Journal of Legal Studies and Researches
e-ISSN: 2676-1688 p-ISSN:2437-1084
JLSR
Vol: 11 N°1, January 2026, p. 13–31

Electronic Forgery As a Manifestation of Digital Corruption

Khiari Rayane[1] *, Selmani Hayette[2]
[1] University of badji mokhtar, Annaba, ryane.khiari@univ-annaba.dz
https://orcid.org/0009-0009-5147-8446
[2] university of badji mokhtar, Annaba, hayet.selmani@univ-annaba.dz,
https://orcid.org/0009-0009-5371-7682

Received:24/07/2025 | *Accepted:26/09/2025* | *Published*: *15/01/2026*

Abstract:
This article examines the offense of cyber forgery as a major threat in the field of digital corruption. Cyber forgery demonstrates how technology can be used for illegal purposes, such as tampering with digital documents, hacking into systems, and falsifying data for illicit gain. These actions demonstrate that cyber forgery is not just a cyber crime, but an integral part of digital corruption, negatively impacting society and the economy as a whole. One of the main effects of cyber fraud is that it undermines trust in digital systems. This type of crime contributes to digital corruption by manipulating electronic processes and falsifying official documents.
Moreover, cyber forgery contributes to hampering efforts to achieve transparency and integrity in various institutions, whether governmental or private. By analyzing the impact of this crime, this article seeks to clarify the complex dimensions of cyber forgery and the importance of developing effective strategies to combat it and enhance digital security.

Keywords:
Digital corruption; electronic forgery; official documents; electronic signature.

**** Corresponding author***

1. INTRODUCTION

Some legal studies have observed that modern legislations, such as the Algerian anti-corruption law, have not merely reorganized classical offenses like embezzlement and abuse of office, but have also expanded the scope of criminalization to include new acts that were not previously addressed in the general Penal Code. This trend reflects a broader redefinition of what constitutes corrupt conduct.[1]

Such legal expansion allows for the inclusion of acts committed through modern technological means—such as electronic forgery—within the extended scope of corruption, particularly when perpetrated by public officials or for the purpose of obtaining unlawful advantage.

This type of forgery raises complex legal questions regarding its nature, its distinction from traditional forgery, and the extent to which it can be classified as a manifestation of digital corruption, especially as electronic documents and digital signatures become increasingly integrated into official transactions. These developments necessitate a reconsideration of classical legal definitions of criminalization and call for their expansion in light of technological change.

Accordingly, this research seeks to analyze electronic forgery as a form of digital corruption, by examining its legal components, identifying its manifestations, and focusing on the specific features of moral forgery committed through electronic means, as well as the legal treatment of electronic signatures within the framework of this offense.

The paper is structured around the following key axes:

Electronic forgery as an emerging form of digital corruption;

The constitutive legal elements of electronic forgery;

The technical manifestations of electronic forgery;

Moral forgery committed through technological means;

2. The Crime of Electronic Forgery

In this section, we will learn about the crime of electronic forgery, as we will review the nature of this crime, discuss its elements and characteristics, and discuss the methods of provingit. The first requirement: The first requirement: Definition of electronic forgery

2.1. Definition of Electronic Forgery

Forgery is generally defined as the fraudulent alteration of a document or record, potentially harming public or private interests. With the advancement of technology, this definition has become applicable to the forgery of data stored in computers. Traditional methods of physical forgery can also apply to electronic forgery. However, electronic forgeryis not limited to these methods alone; it is expanding with the advancement of technology [2]

Ali Abdul Qader Al-Qahouji defined electronic forgery as: “A change in the truth that results from…”Computer records, whether they are written paper outputs such as those produced by a printer or drawn by a plotter, and itis the same in the electronic document whether it iswritten in Arabic or any other language that has significance, and it maybe in paper outputs, provided that it is saved on a medium, and the condition is that the electronic document has an effect in proving a right or a legal effect.[3]
Some laws have addressed cybercrimes.

