SCIENTIFIC CULTURE

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 12467-12480
Open Access. Online & Print

DOI: 10.5281/zenodo.12212026954
www.sci-cult.com

THE IMPACT OF DEEPFAKE TECHNOLOGY ON THE AUTHENTICITY OF VISUAL EVIDENCE IN FORENSIC EVIDENCE IN THE SAUDI EVIDENCE LAW

[1]*Aidan-Shaikha Hamad Al

[1]Assistant Professor of Criminal Law **Taif University**

Abstract

This research examines the impact of deepfake technology on the authenticity of visual evidence in forensic evidence, in light of the rapid development of artificial intelligence applications and the resulting advanced ability to produce manipulated visual content with a high degree of realism, which raises legal and technical challenges that affect the reliability and technical integrity of visual evidence. The research aims to explain the concept of deepfakes, the mechanisms of its creation and detection, and to analyze its impact on the evidentiary value of visual evidence, while studying the position of the Saudi Evidence System on digital and visual evidence affected by deepfake techniques.

The research relied on the descriptive-analytical approach in addition to the comparative method, by reviewing the technical aspects of deepfake manipulation, analyzing the statutory texts, and jurisprudential and judicial trends related to the authenticity of visual evidence, with a focus on the provisions of the Saudi Evidence Law and the use of some relevant judicial applications and rulings. The research found that deepfakes are no longer just a technical challenge, but a real threat to the reliability of visual evidence in the criminal field, which has weakened the traditional assumption based on the association of the image with reality, and highlighted the need for technical verification of the technical integrity of visual content before considering its evidentiary value. The results also showed that traditional controls for the admissibility of evidence alone may not be sufficient to counter highly complex artificial visual evidence, necessitating the development of more specialized technical and procedural mechanisms for verifying the authenticity and technical integrity of visual evidence.

The research concluded with a set of recommendations, the most important of which are the development of statutory and technical controls for visual evidence affected by artificial intelligence technologies, enhancing the integration between technical expertise and judicial authorities, adopting standardized protocols to detect deepfakes, in addition to supporting the training of specialists in investigation agencies and developing mechanisms to verify the technical integrity of visual content in criminal cases.

Keywords: Deepfake Technology, Visual Evidence, Forensic Evidence, Artificial Intelligence, Digital Evidence, Saudi Evidence law**.**

Introduction

In recent years, the world has witnessed an accelerated development in artificial intelligence technologies, one of the most prominent applications of which is known as deepfake, a technology that relies on deep learning algorithms to produce or modify visual or audio content in a way that makes it difficult to distinguish it from real content. This technological development has led to the emergence of contemporary legal challenges, especially in the field of forensic evidence, where visual evidence – such as video recordings and digital images – has become one of the most important means of proof that the judiciary relies on in revealing the truth and proving criminal facts. The digital revolution has contributed to the reliance on visual evidence as an effective means of proving crimes, due to its ability to document facts and events directly. However, the advent of deepfakes has cast doubt on the reliability of this evidence, as it has become possible to manipulate visual content or fabricate it in an elaborate way that is difficult to detect by traditional means, which raises fundamental questions about the authenticity of visual evidence in light of these modern technologies, and the extent to which legal systems are able to deal with these technical challenges. In this context, the issue of the authenticity of visual evidence is of particular importance in the Saudi Law, especially in light of the legislative development witnessed in the field of evidence with the issuance of the Evidence Law, which recognized the digital evidence and granted it the same evidentiary value as written proof when the necessary legal conditions for its admissibility were met. However, the rapid development of deepfake techniques poses new challenges that may affect the reliability of visual evidence, which necessitates studying the impact of these techniques on the evidentiary value of visual evidence in forensic evidence, and demonstrating the adequacy of existing statutory rules to address this problem. Hence, this study examines the impact of deepfake manipulation on the authenticity of visual

evidence in the Saudi Law, through the analysis of the statutory framework for proof, and the challenges that these modern technologies impose on the reliability of visual evidence, while trying to clarify ways to deal with this problem in a way that achieves a balance between technical development and the requirements of criminal justice.

