Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 1, March, 2026, pp. 295-307
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 133

A Review of Anti-Forgery Technologies for Official Identification Documents: Trends, Challenges, and Future Directions

Ibrahim F. Mohamed[1], Tayseer S. Atia[2]
[1]Department of computer engineering, AL-Iraqia University, Baghdad, Iraq
[21]Department of computer engineering, AL-Iraqia University, Baghdad, Iraq

Article Info

Article history:

Received Dec., 17, 2025
Revised Jan., 10, 2026
Accepted Mar., 12, 2026

Keywords:

Identification Document Security
Multi-Layer Authentication
QR code Security
Elliptic Curve Cryptography (ECC)
Physical-Digital Security Integration

ABSTRACT

Over the last two years, advancements in the security of physical government-issued identity documents against forgery have been made through three key research areas: the use of deep learning to detect forgeries, the development of cryptographic verification systems, and improvements in the security of QR codes. While advances have been made in these three areas, the vast majority of these developments happen independently of each other and create a significant vulnerability to hybrid attacks that use the disconnect between paper-based and electronic security features. This paper highlights a missing component to establish a comprehensive solution that would combine tamper-evident physical security features (such as Guilloche patterns) with powerful electronic mechanisms (like elliptic curve cryptography and desirable secure data storage methods, such as QR Codes). The authors suggest that research should focus on developing unified multilayered security systems that support the principles of scalability, interoperability, and usability so that we can effectively combat the growing threat of sophisticated and frequent forgeries and, in turn, restore trust in both electronic and physical forms of identification.

Corresponding Author:

Ibrahim F. Mohamed
Department of Computer Engineering, AL-Iraqia University
Almasafi street, Baghdad, Iraq
Email: ibrahim.f.mohamed@aliraqia.edu.iq

1. INTRODUCTION

Maintaining the integrity of legal identification documents is a crucial component of the operation of our society through Law Enforcement, Border Security, Financial Services, Healthcare, and Academia. Legal identification documents such as national identification cards, passports, driver's licenses and academic certificates provide a connecting point between an individual's real-world (i.e. physical) identity and an individual's digital identity. Legal identification documents also empower individuals with access to certain rights, benefits, and services [1]. On the downside, the value of Documents of Legal Identification Documents has made them a prime target for forgery, and with technology advancing the techniques used to create counterfeit Documents of Legal Identification Documents, counterfeiters will continue to develop increasingly sophisticated ways to create more realistic, less visible, and harder-to-detect forgeries in an ongoing battle of technologies.

The threat landscape is diverse and includes many attacks against the various layers of document security. Forged documents can be created by replicating or altering the physical aspects of a document. New technology, including high-resolution scanners and advanced graphics programs, now allow forgeries to closely match the complex security features of a document, such as guilloches and micro-printing [2]. Many forgery techniques make use of photo substitutes, altering data, and adding holographic overlays, which exploit human optical capabilities [3]. Digital tampering typically focuses on manipulating and altering the digital data that is embedded into a document and its machine-readable components, such as QR codes and bar codes. The tampering of digital files can be accomplished in many ways, such as creating copies of QR codes or bar codes and changing the content of the code digitally, or bypassing the security measure(s), which are designed to maintain the security and/or authenticity of QR codes and bar codes.[4] In Hybrid Attacks (physical changes to documents that impact a document's digital

image), it represents a very serious threat to the trustworthiness and veracity of digital files, where there is a chance the document may pass both a human and machine verification process [5]. In response, the document security industry has developed a double-pronged countermeasure strategy designed to counteract the different types of attacks. The use of specialized designs makes it difficult for someone to reproduce physical security features without access to specialized knowledge and equipment. Examples of these designs are intricate guilloche patterns, which create a moiré effect when copied; colour-shifting ink; holographic images; and micro text [6]. These designs represent the key strength of giving people immediate visual evidence of tampering. Digital security features leverage cryptography and IT to protect the data contained in the document, as well as the authenticity and integrity of that data. The use of a cryptographic hash function, such as SHA-256, allows anyone who alters the data in a document to detect tampering [7]. Digital signature algorithms, particularly those based on Elliptic Curve Cryptography (ECC), such as ECDSA, provide a means to verify the issuing authority and ensure the data has not been modified since it was signed [8]. Furthermore, All PDF versions of documents contain a source document containing the digital signature and thus provide an environment in which their contents are safe. However, the use of QR codes has enabled the storage of this signed/encrypted data in a fast way (machine-readable) [9], allowing easy machine verification of signed/encrypted documents. Despite these developments, significant vulnerabilities remain between the physical layer and the digital layer. Most currently employed security systems consider the physical and digital layers as separate silos. Therefore, even if a document has a strong digital signature, it could still be successfully forged as long as the QR code on the original document is replicated. As such, the digital verification process would succeed and fail to recognize the physical forgery [10]. A security solution that relies only on the visual assessment of the physical characteristics of the document is also compromised, as high-quality reproductions will pass the visual inspection test and offer no protection against alteration of the digital data. The disparate security approaches create opportunities for sophisticated adversaries to exploit. The costs of these security failures extend far beyond dollars alone. By 2025, it is estimated that cybercrime associated with identity fraud and document forgery will cost the world economy $10.5 trillion USD annually [11], as shown in Figure 1.1. This real-world example highlights the need to move away from isolated security solutions, which provide a fragmented security architecture, to a unified and multi-layered security architecture [12].

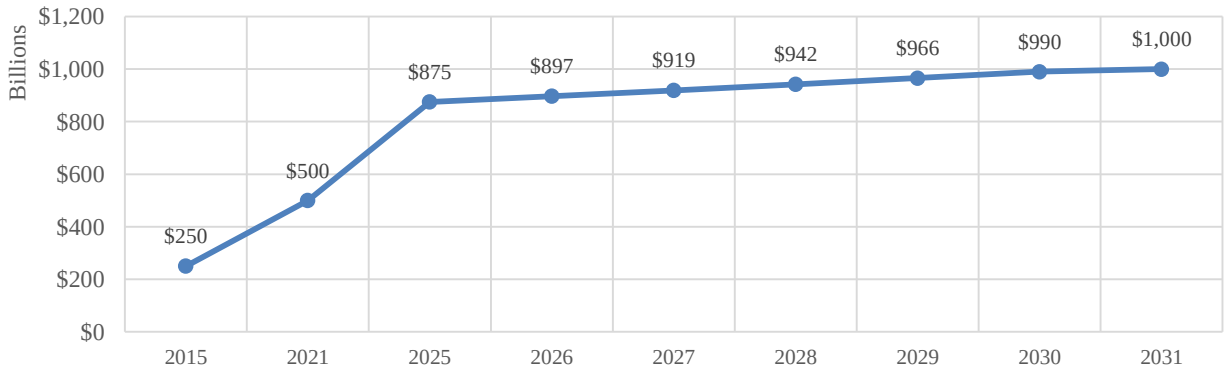


Figure 1. Global cybercrime damage cost per month each year predictions in USD [11].