Several national legislations have addressed electronic forgery. The Egyptian Electronic Transactions Law of 2001 defines an "electronic document" as any statement recorded, stored, or transmitted via an electronic medium, and an "electronic signature" as symbols or letters that identify the signatory. Similarly, Jordanian lawmakers have introduced definitions of electronic records and signatures to include data that helps identify the signatory. The UK Forgery and Counterfeiting Act of 1981 broadened the scope of forgery to encompass electronic media such as magnetic disks and tapes.

The amended Iraqi Penal Code No. 111 of 1969 defines forgery as the deliberate alteration of truth in a document or instrument—by material or moral means—in a way that harms public or private interests. These legal definitions collectively demonstrate that electronic forgery may be based on electronic documents or signatures, especially in jurisdictions with dedicated cybercrime legislation.[4]

2.1.1 Elements of the Crime of Electronic Forgery

The crime of electronic forgery consists of two essential elements: material and mental. The material element involves altering the truth to distort relative legal reality, whether totally or partially, through a written lie. This may take the form of material forgery—such as manipulating electronic signatures using counterfeit software, breaking access codes, or exploiting information systems—or moral forgery, which includes fabricating obligations, agreements, or inserting false content into official documents prepared to receive data.[5]

Methods of physical forgery include scanning and inserting signatures or seals, forging personal photographs, copying software without a license, or creating fake digital documents attributed to false sources.[6]

Algerian law (Article 215) further defines moral forgery as altering notarized agreements, issuing false certificates, or deliberately changing declarations submitted to public officials. Such acts may cause actual or potential harm to legally protected interests, as seen in a case where a bank employee falsified account balances to enable fraudulent withdrawal.

On the other hand, the mental element requires general intent, awareness of the act of forgery, its illegality, and its potential consequences, and specific intent, which is the deliberate aim to use the forged document unlawfully. If the purpose is merely to joke or to showcase technical skills without intent to exploit the forgery, criminal liability does not apply.[7]

According to the information we have included regarding the crime of electronic forgery, information forgery can be considered a tool for digital corruption to achieve illegal goals as follows:

-Financial embezzlement: Information falsification can be used to falsify bank accounts or create fake invoices to steal money.

-Data manipulation: Individuals may alter data or modify digital facts in administrative systems to thei radvantage or that of third parties, there by compromising the integrity of digital systems.

-Identity theft: Facilitating financial fraud and money theft by manipulating personal data online.

Digital corruption relies heavily on the use of forgery to circumvent laws and ethical principles, such as:

-Concealing illegal transactions: By creating forged electronic documents that make fraudulent transactions appear legitimate, in order to conceal corruption.

-Forging electronic signatures: to sign contracts or agreements without the knowledge of the parties involved, enabling illegal transactions.

-Information fraud poses a real threat to trust in digital systems and institutions, undermining the principles of transparency and integrity the very essence of digital corruption. Prominent examples include:

- Electronic electoral fraud: Manipulating digital voting systems to change the results in favor of a particular party.
- Hacking government systems: Using forgery to gain illicit benefits by manipulating government data.

2.1.2. Characteristics of the Crime of Electronic Forgery

Electronic forgery is a highly serious form of cybercrime, particularly when it involves official documents issued by authorized personnel, as this undermines public trust in institutional credibility. This crime exhibits several distinctive characteristics:

- Flexibility of execution: It can be committed at any stage of a digital system’s operation during input (e.g., inserting false data or omitting key information), processing (e.g., manipulating software for unlawful purposes), or output (e.g., altering system-generated results like academic grades).

- Lack of physical evidence: Unlike traditional forgery, electronic forgery leaves no visible traces on the document, making it a technically sophisticated and covert offense.
- Specific offender profile: Perpetrators often possess advanced IT skills and may act out of personal motives such as curiosity, entertainment, or to expose system vulnerabilities. For instance, a group of hackers forged ATM cards to demonstrate flaws in a bank's security system[8] .

When viewed through the lens of the United Nations Convention against Corruption, electronic forgery emerges as a direct threat to principles of integrity, transparency, and accountability. It aligns with various forms of corruption that the Convention seeks to prevent, especially those involving abuse of power in both public and private institutions.