Research Problem

The problem with this research is that the technical development in the field of artificial intelligence has provided unprecedented possibilities for the manipulation of visual content through deepfake techniques, which raises a real challenge to the forensic system that increasingly relies on digital and visual evidence to uncover the truth. In light of the systematic recognition of digital evidence in the Saudi Law and granting it evidentiary value in proof, fundamental questions arise about the extent to which these technologies affect the reliability of visual evidence, and to what extent The judiciary can rely on it as it can be manipulated using deepfake technology.

Accordingly, the problem of the research is the following main question:

To what extent does deepfake technology affect the authenticity of visual evidence in forensic evidence in the Saudi Law?

:questions-This question is divided into a number of sub

.1 What is deepfake technology, and what are its ?most prominent technical characteristics

.2 What is the legal basis for the admissibilityof vidence in thevisual evidence in forensic eSaudi Law?

.3 How much impact do deepfake techniques have on the reliability of evidence seen before criminal courts.

4. What legal and technical mechanisms can reduce the risk of deepfakes and enhance reliability of visual evidence?

The importance of the research

The importance of this research is manifested in several :aspects, most notably

1. Scientific Significance: The research contributes to addressing a contemporary legal problem related to the logies on the impact of artificial intelligence techno .means of forensic evidence

2. Practical Importance: Helps clarify the challenges facing the judiciary in evaluating visual evidence in light of the possibility of manipulation using deepfake techniques.

3. Regulatory Importance: Highlights the adequacy of the statutory rules in the Saudi Law to deal with these modern technologies, and the need to develop legal frameworks regulating digital evidence.

Research Objectives

:This research aims to achieve the following

1. and its technical Explain the concept of deepfakes characteristics.

2. Analysis of the Authenticity of Visual Evidence in Forensic Evidence in the Saudi System.

3. To study the impact of deepfake techniques on the reliability of visual evidence.

4. Highlight the most important legal and technical means that can enhance reliability of visual evidence in the face of deepfakes.

Research Methodology

This research relies on the descriptive-analytical approach, in addition to the comparative method, by reviewing the technical aspects of deepfake manipulation and analyzing the statutory texts related to forensic evidence in the Saudi Law and comparing them with jurisprudential and judicial trends related to the authenticity of digital evidence, with the help of some relevant applications and judicial rulings, to show the impact of deepfake manipulation on the technical integrity of digital evidence and its evidentiary value in the criminal field**.**

Previous Studies

Recent years have seen a growing academic interest in the study of deepfake techniques and their implications in multiple fields, especially with the rapid development of artificial intelligence technologies and the resulting challenges related to the reliability of digital content and visual evidence. Many studies have dealt with this subject from various technical and legal aspects, the most prominent of which are the following:

Michael Westerlund's 2019 study, "The Emergence of Deepfake Technology: A Review", examined the evolution of deepfake technology and its implications for the media and society, highlighting the risks associated with the misuse of manipulated digital content and its impact on trust in information and digital media.

Ruben Tolosana et al.'s 2020 study, "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection," presented an analytical presentation of face manipulation methods and deepfakes detection methods, highlighting the most prominent technical challenges facing detection tools as a result of the continuous development of artificial intelligence algorithms. On the legal side, Danielle Keats Citron and Robert Chesney's 2019 study "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" discussed the legal and security risks associated with deepfakes, particularly in relation to disinformation, invasion of privacy, and the impact of technology on trust in digital content. Matthew Freeman's study , "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," published in 2024, examined the impact of deepfakes on the criminal justice system and discussed the challenges that investigators and courts may face in verifying the admissibility and reliability of digital evidence as deepfake technologies evolve. In the Arab context, Rabab Mustafa Al-Hakim's study "The Legal Aspects of Deepfakes" addressed the legal problems associated with this technique and discussed the adequacy of traditional legal rules in the face of crimes

arising from the use of deepfakes. Despite the importance of the previous studies and the technical and legal treatment they provided, most of them dealt with the subject either from the technical aspect related to the mechanisms of creation and detection, or from the perspective of general legal risks, without focusing in a specialized way on the impact of deepfakes on the authenticity of digital evidence in criminal evidence in light of the Saudi Law. Hence the importance of the current research in combining the technical and legal aspects, and analyzing the impact of deepfakes on the integrity and evidentiary value of digital evidence. Examine the position of the Saudi evidence system on this evidence and indicate the adequacy of the legal and technical controls to confront the risks of deepfake manipulation in the criminal field.