2. BACKGROUND

A multi-dimensional security model establishes a framework that includes a foundational understanding of physical documents and their associated security systems (i.e., types of identification documents) (see [13], [14] for definitions) as well as a description of systematic threat analysis that identifies all potential threats to a physical document and describes how those threats can be managed through sophisticated security systems (as shown in [15], [16]). Afterward, this section discusses in detail the security technologies referenced within the literature, including a categorization of countermeasures as physical and digital. The analysis of Guilloche patterns illustrates the well-known use of Guilloche patterns to improve the security of physical documents [17][18]. The discussions on digital security within this section will provide an in-depth analysis of digital security technologies, including QR codes as data carriers [19][20], and the SHA-256 hash function [21][22], as well as Elliptic Curve Cryptography (ECC), which has been widely used for digital signatures (ECDSA) [23][24] and encryption (ECIES). This structured approach offers an understanding of the issue and the various technologies that can secure sensitive documents.

2.1. Official Identification Documents

The official identification documents are legally recognized by the state or issued by institutions. They are used to confirm and validate personal characteristics and provide individuals access to many services, allow individuals to exercise their rights and participate in regulated activities [13], [25] The reliability of these processes (either exercising rights or accessing services) is dependent upon the authenticity and integrity of the documentation and thus the security of these documents is of utmost importance. [14]

2.1.1. Common Types and Content

While the specific design varies by jurisdiction and purpose, most official IDs share common structural and data elements. Key document types include:

a) National ID Cards: Government-issued primary identity credentials used for domestic identification [29].
b) Passports: Internationally recognized travel documents that certify the holder's identity and nationality [27].
c) Driver's Licenses: Permits authorizing vehicle operation, often serving as a de facto standard identity card [14].
d) Student ID Cards: Institution-specific credentials granting access to educational resources and verifying enrollment status.[26]

In general, the information contained in the document will include, at minimum, your full name, an identification number (unique), your photo, your address, your date of birth and the date that the document is issued and will expire, and additional security features that are intended to be overt or covert [14]; [28]. Adding all of this personal information, along with the security features, to a physical card makes it extremely difficult to reproduce an exact copy of that card without detection.

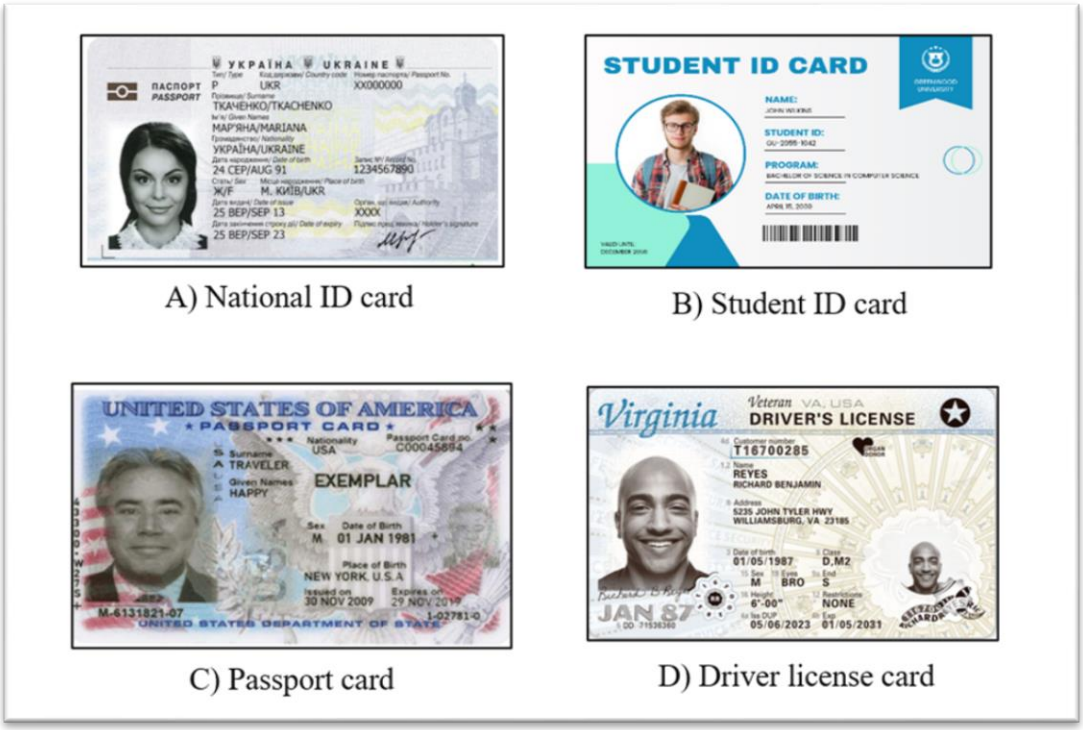
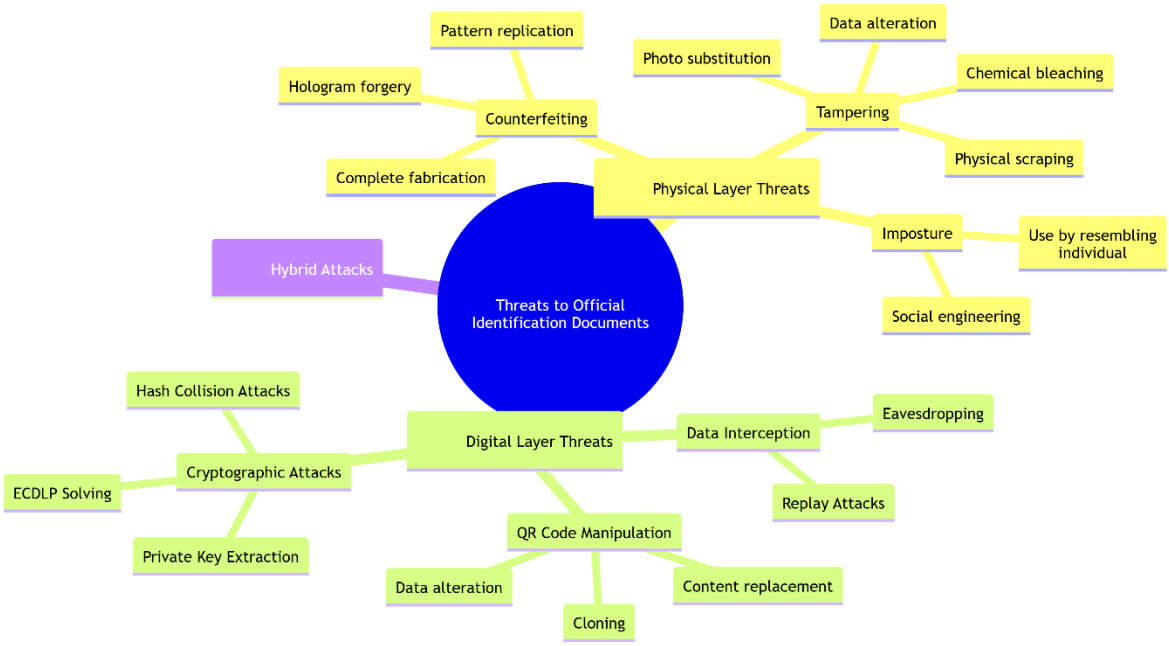