2.2. Evidence of Electronic Forgery

Evidence of electronic forgery is grounded in evolving legal definitions and modern scientific methods. The Iraqi Electronic Signature Law No. 78 of 2012 defines electronic writing as any symbol, number, or character affixed to a digital or similar medium that conveys intelligible meaning, while the Egyptian Law No. 15 of 2004 describes an electronic document as a data message created, stored, or transmitted electronically. Egyptian jurisprudence further expands the definition of a document to any meaningful, stable, and attributable text capable of creating legal effect.

However, the growing reliance on digital technologies has exposed gaps in traditional penal codes, which often fail to capture the realities of cyber forgery. Legislators are therefore urged either to explicitly criminalize such acts or to interpret existing provisions carefully without violating the principle of legality. In contrast to many Arab legislations that enumerate forgery methods, French law, under Article 441, defines forgery broadly as any fraudulent alteration of the truth causing harm, regardless of method[9]

This generality allows French law to encompass both traditional and modern forms of forgery including digital data, magnetic storage, and

computer-generated documents thus reflecting a shift from classical penal principles to the domain of information criminal law , Some scholars even advocate for admitting scientific evidence under the rules governing information crimes, given the absence of any legal prohibition.

In essence, proving electronic forgery now relies heavily on technologically advanced methods, but it remains crucial that such evidence be gathered in accordance with procedural legality, This framework helps address legislative shortcomings, prevents offenders from exploiting legal loopholes, and ensures effective punishment for emerging digital forgery crimes.[10]

3. Types of Electronic Forgery

In this section, we will address various types of electronic forgery, focusing on those we consider most closely associatedwith corruption: forgery of official documents and forgery of electronic signatures. This study will demonstrate how the digital space can be exploited to forge documents and data, and the consequent impact this has on the credibility of official documents.

3.1. Forgery Involving Electronic Documents

In this section, we will address the forgery of electronic documents, focusing on official electronic documents. Tampering with these documents is closely linked to corruption, as it has negative effects on legal and administrative integrity.

3.1.1 Electronic Document as a Site for Information Forgery

a. Definition of Electronic Document

The electronic document is considered one of the most important elements relied upon to embody the concept of e-administration that has emerged from the digital society.

Under the UNCITRAL Model Law, an electronic document is defined in Article 2, paragraph (a), as "data message," meaning information generated, transmitted, received, or stored by electronic, optical, or similar means.

Such means include, for example, electronic data interchange (EDI), electronic mail, telegram, facsimile, or telecopy. Examining the text of this

article, we find that the term "data message" has been used instead of "electronic document" due to the variety of means by which this type of document is processed.

As for the French legislator, he did not define the electronic document, but rather simply defined writing as one of the components of the document, despite the significant difference between the writing included in the electronic document and the document itself, which is an electronic medium, whether official or customary. Meanwhile, the Egyptian legislator defined the electronic document in the Electronic Signature Law as "a message containing information created, incorporated, stored, sent, or received, in whole or in part, by electronic, digital, optical, or any similar means."[11]

The Algerian legislator defined electronic writin gunder Article 323 bis of Law 05-10 amending and supplementing the Civil Code, as: “A sequence of letters, descriptions, numbers, or anysigns or symbols with an understandable meaning, regardless of the means by which they are contained and the methods of sending them. It is noted that the Algerian legislator has kept pace with its French counterpart, as electronic writing was not limited to the traditional concept of writing as a group of letters, but rather added to it everything that conveys a meaning agreed upon between the parties, from descriptions, numbers, signs, or symbols, and also added a phrase by anymeans and regardless of the method of sending it.[12]

b. Elements of the Crime of Forgery in Electronic Documents

The crime of electronic forgery is based on two elements:
a material element that includes changing the truth in a document in one of the ways specified by law, and that this change results in harm to others, and a mental element that includes the general intent that is represented by the perpetrator’s knowledge of the act of changing the truth in the document, and the special criminal intent that means combining knowledge with the intent to deceive, i.e. the intent to use the forged document with the intent of achieving unlawful objectives.

Under French law, the crime of forgery in the field of electronic documents has become the same elements as the crime of forgery in ordinary paper documents, so the subject of forgery includes the document on a paper medium or anyother medium, and of course also includes the electronic medium.

