability to select the correct kernel function, a process that is both crucial and demanding (Dakhaz & Adnan, 2021). Traditional single-objective models also frequently overlook the varying costs associated with different types of misclassifications, such as the severe implications of medical misdiagnosis (Liu et al., 2021).

While the original SVM was designed for binary problems, it has been extended to multi-class scenarios through methods such as one-against-one (OAO) and one-against-all (OAA). OAO is generally considered more suitable as it constructs multiple classifiers to compare class pairs, whereas OAA can suffer from imbalances in data quantities. To enhance reliability and efficiency, researchers have introduced advanced models like the projected multi-objective SVM, which addresses the training bottlenecks of traditional multi-class methods (Liu et al., 2021). By providing a wider set of options for various misclassifications and guaranteeing pareto-optimal solutions, these refined multi-class approaches ensure higher out-of-sample quality and greater flexibility for decision-makers.

2.7 Comparison of Random Forest & Support Vector Machine Algorithms

The SVM and RF are both high-performance, non-parametric machine learning algorithms widely used for complex classification tasks, yet they operate on fundamentally different mathematical principles. SVM is a kernel-based algorithm that seeks to solve a convex quadratic optimization problem to find a globally optimal hyperplane that maximizes the margin between different classes (Sheykhmousa et al., 2020). In contrast, RF is an ensemble learning method that constructs a multitude of individual decision trees and aggregates their results through a majority-voting process to produce a final classification (Salman et al., 2024). While SVM is inherently a binary classifier that requires specific strategies like "one-against-one" to handle multiple categories, Random Forest naturally accommodates multiclass problems without requiring architectural modifications (Sheykhmousa et al., 2020).

A significant distinction between the two models lies in their sensitivity to parameter configuration and overall ease of use. RF is celebrated for its stability and relative insensitivity to hyperparameter modulation, often producing high accuracy even without extensive tuning (Lachaud et al., 2023). Conversely, the performance of an SVM model is heavily dependent on the appropriate selection of a kernel function, either as linear, polynomial, or radial basis function (RBF), as well as the precise adjustment of parameters like the penalty term (C) and the kernel coefficient (gamma). Because the mathematics behind SVM can be quite complex, it is sometimes considered less accessible for non-expert users compared to the more intuitive decision-making process of a Random Forest (Sheykhmousa et al., 2020).

In terms of stability and robustness, RF often exhibits superior resistance to common data challenges like noise and overfitting. This durability is attributed to its use of bagging and random feature selection at each node split, which decorrelates the

individual trees and enhances the model's ability to generalise to new datasets (Salman et al., 2024). While SVM is highly effective at managing high-dimensional data and can work well with small training sets, it is more susceptible to overfitting if the dataset is too limited or if a complex kernel is applied without sufficient regularisation. For instance, comparative studies in mineral mapping have shown that while SVM might achieve higher accuracy on training data, RF remains more stable and provides better predictive success rates when training data is limited (Lachaud et al., 2023).

Finally, the two algorithms differ remarkably in their computational efficiency and interpretability. RF is generally faster to train and can process thousands of input variables efficiently without the need for premature data deletion (Salman et al., 2024). It also provides high interpretability through built-in mechanisms that rank variable importance, allowing researchers to understand which features contribute most to the model's decisions. SVM, however, can be computationally expensive and resource-intensive when dealing with massive datasets or iterative optimisation processes (Sheykhmousa et al., 2020). Furthermore, SVM is often characterised as a "black box" technique because it does not inherently provide information regarding the relative role or significance of individual features in the final predictive model (Lachaud et al., 2023). In this study, these two models were compared and investigated for their respective performances in differentiating genuine and fake certificates.

CHAPTER 3

METHODOLOGY

3.1 Research Methodology

The sample preparation process in this study involved a structured sequence of steps designed to generate both authentic and fake certificate images for forensic analysis. The overview of the methodology as in Figure 3.1.