Figure 2.1. Different types of official ID documents (National ID, Student ID, Passport, Driver's License)

2.2. Threat Modeling for Official Documents

Developing a strong security plan requires developing a thorough threat modelling process for each potential threat to an organisation's information. The array of threats to official/documents is extensive, including threats to both their physical and electronic aspects (29). Figure 2.2 outlines the taxonomy of all the various threats to official documents that will ultimately be a part of the finished product's security plan. Figure 2.2 provides a comprehensive



view of the various ways that people can attack the products that result from the new information security system.Figure 2.2. Taxonomy of Threats to Official Identification Documents

2.2.1. Physical Layer Threats

These attacks target the tangible document itself, focusing on replicating or altering its physical characteristics.

a) **Counterfeiting:** is the process of creating a completely new document by reproducing as closely as feasible the appearance of the authentic document, including all of the security measures built into the genuine document, such as holograms and guilloche patterns [16], [30]. Counterfeiters use advanced technology to replicate patterns and make imitation materials.
b) **Tampering/Alteration:** it's when a legit document is tampered with and some of its key aspects are modified, such as changing its picture, name, and DOB ([15], [31]). Examples of this would include taking a picture of someone else's face and putting it on the document, using a chemical bleaching agent to remove the original information, or scrapping the graphic on the document.
c) **Imposture** refers to the situation where an individual uses a valid document that bears a likeness to them, taking advantage of the limitations of the human eye and verification methods [32]. The threat of imposture combines elements of social engineering and physical likeness.

2.2.2. Digital Layer Threats

These attacks target the machine-readable data and the cryptographic protocols protecting them, focusing on the electronic representation and verification mechanisms.

a. **QR Code Manipulation:** An individual with malicious intent can clone a legitimate QR code found on a legitimate document and paste it into an illegitimate document, or alter the data encoded in the legitimate QR code to provide false or misleading information [20], [33]. This includes the complete replacement of all content within the original QR code to accommodate the physical changes in the document.
b. **Data Interception and Replay:** Eavesdropping on verification communications or capturing and re-sending valid data packets to impersonate a legitimate holder [34]. These attacks exploit vulnerabilities in the communication channel between the document and verification systems.
c. **Cryptographic Attacks:** Direct attempts to break the underlying cryptography, including finding hash collisions in SHA-256 [35], solving the elliptic curve discrete logarithm problem (ECDLP) to derive private keys [23], [36], or side-channel attacks to extract cryptographic secrets.

2.2.3. Hybrid Layer Threats

Modern sophisticated attacks often use a combination of digital and physical elements to generate more persuasive fake documents that defeat many levels of security controls. One example is the use of a expertly produced counterfeit document in conjunction with a tampered with QR code containing matching fraudulent information and legitimate cryptographic signatures obtained from other sources. Compound threats like this are the most difficult to identify and prevent [16], [37] from occurring.

2.3. Anti-Counterfeiting techniques

An efficient anti-counterfeiting strategy utilizes a defense-in-depth strategy that combines attributes of multiple visibility, verification methods and underlining security features. This article categorizes and evaluates popular techniques based on their three major categories: Overt (Level One), Covert (Level Two) and Digital/Machine-Readable (Level Three) according to their costs, security levels and performance.

2.3.1. Overt Security Features (Level 1)

Overt features are designed for immediate, unaided visual authentication by the public and officials, serving as a primary deterrent [38]. Their effectiveness relies on recognize ability and difficulty of simulation.

A. Holograms: Holograms are diffractive optical elements that produce dynamic three-dimensional images with kinetic color-shift effects [39].

- **Cost:** Moderate unit cost for mass production, with high initial setup costs for mastering and embossing dies [40].
- **Security:** Medium to High. Highly effective against casual counterfeiters but vulnerable to sophisticated simulation using generic foils or advanced printing [39].
- **Performance:** Excellent for instant public verification. Durable, though prone to abrasion. Verification is fast and intuitive [40].

B. Guilloche pattern: Guilloche refers to intricate, finely interwoven line patterns generated by precise engraving, creating complex graphical backgrounds that resist reproduction [10].

- **Cost:** Low to Moderate. The cost is primarily in the digital design; printing adds negligible marginal cost to high-resolution processes [18].
- **Security:** Medium. Effectively thwarts standard photocopiers and scanners (causing moiré effects) but can be replicated by high-resolution digital printing [31].
- **Performance:** Serves as an overt/covert hybrid. Visible to the eye, but full authentication often requires a loop. Passive and durable [31].

2.3.2. Covert Security Features (Level 2)

Covert features require simple tools, training, or knowledge for verification, providing a secondary authentication layer for inspectors, retailers, or authorized personnel [38].

A. Micro printing: Micro printing involves embedding text or patterns at a scale below 0.2mm, appearing as a solid line to the naked eye [41].

- **Cost:** Very Low. Utilizes existing high-precision printing without special materials [42].
- **Security:** Low to Medium. A strong deterrent against low-resolution reproduction but offers no cryptographic security and is vulnerable to high-resolution copying [41].
- **Performance:** Reliable for tool-assisted checks. Verification is fast with a magnifier. Durability depends on print and substrate quality [43].

B. Digital Watermarks: Digital watermarks imperceptibly embed information into the pixel data or frequency domain of an image or graphic [44].

- **Cost:** Variable. Software embedding has low cost, but robust systems require algorithm development and potentially licensed detection software/hardware [44].
- **Security:** Medium to High. Security depends on the algorithm's robustness to distortion and use of cryptographic keys for embedding/detection [45].

- **Performance:** Excellent for covert tracking and forensic analysis. Automated detection is fast with the correct key. Performance degrades under severe image manipulation [46].

2.3.3. Digital and Machine-Readable Security Features (Level 3)

This category encompasses features that enable automated authentication, unique item identification, and cryptographic assurance, linking the physical item to a digital trust infrastructure [47].

A. Radio frequency identification (RFID) and near-field communication (NFC) technologies utilize wireless (electromagnetic) chips, which are commonly referred to as tags, to store and transmit identifying information when energized by a reader [48].