French law made an important change related to not specifying the methods of forgery (such as methods of changing the truth), so the methods of forgery are no longer mentioned exclusively and specifically as was previously. The French legislator defined forgery in the text of Article 1/141 of the new Penal Code as: "Forgery is considered any change by fraud in the truth, which is likely to cause harm, whatever it maybe."

The method by which it is conducted, in a document or in anyother medium, expresses an idea that aims or may result in evidence proving a right or fact with legal effects.

The crime of forgery in electronic documents is no different from other crimes, as it is based on two elements: a material element and a mental element.[13]

3.1.2. Forgery Involving Official Documents

Forgery involving public or official documents stipulated and punishable in Articles 214 to 216, in addition to the common elements of all forms of forgery, requires that the forgery be committed against a public or official document and that the forgery be carried out by one of the material or moral means specified in Articles 214 to 216 of the Algerian Penal Code.

In order to be considered an official document, this document must include three conditions: capacity, jurisdiction, and form. In addition to that, the document must be issued by the state or one of the public legal persons, and it must be recorded in accordance with the conditions and procedures specified by law.

The state, as a public legal person, is assisted in performing its duties by a group of people who express of its own free will, and they have the capacity to represent it, and these persons are public employees and the documents issued by them have an official character, and accordingly the

document must be issued by a public employee who is competent to issue the document in terms of subject or place, and by implication the documents issued by someoneo ther than a public employee are not considered official documents, and an example of this is the documents issued by companies or banks of various types that are not considered official documents, nor are they considered customary documents.

As for the second element of the official document, it must be recorded in accordance with the conditions and procedures specified by the laws and regulations, and accordingly the document is considered official[14].

Official documents, such as those issued by public officials or government agencies, are among the most vulnerable to forgery. Any tampering with these documents constitutes a violation of public trust and poses a threat to the entire legal system. Thus, forgery of electronic documents represents one of the most prominent forms of digital corruption, where modern technologies are exploited for illegal purposes. Digital corruption in this context includes the unlawful manipulation of data and official documents circulated electronically, compromising the integrity of the digital system and fostering an environment of opacity and legal violations. This type of corruption undermines trust in digital systems and negatively impacts the fairness and reliability of electronic transactions.

- Legal conditions for official electronic documents:

Given the legal and practical importance of official electronic documents, Egyptian and French legislation has set general and specific conditions to ensure their reliability and maintain their official character, while taking into account their non-material nature.

a) General Conditions: The general conditions for electronic documents are the same as those for traditional documents, subject to modifications that ensure their compatibility with the electronic environment:

- Issuance of the editor by a public employee or public body:

The document must be issued by a public employee, public officer, or person charged with a public service.[15]

Some legal analyses have noted that corruption-related offenses are frequently committed by public officials in connection with their duties, especially when they exploit their position to manipulate official documents. This understanding aligns with the broad definition of a "public official" as set forth in the United Nations Convention against Corruption, which includes any person holding a legislative, executive, administrative, or judicial office.

In such cases, the electronic forgery of official documents whether through unauthorized alterations, false certifications, or digital impersonation can be considered not just a cybercrime, but a modern extension of traditional corruption practices. These acts are often fueled by a combination of psychological factors (such as weak ethical conscience, opportunism, or personal frustration), economic motivations (like financial hardship, job insecurity, or the pursuit of illicit gain), and educational shortcomings, where a lower level of legal awareness or professional training increases vulnerability to engaging in such misconduct.[16]

Documents issued electronically by ministries or departments, and certificates issued by public bodies, such as the Information Technology Industry Development Agency, are considered official.

- Issuance of the editor by a competent authority in terms of place, time and subject:

Documents must be issued by a legally competent body or employee, within the legally defined spatial and temporal scope. Example: Certificates issued by the Information Technology Industry Development Agency must be directed to a specific person and for the appropriate period of time.[17]

- Taking into account the legal conditions in writing the editor:

These conditions include the signature of the parties and witnesses (if any), the signature of the public officer, verification of the identity of the parties, and ensuring the legibility of the writing.