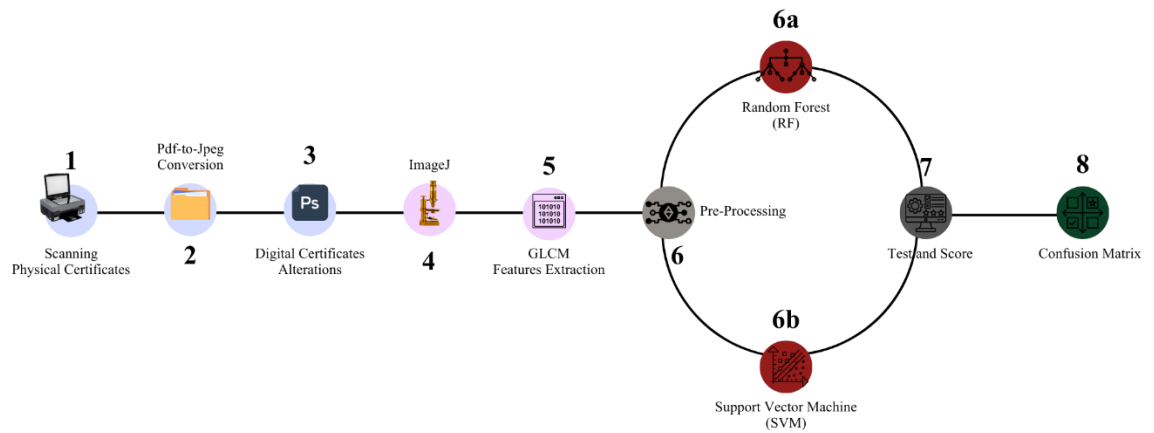


Figure 3.1: Flow Chart of Methodology

In this study, several variables were established to structure the research design. The dependent variables were defined by two controlled components, namely the authenticity of the certificate, which was categorized as either genuine or fake using Adobe Photoshop and the scanning resolution applied during the digitization process. Additionally, the manipulated variable was represented by the nine forgery types that were systematically introduced to assess the robustness of the detection framework, also serving as the dependent variables, with an aim to distinguish among the forgery types. The dependent variables encompassed the extracted gray-level co-occurrence matrix (GLCM) texture features. With that, the performance outcomes of the machine learning classifiers were evaluated through standard performance metrics. This

arrangement ensured that the study could effectively examine how variations in certificate authenticity, scanning resolution, and forgery type influence both the texture-based feature extraction process and the accuracy of classification models in distinguishing between genuine and fake certificates.

3.2 Sample Preparation

The preparation of certificates samples was a critical stage in ensuring the reliability and validity of the GLCM feature and algorithm analysis. In the sample preparation, it started with scanning physical certificates and ended with original certificate images alteration by using selected software.

3.2.1 Scanning Original Certificates

The original certificates were first scanned using a Canon ImageCLASS MF3010 scanner (Canon Inc, Tokyo, Japan) at four different resolutions, namely 100, 200, 300 and 400 dots per inch (dpi). This step was crucial to ensure that the digital copies captured varying levels of detail and clarity, which could later be used for comparative analysis. Each scanned file was saved in portable document format (PDF) and systematically stored in a designated folder on the computer to maintain proper organisation and accessibility for subsequent stages of the methodology. By preserving the certificates in PDF format, the integrity of the scanned images was retained while providing a standardised file type for further processing.

3.2.3 Conversion of Original Portable Document Format (PDF) into Joint Photographic Experts Group (JPEG)

Following the scanning process, the PDF files were converted into joint photographic expert group (JPEG) format using three different software applications, including Adobe® Acrobat®, Adobe® Photoshop®, and Adobe® Illustrator® (Adobe, 2026). The conversion was necessary because the ImageJ software employed in the subsequent analysis was only capable of processing JPEG files for pixel-based evaluation. Utilising multiple software ensured that the conversion process was consistent and reliable, while also allowing for the detection of any potential discrepancies in image quality across different platforms. This step effectively prepared the certificates for pixel analysis by transforming them into a format compatible with the analytical tools used in the study.

3.2.2 Alteration of Original Certificates

The alteration of the original certificates was carried out using Adobe® Photoshop®, focusing specifically on the 300 dpi resolution files to maintain a balance between image clarity and processing efficiency. Nine distinct alteration methods were applied, each designed to simulate realistic forgery techniques that could occur in practice. The first method involved copying the background, applying blur, and then adding new elements to the certificate. This approach was intended to disguise modifications by softening the edges of inserted content, thereby creating a seamless blend with the original document.

The second method utilised content-aware fill combined with insertion, where portions of the certificate were intelligently filled to remove original details before new elements such as names or logos were inserted. This technique allowed for