- **Cost:** Cost of tags, readers, and database infrastructure may be moderate to high, depending on the security of the tags purchased; for example, secure crypto tags have a much higher cost than standard ones [49].
- **Security:** The security level for basic RFID/NFC tags is low, while secure RFID/NFC tags with sophisticated cryptographic methods have a very high security level [50].
- **Performance:** RFID/NFC allows very high-performance, non-contact batch reading and unique device address tracking. This performance is affected by the read distance and by interference from other electronic devices in the environment [48].

B. Quick Response (QR) Codes: QR codes are 2D matrix barcodes that store data, often used to link a physical item to a digital resource [51].

- **Cost:** Extremely Low. Generation and printing are virtually free; scanning uses ubiquitous smartphones [51].
- **Security:** Low in isolation. Security is derived entirely from the content (e.g., cryptographically signed data or dynamic online verification) [52].
- **Performance:** Excellent for machine-readable data bridging. Scanning is fast and robust to mild damage. Performance depends on network connectivity for online verification [53].

C. Digital Signatures: Digital signatures use public-key cryptography to bind an entity's identity to digital data, ensuring integrity, authentication, and non-repudiation [54].

- **Cost:** Low operational, Moderate systemic. Computation is cheap, but establishing a Public Key Infrastructure (PKI) for trust is complex and costly [55].
- **Security:** Very High. Based on computational hardness assumptions; provides the highest level of cryptographic assurance [56].
- **Performance:** Verification is computationally fast. The key challenge is the secure management of keys and the trust infrastructure (PKI) [54].

The analysis underscores that no single technique is sufficient. A synergistic integration across all three levels is essential [29]. An optimal security document might combine an overt hologram (public deterrence), covert micro printing (inspector verification), and a digital layer comprising a unique RFID identifier linked to a digitally signed record accessible via a QR code. This layered approach balances cost and security, ensuring resilience by requiring an attacker to defeat multiple, diverse protective mechanisms simultaneously [57]. Table 2.1 below summarize each technology according to (Cost, security and performance).

Table 2.1. Anti-Counterfeiting techniques specifications

Technology	Cost	Security	Performance
Hologram	Moderate	High	High
Guilloche pattern	Moderate	High	High
Micro printing	Low	High	Moderate
Digital watermarks	Low	Moderate	Moderate
RFID	High	Very High	High
QR	Low	Moderate	High
Digital signatures	Moderate	Very High	High

3. LITERATURE REVIEW

The growth in innovations within digital technology has resulted in improved ways to forge or counterfeit documents that have been very challenging to security systems across the globe. The purpose of this literature review is to provide a summary of research (from 2021 to 2025) related to the detection and prevention of forgery, in particular relating to identity documents, QR code (Quick Response code) technologies, and both digital/paper-based certificates. A significant part of this literature review includes an analysis of each paper and a summary of what are considered the two primary research streams, as well as any research gaps that currently exist. From the analysis, we were able to demonstrate the trends in forgery methods, assess detection algorithms' effectiveness, and demonstrate a way forward in providing an effective solution that balances security with employee convenience. Traditionally, this literature review was structured to demonstrate the differences between established technologies and current developments and innovations, as well as demonstrate how these technologies can be used to develop a business model based on scalability, accuracy, and practicality within the workplace.

3.1. Deep Learning for Forgery Generation and Detection

A significant portion of recent research leverages deep learning to both create and combat sophisticated forgeries, highlighting an ongoing arms race in document security.

L. Zhao, C. Chen, and J. Huang (2021) [5] proposed a new document forgery detection algorithm, which is based on a deep learning model, as opposed to prior methods that primarily relied upon multimedia-type technologies for this function. This new approach attempts to address a number of specific problems that occur when using current tools, particularly with respect to the complex characters and backgrounds found in most document images, by separating the background out from the content (i.e., textual) portion of an image; by offering an auxiliary skeleton of the text portion of a document; and by removing the visual evidence of forgery via post-processing techniques. The practical application of this study is demonstrated by showing that an attacker can manipulate a single sample of an authentic identity document and produce multiple forgeries of that document, all of which will pass verification by the state-of-the-art document authenticity checking methods currently in existence. This research shows how easily advanced deep learning technologies can be used to create realistic counterfeit identity documents, as well as highlighting the potentially serious implications for the safety and security of citizens when such technologies are misused. Similarly, Al-Ghadi et al. (2023) [10] presented the FMIDV dataset, which contains fraudulent identity documents that feature guilloche designs, and developed two different types of ML model to detect fraud through ID verification using guilloche designs on ID documents and the similarity of these designs to authentic documents. The findings of the studies by these authors show how effective their methods were in identifying fraudulent documents and creating a reference point for future research on document authentication. This was accomplished with a novel approach using advanced machine learning techniques, which have proven to be highly accurate in identifying fraudulent document identifiers. The goal of the team from L. Dong, W. Liang and R. Wang (2024) [58] was to create a novel approach for detecting and identifying counterfeit documents from digital images of text, however, they also include many other digital document types and documents such as: Certificates. The new approach presented in this research is presumed to be able to process a wide variety of Federal Protective Service products using active and passive forensic methods. Specifically, the researchers tackled the concern of tracking an original paper document with physical evidence that may have been changed by later modification and built a method by which one could take advantage of processes to assist in discovering forgery. By combining both high-level semantic features and low-level visual characteristics, and using multi-scale attention mechanisms, the framework assists with improving upon the important feature of locating a forgery on a document more accurately. Based on a very large and diverse data set, the authors have demonstrated through the use of the framework presented in their article that their framework for Document Verification is superior to all existing Document Verification Methods in terms of accuracies in the verification of documents. The authors also state that their framework demonstrates various advantages in terms of improved accuracy in the identification of forgeries, particularly with certified and scanned documents. The research of M. Sirajudeen and R. Anitha (2025) [59] proposes an automated verification model, which is based upon Convolutional Neural Networks (CNN), Optical Character Recognition (OCR), and Linear Binary Pattern (LBP), to provide three forms of verification mechanisms to help improve accuracy during Document Verification Phase by authenticating Text and Image, including Seal and Hologram Verification. Additionally, through the automation of Document Verification, it is anticipated that there will be a significant reduction in Administrative Overhead incurred by Document Management Systems and an overall increase in Operational Efficiency of Document Management Systems. Log-Transform Histogram Equalization (LTHE) is a recent approach to improving the detection of counterfeit documents using deep learning models. This novel approach was developed by Y. Bae, D. Cho and K. Jung (2025) [60] to address the challenging problem of detecting forged document images using deep learning models. The LTHE technique improves the

ability to detect subtle pixel level differences in the forged document through the application of a logarithmic transformation followed by histogram equalization. By utilizing this approach, the forged document image will exhibit stronger contrast, allowing for greater visibility of the dissimilarities between the forged and real portions of the image. The findings presented in this wok establish that classifying many different CNN architectures using the LTHE enhances the accuracy of many different CNN architectures used to classify many different types of document images (forged), thereby demonstrating the benefits of using this technique when developing deeper learning systems for detecting forgeries in document images.