These procedures are implemented electronically, with the exception of the presence of witnesses, which the French legislator considers to be specific to traditional documents.

b) Special conditions: The special conditions relate to technical controls that take in to account the electronic nature of official documents, as stipulated by the Egyptian legislator in Executive Regulations No. 109 of 2005.

-Proof of creation time and date: It must be technically possible to determine the time and date of creation of electronic documents.

This is done through an independent electronic filing system that is not subject to the control of the editor's creator.

- Identify the source of creation: The source of the electronic editor, the degree of control the creator had over the source, and the media used to createit must be identified.[18]

- The status of the perpetrator in the crime of forgery of official or public documents :

Forgery of official or public documents maybe committed by a public employee or someone considered to be in a similar position, as well as by ordinary individuals, as we will explain in the following points:

- The status of a public employee or someone in a similar position:

According to Articles 214 and 215 of the Algerian Penal Code, the crime of forgery of official or public documents requires the perpetrator to have a specific qualification, namely that he be a public employee or of equivalent standing.

It is clear from these two articles that the basic element in the crime of forgery of official documents is the job title of the perpetrator, such that:

- A judge in ordinary, administrative, or military courts.
- A person who performs a public service under the laws and authorization of a state, such as notaries, court bailiffs, or translators..

In the General Basic Law of the Civil Service (Article 4), a public employee is defined as any employee who holds a permanent public position and is appointed to the administrative hierarchy.

In the Penal Code (Law 06-01 on the Prevention and Combating of Corruption), the definition of a public employee has been expanded to include:

o Any person holding a legislative, executive, administrative, or judicial office, whether elected or appointed, permanent or temporary, paid or unpaid, regardless of rank or seniority.

o Any person who holds a temporary position or agency, with or without pay, and contributes in this capacity to the service of a public body or institution, or an institution in which the state owns all or part of its capital, or which provides a public service.

o Every person who is considered a public official or equivalent in accordance with applicable laws and regulations, based on Article 2 (paragraph a) of the United Nations Convention against Corruption (October 31, 2003).[19]

- Forgery committed by committed by someone other than an employee or someone in his position

Article 216 of the Algerian Penal Code stipulates that any person, with the exception of the categories specified in Article 215, who commits forgery in public or official documents using one of the following means shall be punished:

o Imitation or forgery of a writing or signature.

o Forging agreements, texts, commitments or releases by later including them in those documents.

o Adding, deleting, or falsifying the terms, statements, or facts that these documents were prepared to document or prove.

o Impersonating or claiming to be someoneelse.

Article 212 of the Egyptian Penal Code stipulates that any person who is not a public employee who commits forgery as described in the previous article shall be punished by imprisonment with hard labor or imprisonment for a period of up to ten years.

A non-public employee is anyone who does not belong to the category of public servants. Therefore, an ordinary individual is considered to have committed the crime of forgery in an official document, and an official is also considered to have committed the crime of forgery if the act falls outside the scope of his or her authority and the document is obtained illegally.

All of these methods include material or moral forgery. Although the apparent text of Article 216 indicates that it applies only to ordinary individuals, not to public employees or those in a similar position, it does not, in fact, apply to employees or those in a similar position if the forgery occurs during the performance of their duties. Rather, it applies in other cases.[20]

In conclusion, we can highlight that forgery of official documents, whether committed by a public official or a privateindividual, is a serious violation of the credibility of official documents and the transparency of administrative processes. This type of crime is a key tool for promoting corrupt practices, whether through falsifying facts, facilitating the misappropriation of public funds, or manipulating administrative and legal transactions.

In the digital age, electronic forgery of official documents constitutes a significant development in this type of crime, where by advanced technological means are employed to create fake documents or modify original documents in a way that undermines their authenticity. Thus, electronicforgery of official documents can be considered a type of "digital corruption," presenting a new challenge for governments and institutions as they seek to promote integrity and combat corruption in an increasingly digital enabled environment.