Research Plan

The nature of the research necessitated its division into two main topics, as follows:

First Topic: What is Deepfake Tehcnologyand the Authenticity of Visual Evidence in Forensic Evidence

- The First Requirement: The Concept of Deepfakes
- The Second Requirement: What is Visual Evidence and Its Authenticity in Criminal Evidence in the Saudi Law

Second Topic: The Impact of Deepfake Technology on the Authenticity of Visual Evidence and Ways to Counter It

- The first requirement: The effect of deepfakes on .lity of visual evidencethe reliabi
- Second Requirement: Technical and Statutory Mechanisms to Enhance the Authenticity of Visual Evidence in the Face of Deepfakes

The first topic

What is Deepfake Technology and the Authenticity of Visual Evidence in Forensic Evidence

Introduction

Recent years have witnessed an accelerated development in artificial intelligence technologies, one of the most prominent applications of which is the deepfake technology, which enables the production or modification of visual or audio content with a high degree of realism that makes it difficult to distinguish between real and artificial. This development has created fundamental challenges for forensic systems, especially with regard to the authenticity of visual evidence, which necessitates verifying the credibility of this evidence before it can be relied on judicially. Accordingly, this topic deals with the concept of deepfakes and its technical characteristics. The concept of the authenticity of visual evidence in criminal evidence in the Saudi Law is then presented, in preparation for examining the impact of this technology on the reliability of evidence before the judiciary, which we address in two demands:

The First Requirement: The Concept of Deepfakes

The Second Requirement: What is Visual Evidence and Its Authenticity in Criminal Evidence in the Saudi Law

The first requirement

The Concept of Deepfakes

First: Definition of Deepfakes

The term "deepfake" is a relatively recent term in the technical literature, and it arose as a result of the combination of the words "deep" in reference to deep learning techniques, and "fake" in the sense of fake. The term is used to refer to digital media that are generated or modified using artificial intelligence technologies, particularly multi-layered neural networks, resulting in the production of visual or audio content that looks too realistic to be distinguished from real content.

Definitions of deepfakes in the scientific literature have varied according to the different angles that have dealt with this phenomenon, as it is defined as media that is composite or modified using artificial intelligence techniques so that it is difficult to distinguish it from the real original[1], and it is defined as a form of facial manipulation based on deep learning techniques to create high-realistic artificial visual content[2]. In another definition, it is seen as artificial media – such as images, videos, and audio recordings – that are produced using generative AI tools Based on machine learning models trained on huge datasets[3].

Another trend is to define deepfakes as a method of using artificial intelligence to manipulate images, videos, and audio recordings to create new content that looks real despite being unrealistic[4]. It is clear from the sum of these definitions that the concept encompasses two main types: manipulation of existing media, or the generation of entirely new media, using models capable of simulating human patterns with a high degree of accuracy[5].

Deepfakes are not just traditional technical editing, but are advanced digital simulations of human reality,

[1] Enes Altuncu, Virginia N. L. Franqueira, and Shujun Li, "Deepfake: Definitions, Performance Metrics and Standards, Datasets and Benchmarks, and a Meta-Review," arXiv preprint arXiv:2208.10913 (2022), at 1.

[2] Ruben Tolosana et al., "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection," Information Fusion 64 (2020): 131–148, at 132.

[3] Ebba Lundberg and Peter Mozelius, "The Potential Effects of Deepfakes on News Media and Entertainment," AI & Society 40, no. 4 (2025): 2159–2170, at 2159.

[4] Hakim, "The Legal Aspects of -Rabab Mustafa Al Deepfakes", Journal of Jurisprudential and Legal Research, Vol. 48 (2025): 2680

[5] Altuncu et al., "Deepfake," at 1.

capable of reproducing physical, vocal, and behavioral features with a high degree of persuasiveness, by training AI models on real data. This raises fundamental problems in the field of forensic evidence, especially with regard to the authenticity of visual evidence and its judicial admissibility.