3.2. QR Code Security Enhancements

QR Code technology has continued to be used in many consumer services; however, QR Codes have also become involved with efforts by security researchers to integrate secure methods of verifying codes directly into the QR Codes themselves. Justin Picard's system (2021) [4] has created a copy detection pattern that can be embedded within a QR Code, so as to allow for enhanced verification of that QR Code. This system provides enhanced security against cloned and serialized QR codes, and uses mobile devices to allow users to scan and examine the patterns. The proposed system allows consumers to verify that the product they purchased is an authentic one through a very simple scanning process and gives manufacturers a means of establishing product authenticity. T. Wang, H. Zheng, C. You, and J. Ju's (2023) [9] research investigated how to embed random texture patterns into QR codes to combat illegal duplication through the use of an embedded texture-hiding technology based on a Gaussian distribution combined with an information-hiding technology; both of these technologies have been successfully tested to create a quality assessment algorithm and a dual feature detection algorithm that will assist in validating the authenticity of QR Codes. This research has developed a secure method for authenticating products while maintaining the generality of QR Codes and has shown excellent feasibility and performance in experimental settings. Another work is proposed by M. Chapel, M. AL-Ghadi, and J. Burie (2023) [61] that provides a novel approach to secure QR Codes through the implementation of distinct visual elements added to the QR Code which are nearly impossible to duplicate and will only allow verification through a proposed mobile app. The presenters of this research show that this method provides trustworthy verification of QR Code authenticity with a high degree of success rate. The authors have demonstrated a reliable solution for establishing verifiable trust in the intended QR code usage using a highly secure QR Code solution developed by N. Wang, L. Zhang, T. Jiang, and T. Shen (2025) [62]. This solution leverages a Convolutional Neural Network (CNN) and a Twin Network. The objective of the technical work presented in this study is to enable the embedding of confidential data into QR codes, while still maintaining their invisibility and durability. The authors want the information that is encoded in the QR Codes to be hidden from the users while they build a strong mechanism to prevent counterfeiting and tampering of the QR Codes. As shown by tests performed on this solution, it is resistant to numerous types of attacks and has received high ranking for its invisibility and its accuracy in establishing the authentication process.

3.3. Cryptographic Verification Systems

This stream of research prioritizes data integrity and authenticity through the application of cryptographic principles, from simple hashing to advanced public-key cryptography.

In an effort to provide localized encryption techniques, Researchers are continuing to develop Digital Security verification methods. Hamad, Hameed, and Ali [63] discuss secure mobile transactions based on a hybrid AES / ECC encryption approach to store the encrypted transactional data in a QR code on the end user’s device, allowing for 2 or more MFA authentication and improving both security and accessibility within Mobile Banking environments. Several studies published in 2024, have focused on the fight against Document Fraud. Kunekar et al. [64] developed a method of creating a tamper proof seal for documents via a random number generator with SHA256 hash function for the Document Seal and maintaining the verification of the data in a database in the Cloud. Boonkrong [7] developed an analysis of several types of Cryptographic Hash Functions that protect Academic Documents. Advancing beyond these methods, Diarra, Bissyande, and Poda [65] have developed an Unsupervised Machine Learning Model called Doc-Patch, which utilizes both Self-Attention based models and the FAISS k-nearest neighbor search to analyse document patches for inconsistency detection. In order to identify forgeries of 96.51% precision this approach outperforms the traditional methods of document verification.

3.4. Synthesis and Identified Gap

The products of these various areas of development are detailed and summarized in Table 3.1 of this literature review. While there is evidence that improvements in deep learning techniques (including adversarial learning and convolutional neural networks) may have led to greater accuracy and reliability in the forensic analysis of identity documentation and detection of scanned certificates forged through forgery, there have also been

developments in additional areas of technological development with respect to the security of QR codes against cloning and manipulation. QR codes are no longer simply data carriers; they have advanced and developed to become secure authentication tokens. With regard to cryptographic methods and the emerging technologies in both Hybrid encryption and advanced hashing (very strong hashing), cryptography will continue to be important to maintain data integrity and to provide non-repudiation for electronic commerce transactions. These research efforts have great potential. Yet, the commonality throughout these research opportunities in literature review is that they silo themselves from each other. For instance, deep learning is great at detecting visual anomalies. However, deep learning cannot verify a document's provenance through cryptographic verification. Cryptographic systems protect the data but cannot distinguish excellent quality counterfeit documents that leave behind a digital fingerprint. Additionally, QR code enhancements provide increased protection around a code's physical characteristics than they do around the QR code itself. Without cohesive, comprehensive systems that encompass the entire document lifecycle - from the design of documents with security embedded physically, to cryptographic origination, to combined methods for verifying both the physical document and the cryptographic verification layer are missing and therefore create a separation between methodologies. To realize these methods a unified approach to document security will be a primary objective of this research.

Table 3.1. Summary of Literature review

Related Work	Aim	Technique	Document type	Evaluation framework	Application domain	Literature review summary				
						Flexible	Scalable	Time	Security	Cost
L.Zhao (2021) [5]	Analyze forgery attacks	Deep Learning	Document Images	Performance against forgery attacks	Document Management	Yes	Yes	Moderate	High	High
J.Picard (2021) [4]	QR code authentication	QR Code with Copy Detection Pattern	Product Packaging	Effectiveness in counterfeit detection	Industrial Products	Yes	Yes	Moderate	High	Moderate
M.Al-Ghadi (2023) [10]	Detect guilloche patterns	Contrastive & Adversarial Learning	Identity Documents	Detection accuracy on FMIDV dataset	ID Verification	Yes	Yes	Moderate	High	Moderate
T.Wang (2023) [9]	Hidden texture QR codes	Texture Embedding in QR Codes	Product QR Codes	System feasibility and performance	Product Authentication	Yes	Yes	Moderate	High	Moderate
Marie-Neige Chapel (2023) [61]	Verify hologram authenticity	Pattern Analysis & Mixed Pattern Verification	Security Documents	Authentication, accuracy and robustness	Security Documents	Yes	Yes	Moderate	High	High
N. J. Hamad (2024) [63]	Secure cardless transactions	QR Code & Hybrid Encryption	Mobile banking transactions	Demonstrated data confidentiality and integrity	Mobile Banking	Yes	Yes	Moderate	High	Moderate
P.Kunekar (2024) [64]	Improve document verification	Cryptographic Hashing & RNG	Digital Documents	Verification accuracy and reliability	Various (Legal, Academic)	Yes	Yes	Moderate	High	Moderate
L.Dong (2024) [58]	Enhance tampered text localization	Multiscale Attention & Image Processing	Scanned Documents and Certificates	Localization accuracy	Various (Legal, Academic)	Yes	Yes	Moderate	High	Moderate
S.Boonkrong (2024) [7]	Academic forgery detection	Deep Learning	Identity Documents	Practical scenario effectiveness	Universities, Academic Institutions	Yes	Yes	Low	High	Moderate
A. DIARRA (2024) [65]	Unsupervised forgery detection	Unsupervised Learning	Digital Documents	High precision in unsupervised detection	Legal, Academic	Yes	Yes	Moderate	High	Moderate
N.Wang (2025) [62]	Prevent QR code tampering	Deep Learning & QR Code	Product QR Codes	Performance in tamper prevention tests	Product Authentication	Yes	Yes	Moderate	High	Moderate
M.Sirajudeen (2025) [59]	Automate document verification	Cognitive Techniques	Various Documents	System accuracy and efficiency	Government, Private Sector	Yes	Yes	Moderate	High	High
Yong-Yeol Bae (2025) [60]	Enhance feature extraction	Image Enhancement & Deep Learning	Document Images	Improved classification accuracy	Document Management	Yes	Yes	Moderate	High	Moderate