3.2. Electronic Signature Forgery

Electronic signature forgery differs fundamentally from traditional signature forgery. While traditional forgery involves imitating someone's handwritten signature usually producing an inexact replica electronic signature forgery occurs when an unauthorized person gains access to another's electronic signature system (through hacking, spying, or similar means) and uses it to sign documents. In such cases, the signature appears valid, yet it was executed without the consent of the rightful owner.

Unlike traditional forgery, which can be detected by comparing signatures, detecting electronic forgery requires proving that the legitimate owner did not authorize the signature and identifying the person who misused the system. Due to these complexities, the UNCITRAL Model Law on Electronic Signatures has emphasized the reliability of electronic signature systems and set out conditions for their legal validity, including secure linkage to their owner at the time of use.

If any of these legal pillars are missing, the signature is not considered reliable. This Model Law has influenced all electronic signature laws worldwide, forming the basis for consistent legal standards regarding the authenticity and reliability of electronic signatures.[21]

- Characteristics of the crime of electronic signature forgery:

The crime of electronic signature forgery possesses distinct characteristics that set it apart from traditional forgery, as it takes place in a virtual environment using advanced technological methods. It is often linked to theft and hacking, since electronic signatures rely on encrypted identifiers like magnetic card codes or biometric traits (e.g., fingerprints or iris scans), which can be compromised through data breaches, decryption, or online attacks—as in the 2004 breach involving eight million cards, where website flooding was used to extract sensitive information. Unlike handwritten signatures, electronic signatures leave no physical trace, making them harder to detect and requiring technical expertise to forge.[22]

This crime represents a form of digital corruption, as it involves manipulating electronic systems and data for unlawful gain. It mirrors other corrupt practices in the digital realm by undermining trust, enabling fraud, and contributing to broader legal and economic instability.

4. CONCLUSION

In conclusion, cyber fraud represents one of the most prominent forms of digital corruption, undermining the integrity of digital systems and threatening the stability of institutions. It is imperative to intensify efforts to update national and international legislation and adopt advanced technologies to combat this type of crime.

By enhancing cooperation between the government and private sectors and providing specialized training, we can ensure effective countermeasures against cyber fraud, there by enhancing transparency and integrity in digital transactions and protecting the national economy.

Recommendations:

- The crime of electronic forgery must be clearly included in anticorruption laws, given that this crime directly impacts the integrity of digital transactions and facilitates corruption in the government and financial sectors. Electronic forgery involves the manipulation of data and documents via digital systems, facilitating financial fraud, administrative corruption, and money laundering, there by undermining the foundations of justice and transparency.
- Traditional anti-corruption laws, which lack clear provisions to address cybercrime, must be reconsidered. Legislation must be updated to include specific aspects related to digital crimes, particularly those related to the forgery of official documents and papers. With on going technological developments, crimes such as cybercrime have become more complex, requiring specialized laws that keep pace with digital advancements and effectively combat this type of corruption.
- Strict oversight must be imposed on digital systems used in financial and administrative transactions, with technologies such as blockchain being used to verify the authenticity of digital data and documents. Electronic

forgery opens the door to digital corruption in financial and administrative institutions, where individual scan manipulate data to alter transaction outcomes or transfer funds illegally.

- Investigations into digital corruption crimes should include measures to verify cyber fraud at all levels of corruption, by examining digital transactions and falsified data used in other corrupt activities.Electronic forgery is not an independent crime, but is closely linked to many otherforms of corruption, such as financial and administrative corruption, and bribery, which require sintegrated investigation and punishment mechanisms.
- Strengthening international cooperation to combat cybercrime and digital corruption. International agreements to combat cybercrime, such as the Budapest Convention on Cybercrime, should be activated, and information exchange between countries should been couraged to prosecute those involved in digital corruption.

Given the cross-border nature of digital crimes, international cooperationis essential to uncovering digital corruption and cybercrime networks that may extend across multiple countries.