Second: Characteristics of Deepfakes

Deepfakes have a number of technical characteristics that make it qualitatively different from other forms of traditional digital content, as it is not limited to superficial modification of media, but is based on reconstructing content using deep learning models. One of the most prominent of these high-realities is that models based on generative neural networks produce visual and auditory content with an advanced degree of persuasiveness, making it difficult for even experienced users to distinguish between real and fake[6].

Deepfakes are also characterized by the dual ability to manipulate and generate, as it can be used to modify existing media by replacing faces or voices, or to generate entirely new content that did not actually happen, reflecting a transition from "media editing" to "digital reality manufacturing" [7] and is closely related to its intrinsic reliance on artificial intelligence technologies, particularly adversarial generative network models (GANs), which train two competing models to produce data that mimics human patterns with high accuracy [8].

In addition, deepfakes are highly reproducible and modifiable, as the same content can be reproduced in multiple formats with varying changes with relative ease, due to its reliance on retrainable and continuously improved models[9] . This gives it a dynamic and renewed character that makes it more difficult to adjust or validate.

Taken together, these characteristics not only reflect a technological development in media processing, but also establish a fundamental shift in the nature of digital content, raising profound legal challenges related to its admissibility and reliability, especially in light of the difficulty of verifying its source and integrity.

Deepfakes have several basic characteristics that distinguish it from any other digital content, the most prominent of which are:

.1 Realism: The resulting content appears to be visually and audibly real, making it difficult for the average viewer to distinguish it from the original.

2. Ability to manipulate existing media or generate new media: Modify pre-existing content or create content that didn't exist before.

.3 Artificial Intelligence and Deep Learning: Uses deep learning models such as generative neural networks (GANs).to achieve accurate realism

4. Repeatability and editability: Multiple copies of the same content can be easily produced with minor or significant changes.

The second requirement

What is Visual Evidence and Its Authenticity in Criminal Evidence in the Saudi Law

First: What is the Visual Evidence

When looking for the definition of visual evidence in the Saudi Law and legal references, we find that it is often included in the concept of digital evidence. Digital evidence is defined as any digital data that can be submitted before the court to prove a fact, whether it is photos, video recordings, electronic documents, or others. In this sense, visual evidence is considered one of the types of digital evidence, and it is subject to the same conditions of evidentiary value, especially proving the authenticity and technical integrity before it is admitted before the court.

The Saudi legislator has defined digital evidence, which is any evidence derived from data that is created, issued, received, preserved or communicated by a digital means, and can be retrieved or obtained in an understandable manner[10]. In other words, digital evidence includes any digital data that can be presented and understood before judiciary as a means of proving a fact, including visual evidence.

Visual evidence is also defined as legal evidence based on sight and observation, and is extracted from fixed electronic means, whether it is images, animated videos, or text flashes, such as messages, mobile phones, or various smart applications.[11]

Modern jurisprudence defines visual evidence as any digital images or video recordings used to prove the events of a dispute before the courts, provided that the conditions of documentation and authenticity are met, and that it is a correct representation of the facts it claims to present. This concept is used in the legal analysis of digital evidence, especially in cybercrime and violent crimes recorded by video[12].

Visual evidence is classified as digital evidence, which has multiple images according to the nature of the data it contains, it may be visual such as video recordings, audio recordings such as audio recordings, or digital

[6] Tolosana et al., "Deepfakes and Beyond," at 3.

[7] Michael Westerlund, "The Emergence of Deepfake Technology: A Review," Technology Innovation Management Review 9, no. 11 (2019): 39–52, at 41.

[8] Ian Goodfellow et al., "Generative Adversarial Nets," in Advances in Neural Information Processing Systems, vol. 27 (2014): 2672–2680, at 2.

[9] Johan Kietzmann et al., "Deepfakes: Trick or Treat?" Business Horizons 63, no. 2 (2020): 135–146, at 137

[10] Article 53 of the Saudi Evidence Law promulgated by Royal Decree No. (M/43) dated 26/5/1443 AH

[11] Sarah Moussa Odeh, "Electronic Video Recordings and Their Authenticity in Jordanian Criminal Evidence", Jerash for Research and Studies, Volume Volume 2, (2025): 916 ,25

[12] Jonathan W. Hak, Image-Based Evidence in International Criminal Prosecutions (Oxford: Oxford University Press, 2024), at 4.

written documents such as electronic correspondence[13]. However, visual evidence is distinguished from other forms of evidence by its ability to convey facts directly, which gives it particular importance in the area of forensic evidence.