3. TRENDS AND FUTURE DIRECTION

Over time, the security of documents has evolved as a result of the combination of various forms of security technologies (physical, digital, and biometric) which provide users with a better, more flexible, and convenient

experience. Recent developments also indicate an emergence towards Unified Security Systems. While historically, many different forms of security technology (standalone technologies), now we see the rapid acceptance of integrated systems which consist of multiple types of authentication technology, (i.e., cryptographic signatures, QR code-based verification and tamper-evident physical components). The emergence of Unified Security Systems is a significant advancement in the evolution of technology and provides us with a more versatile and integrated solution. The adoption of ECC and SHA-256 as a means of establishing a higher standard of secure and efficient cryptographic standards is an example of how the evolution of technology is utilizing more practical security methods in environments with limited resources, such as smart-identity cards and mobile device verification applications.

Block chain technology's growing role in document verification is due to its ability to facilitate decentralized trust (relying on no central authority) and immutable audits. As a result, companies are increasingly adopting block chain as their source of confirmation for digital documents. In addition to using block chain technology for document verification, organizations are also implementing ML and DL within their workflow in many organizations to either identify forged signatures/documents, or create dynamic models for threats and detections of anomalies in live. Finally, the use of biometrics, such as face recognition, finger prints and iris scans being cryptographically bound to document data, represents another effective approach for enhancing document verification security and usability.

Future studies ought to investigate cost-effective, scalable solutions to hybrid security systems that would be appropriate for developing regions with continuing infrastructure limitations. Quantum Computing will be an ongoing threat to Current Cryptographic Standards. Because of this, it will be necessary to explore the use of Post-Quantum Cryptographic Algorithms for Document Security. In order to create systems that have a high degree of security, and at the same time, provide intuitive usability and accessibility, there will need to be continued collaboration between Cryptography Researchers, Material Science Researchers, and Human-Computer Interaction Researchers.

4. CONCLUSION

The manner in which documents are secured has been thoroughly reviewed and documents that are forged through physical or technological means are still presenting ever-increasing challenges for both individuals and companies. The research into this subject has shown that even though there has been progress through developing individual security technologies, such as deep learning based detection systems or cryptographic verification systems, or QR code security systems, there is still a significant lack of an overall multi-dimensional, integrated security framework that uses the strengths of these technologies. The current trends in document security research demonstrate that a better solution will almost always be preferred and that physical security features and digital authentication mechanisms have historically been developed/tested in an isolated manner. Furthermore, the literature strongly supports the notion that sophisticated threats are growing increasingly reliant upon hybrid attack methods exposing the gaps in security layers believed to exist in many current security systems. An urgent paradigm shift in document security design must take place, moving from developing isolated point security technology solutions towards creating holistic integrated architectures encompassing anti-tampering features, cryptographic protocols, and machine-readable data carriers. Henceforth, integrated systems must address and take into account every aspect of the document lifecycle including secure issuance of documents and binding of data and, when imminent, also provide an intuitive, reliable field verification mechanism.

REFERENCES

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[2] J. Muñoz-Haro, R. Tolosana, J. Fierrez, R. Vera-Rodriguez, and A. Morales, “Privacy-aware detection of fake identity documents: methodology, benchmark, and improved algorithms (FakeIDet2),” Information Fusion, vol. 128, p. 103969, Apr. 2026, doi: 10.1016/j.inffus.2025.103969.

[3] Ferrara, M., Franco, A., & Maltoni, D. (2016). The magic passport. In IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-7).

[4] Picard, J. (2021). Counterfeit detection of variable data using serialized QR codes with copy detection patterns. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (pp. 1-12).

[5] Zhao, L. (2021). Deep Learning-based Forgery Attack on Document Images. In IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops.

[6] Van Renesse, R. L. (2005). Optical document security. In Optical Security and Counterfeit Deterrence Techniques V (Vol. 5310, pp. 1-21). SPIE.

[7] Boonkrong, S. (2024). The Use of Cryptographic Hash Function for the Detection of Modification in Digital Academic Documents. Journal of Information Security and Applications, 103784.

[8] Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, 1(1), 36-63.

[9] Wang, T., & Chen, Y. (2023). Texture-hidden QR code for anti-counterfeiting. Springer Multimedia Tools and Applications, 82(5), 6785-6802.

[10] Al-Ghadi, M., et al. (2023). FMIDV: A Dataset for Identity Document Forgery Detection and Localization. In IEEE International Conference on Image Processing (ICIP).

[11] Cybersecurity Ventures. (2025). Official Cybercrime Report. [Online]. Available: https://cybersecurityventures.com/official-cybercrime-report-2025/

[12] Lam, L. (2019). Man forged documents including NUS degree to get work, snagging 38 jobs in 4 years. Channel News Asia "https:// www. chann elnew sasia. com/ singa pore/ man- forge- docum ents- nus- degree- get- jobs- 38- compa nies- 890881".

[13] R. A. Khan and S. A. Lone, "A comprehensive study of document security system, open issues and challenges," Multimedia Tools and Applications, vol. 80, no. 5, pp. 7039–7061, Feb. 2021, doi: 10.1007/s11042-020-10061-x.

[14] J. Jenis, J. Ondriga, S. Hrcek, and E. Sádovský, "Mechanical Design of a Device for Automatic Implementation of Security Features on Passports," in Transportation Research Procedia, Elsevier B.V., 2023, pp. 538–546. doi: 10.1016/j.trpro.2023.11.179.

[15] I. Marin-Aguilar, L. A. Chavarria-Zamora, and L. Araya-Martinez, "A practical approach to validate the authenticity of identity documents," in 2022 IEEE Latin America Electron Devices Conference, LAEDC 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/LAEDC54796.2022.9908240.

[16] N. Challa, A. Shende, and M. Mullapudi, "Enhancing Document Verification Systems: A Review of Techniques, Challenges, and Practical Implementations," International Journal of Computer Engineering and Technology (IJCET), vol. 15, no. 1, pp. 16–25, 2024, doi: 10.17605/OSF.IO/HVQ8E.