5.Endnotes

[1] Dokhan, Amal (2021), Expanding the Criminalization of Acts of Corruption According to the Law on the Prevention and Combating of Corruption, Journal of Legal Studies and Research, Vol. 6, No. 2, P. 250

[2] Foraqd Aboud Al Ardi (2012), The Crime of Electronic Forgery: A Comparative Study, Al Kufa Journal of Legal and Political Sciences, Vol. 13 (31), March, P. 54

[3] Barhoum Al Tahir, The Crime of Electronic Forgery, a Thesis Submitted as Part of the Requirements for a Master's Degree, Faculty of Law and Political Science, Arbi Tebessi University, Algeria, 2019, P. 18.

[4] Foraq dAboud Al Ardi, The Crime of Electronic ForgeryP55

[5] Ghallab Abdel Haq (2022), The Specificity of the Crime of Forgery of Electronic Signatures in Algerian Legislation, Journal of Legal and Political Studies, Vol. 8, No. 1, January, P. 501.

[6] Adel Al Mustari, Arwahana Zuleikha, The Crime of Electronic Forgery, Journal of Human Sciences, University of Mohamed Khider Biskra, Issue 46, P. 301

[7] Ramzi Bin Al Siddiq (2018), Forgery Involving Electronic Documents Between the Possibility of Being Subject to Traditional Rules and the Necessity of Respecting Privacy, Al-Ijtihad Journal of Legal and Economic Studies, Vol. 7, No. 2, PP. 213–214.

[8] Omar Abdel Salam Hussein Al Jabouri, The Crime of Electronic Forgery in Jordanian Legislation, Master's Thesis, Faculty of Law, Middle East University, Jordan, 2017, P 24

[9] Kahwaji Ali Abdel Qader (1992), Criminal Protection of Computer Programs, Journal of Law for Legal and Economic Research, Faculty of Law, Alexandria University, P. 63.

[10] Saddam Hussein Yassin Al Obaidi (2020), Provisions on Penalties for Traditional and Electronic Forgery in Islamic Jurisprudence and Positive Law, Arab Center for Publishing and Distribution, Egypt, First Edition, P. 304

[11] Khalifi Fatiha (2022), Information Forgery in the Digital Environment, Journal of Legal Studies, Vol. 8, No. 2, June, PP. 261–262.

[12] Alli Rahal, The Evidence of Electronic Documents in Proof in Light of Algerian and Comparative Legislation, Tabna Journal of Academic Scientific Studies, Vol. 4, No. 2, P. 299

[13] Abdullah Belkacem (2020), The Special Nature of the Crime of Forgery in Electronic Documents, Journal of Comparative Legal Studies, Vol. 6, No. 2, P. 985.

[14] Ben Sheikh Walid, The Impact of the Crime of Forgery on Electronic Contracting, Master's Thesis, Faculty of Law, Al Basheer Al Ibrahimi University, Algeria, 2022, P. 33.

[15] Bourbaba Soria (2016), The Evidential Authority of Electronic Documents, The National Forum on the Legal Framework for Electronic Signatures and Certification in Algeria, Faculty of Law and Political Science, Mohamed Cherif Messaadia University, Algeria, January 12–13, P. 3

[16] Nabil Melekia (2020), The Causes and Risks of Occupational Corruption, Journal of Legal Studies and Research, Vol. 7, No. 1, PP. 236–237.

[17] Bourbaba Soria, the evidential authority of electronic documents, P 3

[18] Iman Bounaser, El Hadi Khadrawi (2018), Legal and Technical Developments in the Organization of Official Electronic Documents, Journal of Legal and Political Research, No. 11, December, P. 470

[19] Wafaa Sadrati, Mechanisms for Combating the Crime of Electronic Forgery, Doctoral Thesis in Criminal Law, Faculty of Law, University of Arbi Tebessi, Algeria, 2021, P. 101

[20] Sherif El Tabbakh (2006), Forgery and Counterfeiting in the Light of Islamic Jurisprudence and the Judiciary, Second Edition, National Center for Legal Publications, Egypt, P. 36

[21] Munir Muhammad Al Janbihi, Mamdouh Muhammad Al Janbihi (2006), Forgery of Electronic Signature, Dar Al-Fikr Al-Jami'i, Alexandria, PP. 55–56

[22] Omar Abdel Salam Hussein Al-Jabouri, The Crime of Electronic Forgery in Jordanian Legislation P.85.