[17] A. Abu-Jassar, V. Manakov, and M. Al-Abdallat, "Features of the Formation of Guilloche Rosettes." Journal of Universal Science Research, ISSN: 2181-4570 2023, 1(12), 129–138

[18] M. Al-Ghadi, Z. Ming, P. Gomez-Krämer, and J.-C. Burie, "Identity Documents Authentication based on Forgery Detection of Guilloche Pattern," Jun. 2022, [Online]. Available: http://arxiv.org/abs/2206.10989

[19] Denso Wave, "QR Code essentials," 2022. [Online]. Available: https://www.denso-wave.com/en/technology/vol1.html

[20] M. A. U. Naser, E. T. Jasim, and H. M. Al-Mashhadi, "QR code based two-factor authentication to verify paper-based documents," Telkomnika (Telecommunication Computing Electronics and Control), vol. 18, no. 4, pp. 1834–1842, 2020, doi: 10.12928/TELKOMNIKA.V18I4.14339.

[21] H. E. Michail, G. S. Athanasiou, G. Theodoridis, A. Gregoriades, and C. E. Goutis, "Design and implementation of totally-self checking SHA-1 and SHA-256 hash functions' architectures," Microprocessors and Microsystems, vol. 45, pp. 227–240, Sep. 2016, doi: 10.1016/j.micpro.2016.05.011.

[22] R. Roshdy, M. Fouad, and M. Aboul-Dahab, "DESIGN AND IMPLEMENTATION A NEW SECURITY HASH ALGORITHM BASED ON MD5 AND SHA-256," 2013.

[23] B. P. Kavin and S. Ganapathy, "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves," International Arab Journal of Information Technology, vol. 18, no. 2, pp. 180–190, 2021, doi: 10.34028/IAJIT/18/2/6.

[24] W. Cao, H. Shi, H. Chen, and Y. Wang, "A new weak curve fault attack on ECIES: embedded point validation is not enough during decryption.", Chinese Academy of Sciences, Beijing 100190, China, 2021.

[25] K. B. Bulatov, P. v. Bezmaternykh, D. P. Nikolaev, and V. v. Arlazarov, "Towards a unified framework for identity documents analysis and recognition," Computer Optics, vol. 46, no. 3, pp. 436–454, May 2022, doi: 10.18287/2412-6179-CO-1024.

[26] A. F. Mae Muelan, K. G. Marie Decomotan, and J. N. Lebuna, "Student ID Validation Monitoring System."

[27] P. Sharma and N. Bhatnagar, "Passenger Authentication and Ticket Verification at Airport using QR Code Scanner," SKIT Research Journal, vol. 13, p. 2023, doi: 10.47904/IJSKIT.13.2.2023.10-13.

[28] C. Irimia, F. Harbuzariu, I. Hazi, and A. Iftene, "Official Document Identification and Data Extraction using Templates and OCR," in Procedia Computer Science, Elsevier B.V., 2022, pp. 1571–1580. doi: 10.1016/j.procs.2022.09.214.

[29] R. Sukhija, M. Kumar, and M. K. Jindal, "Document forgery detection: a comprehensive review," International Journal of Data Science and Analytics, vol. 20, no. 5, pp. 4385–4407, Oct. 2025, doi: 10.1007/s41060-025-00723-0.

[30] Q. Wang, A. Ge, X. Chen, J. Wu, S. Liu, and D. Zhu, "Text information security protection method based on computer-generated holograms," Applied Optics, vol. 63, no. 15, p. 4165, May 2024, doi: 10.1364/ao.523616.

[31] M. Al-Ghadi, Z. Ming, P. Gomez-Kramer, J. C. Burie, M. Coustaty, and N. Sidere, "Guilloche Detection for ID Authentication: A Dataset and Baselines," in 2023 IEEE 25th International Workshop on Multimedia Signal Processing, MMSP 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/MMSP59012.2023.10337681.

[32] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," Pattern Recognition Letters, vol. 79, pp. 80–105, Aug. 2016, doi: 10.1016/j.patrec.2015.12.013.

[33] J. Nasereddin and A. A. Salem, "Enhancing Printed Document Security with QR Code-Based Digital Signatures," in 2024 25th International Arab Conference on Information Technology, ACIT 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ACIT62805.2024.10877207.

[34] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[35] M. Stevens, P. Karpman, and T. Peyrin, "The first collision for full SHA-1," in Adv. Cryptol. – CRYPTO, 2016, pp. 570–596.

[36] Y. Yan, "The Overview of Elliptic Curve Cryptography (ECC)," in Journal of Physics: Conference Series, Institute of Physics, 2022. doi: 10.1088/1742-6596/2386/1/012019.

[37] S. Gonzalez and J. E. Tapia, "Forged presentation attack detection for ID cards on remote verification systems," Pattern Recognition, vol. 162, Jun. 2025, doi: 10.1016/j.patcog.2025.111352.

[38] T. Necsoiu, G. Bostan, P. Sterian, and M. Berteanu, "MATERIALS FOR SECURITY ELEMENTS USED IN PROTECTED DOCUMENTS, OPTICAL EXAMINATION METHODS. A REVIEW," 2017.

[39] D. M. Elmahal, A. S. Ahmad, A. T. Alomaier, R. F. Abdlfatah, and D. M. Hussein, "Comparative study between hologram technology and augmented reality," Journal of Information Technology Management, vol. 12, no. 2, pp. 90–106, 2020, doi: 10.22059/JITM.2020.75794.

[40] A. Mukundan, Y. M. Tsao, F. C. Lin, and H. C. Wang, "Portable and low-cost hologram verification module using a snapshot-based hyperspectral imaging algorithm," Scientific Reports, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-22424-5.

[41] Z. Dong and P. A. Levkin, "3D Microprinting of Super-Repellent Microstructures: Recent Developments, Challenges, and Opportunities," Advanced Functional Materials, vol. 33, no. 39. John Wiley and Sons Inc, Sep. 26, 2023. doi: 10.1002/adfm.202213916.

[42] J. Patadiya, M. Naebe, X. Wang, G. Joshi, and B. Kandasubramanian, "Emerging 4D printing strategies for on-demand local actuation & micro printing of soft materials," European Polymer Journal, vol. 184. Elsevier Ltd, Feb. 07, 2023. doi: 10.1016/j.eurpolymj.2022.111778.

[43] F. Mayer, S. Richter, J. Westhauser, E. Blasco, C. Barner-Kowollik, and M. Wegener, "A P P L I E D P H Y S I C S Multimaterial 3D laser microprinting using an integrated microfluidic system," 2019. [Online]. Available: https://www.science.org

[44] P. Kadian, S. M. Arora, and N. Arora, "Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey," Wireless Personal Communications, vol. 118, no. 4. Springer, pp. 3225–3249, Jun. 01, 2021. doi: 10.1007/s11277-021-08177-w.

[45] H. M. Al-Dabbas, R. A. Azeez, and A. E. Ali, "Digital Watermarking, Methodology, Techniques, and Attacks: A Review," Iraqi Journal of Science, vol. 64, no. 8, pp. 4169–4186, 2023, doi: 10.24996/ijs.2023.64.8.37.

[46] Z. Wang et al., "Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography," Apr. 2023, [Online]. Available: http://arxiv.org/abs/2107.09287

[47] P. Wyatt, "Work in progress: Demystifying PDF through a machine-readable definition," 2021. [Online]. Available: https://www.pdfa.org/iso-32000-normative-references/

[48] G. Casella, B. Bigliardi, and E. Bottani, "The evolution of RFID technology in the logistics field: A review," in Procedia Computer Science, Elsevier B.V., 2022, pp. 1582–1592. doi: 10.1016/j.procs.2022.01.359.

[49] A. Haibi, K. Oufaska, K. el Yassini, M. Boulmalf, and M. Bouya, "Systematic Mapping Study on RFID Technology," IEEE Access, vol. 10, pp. 6363–6380, 2022, doi: 10.1109/ACCESS.2022.3140475.

[50] M. M. Mijwil, Kamal Kant Hiran, Ruchi Doshi, and Omega John Unogwu, "Advancing Construction with IoT and RFID Technology in Civil Engineering: A Technology Review," Al-Salam Journal for Engineering and Technology, vol. 2, no. 2, pp. 54–62, Mar. 2023, doi: 10.55145/ajest.2023.02.02.007.

[51] Anita Sondhi and Dr. Ravindra Kumar, "QR Codes in Education : A Review," International Journal of Scientific Research in Science and Technology, pp. 193–205, Feb. 2022, doi: 10.32628/ijsrst229118.

[52] K. Rotsios, A. Konstantoglou, D. Folinas, T. Fotiadis, L. Hatzithomas, and C. Boutsouki, "Evaluating the Use of QR Codes on Food Products," Sustainability (Switzerland), vol. 14, no. 8, Apr. 2022, doi: 10.3390/su14084437.

[53] M. Imanullah and Y. Reswan, "Randomized QR-code scanning for a low-cost secured attendance system," International Journal of Electrical and Computer Engineering, vol. 12, no. 4, pp. 3762–3769, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3762-3769.

[54] D. Diemert, K. Gellert, T. Jager, and L. Lyu, "More Efficient Digital Signatures with Tight Multi-User Security."

[55] Y. Peng, Q. Feng, D. B. He, and M. Luo, "A survey on threshold digital signature schemes," Frontiers of Computer Science, vol. 20, no. 4. Higher Education Press Limited Company, Apr. 01, 2026. doi: 10.1007/s11704-025-41297-1.

[56] J. Chia, J. J. Chin, and S. C. Yip, "Digital signature schemes with strong existential unforgeability," F1000Research, vol. 10. F1000 Research Ltd, 2021. doi: 10.12688/f1000research.72910.1.

[57] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic Literature Review on Security Risks and its Practices in Secure Software Development," IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers Inc., pp. 5456–5481, 2022. doi: 10.1109/ACCESS.2022.3140181.

[58] L. Dong, W. Liang, and R. Wang, "Robust Text Image Tampering Localization via Forgery Traces Enhancement and Multiscale Attention," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3495–3507, Feb. 2024, doi: 10.1109/TCE.2024.3367947.

[59] M. Sirajudeen and R. Anitha, "Forgery document detection in information management system using cognitive techniques," Journal of Intelligent and Fuzzy Systems, vol. 39, no. 6, pp. 8057–8068, 2020, doi: 10.3233/JIFS-189128.

[60] Y. Y. Bae, D. J. Cho, and K. H. Jung, "A New Log-Transform Histogram Equalization Technique for Deep Learning-Based Document Forgery Detection," Symmetry, vol. 17, no. 3, Mar. 2025, doi: 10.3390/sym17030395.

[61] M. N. Chapel, M. Al-Ghadi, and J. C. Burie, "Authentication of Holograms with Mixed Patterns by Direct LBP Comparison," in 2023 IEEE 25th International Workshop on Multimedia Signal Processing, MMSP 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/MMSP59012.2023.10337669.

[62] N. Wang, L. Zhang, T. Jiang, and T. Shen, "Anti-tampering method of QR code hidden information based on deep learning," Signal, Image and Video Processing, vol. 19, no. 4, Apr. 2025, doi: 10.1007/s11760-025-03867-5.

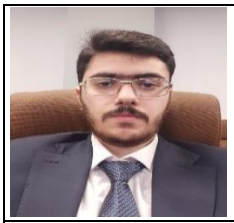
[63] N. J. Hamad, A. A. Abdulhameed, and M. H. Ali, "Enhancing Security and Efficiency through QR Integration with Hybrid AES-ECC Algorithm in Mobile Apps for Cardless Data Transactions," Al-Iraqia Journal for Scientific Engineering Research, vol. 2, no. 4, pp. 103–114, Dec. 2023, doi: 10.58564/ijser.2.4.2023.124.

[64] Kunekar, pankaj and Chandawar, Rachit and others, Optimizing Cryptographic and Image hashing for document verification (January 26, 2025). Proceedings of the International Conference on Innovative Computing & Communication (ICICC 2024), Available at SSRN: https://ssrn.com/abstract=5112131 or http://dx.doi.org/10.2139/ssrn.5112131.

[65] A. Diarra, T. F. Bissyande, and P. Poda, "Doc-Patch: An Unsupervised Approach for Documents Forgery Detection," in ACAI 2024 - 2024 7th International Conference on Algorithms, Computing and Artificial Intelligence, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ACAI63924.2024.10899704.

BIOGRAPHIES OF AUTHORS

The recommended number of authors is at least 2. One of them as a corresponding author.

	**Ibrahim F. Mohamed** completed a bachelor's degree in network engineering from Al-Iraqia University in Baghdad, Iraq, in 2018. Following graduation, worked full-time for four years at Zain Iraq, a leading telecommunications company. Currently, in the second year of research for Master of Science degree. Contact at Email: Ibrahim.F.mohamed@aliraqia.edu.iq
	Tayseer S. Atia is a professor at the department of computer engineering, Al Iraqia University, Iraq, where she has been a faculty member since 2012. From 2013-2014 she was the head of the computer engineering department. From 2014-2015 she was the dean's assistant for scientific affairs. Tayseer graduated with a first-class B.Sc. degree in computer science in 2004 and a M.Sc. in data security in 2007 from the University of Technology, Iraq. She completed her Ph.D. in computer science from Al Mosul University, Iraq. Her research interests are data security and artificial intelligence, especially computational intelligence techniques. She can be contacted Email: tayseer.salman@aliraqia.edu.iq