This type of evidence is becoming increasingly important in light of recent technological developments, especially with the advent of deepfake technologies, which raise serious challenges related to the admissibility and reliability of visual evidence.

Second: The Authenticity of Visual Evidence in Criminal Evidence

A- The Statutory Authenticity of Visual Evidence in the Saudi Law

In fact, the visual evidence does not deviate from being one of the forms of digital evidence, and in this regard, what was decided by the General Assembly of the Supreme Court in the Kingdom of Saudi Arabia, where it was stated in one of its principles that: "The digital evidence is a valid argument in proof when it is delivered from the evidence, and its strength varies in weakness and strength according to the incident, its circumstances, and the evidence that celebrates it."[14]

The Evidence Law in the Kingdom of Saudi Arabia also stipulates the principle of reliance on digital evidence, as Article (55) stipulates that: "Proof by digital evidence shall have the ruling of proof in writing as stated in this law."[15] It is understood from this text that the Saudi legislator has equated the digital and written evidence in terms of authenticity and regulatory effects, and has subjected them to the same requirements for the validity of written proof.

This text is an explicit affirmation of the principle of equality between digital and written evidence in terms of the statutory conditions that must be met in order to be considered in proof. Accordingly, digital evidence does not remain a mere presumption, but rises to the status of evidence once it meets the requirements established by the system, to become a stand-alone evidence with the same evidentiary value as traditional[16] evidence.

Visual evidence is not a rigid legal description, but its legal nature is determined according to its power to reveal the truth; if it is direct and decisive, it is considered evidence, and if it is possible for interpretation, its effect is limited to being a presumption subject to the discretion of the court.

B- Rules for the Admissibility of Visual Evidence in Criminal Evidence

The authenticity of the visual evidence is not complete until we identify the controls that govern its admissibility before the court, as the admissibility is achieved after the evidence has passed the procedural stage of verifying its legality, technical integrity and chain of custody, which requires a detailed explanation of these controls.

1**. Legality of Obtaining Visual Evidence**

The Law of Criminal Procedure recognizes the principle of the legality of obtaining evidence as one of the essential guarantees in the field of criminal evidence, and evidence – whether visible or otherwise – is not considered unless it is obtained in accordance with sound legal procedures that respect rights and freedoms. The effect of the violation does not stop at the procedure itself, but extends to the subsequent proceedings that result from it, when they are based on it and closely related to it, so that the evidence resulting from it is considered invalid according to the invalidity of its origin[17].

The legality of access to visual evidence is the first criterion governing its admissibility, as this requirement is directly related to the protection of fundamental rights, foremost of which is the right to privacy and the guarantees of a fair trial. Comparative systems have adopted multiple approaches in this regard: in American jurisprudence, the Supreme Court established the principle of excluding evidence obtained illegally, which is summarized in the fact that the police searched the defendant's home without a valid search warrant and found illegal materials that were used as evidence to convict her. The defendant challenged the legality of this search, and the US Supreme Court concluded that the evidence obtained in violation of the Fourth Amendment of the US Constitution should not be used, stressing that respect for the guarantees of search and privacy requires the exclusion of any evidence obtained illegally, so that constitutional rights do not turn into only formal guarantees[18].

In contrast, the European Court of Human Rights has taken a more flexible approach, as in Schenk v. Switzerland (1988), where the European Court of Human Rights accepted a video recording that was used to prove a crime despite the alleged illegality of obtaining it, emphasizing that the admissibility standard is not based on the method of obtaining the evidence alone, but on the fairness of the trial as a whole. Since the accused had the opportunity to challenge and discuss

[13] Ziad Majed Al-Abdul-Jabbar, "The Authenticity of Digital Evidence in Proof: A Study in the Saudi Evidence System", Journal of Economic, Administrative and Legal Sciences 6, Vol. 26 (2022): 141

[14] Decree No. 34 dated 24/4/1439 H

[15] Article 55 of the Saudi Evidence Lawi ssued by Royal Decree No. M/43 dated 26/5/1443 H

[16] Ziyad Majid Al-Abd Al-Jabbar, op. cit., p. 141

[17] Article 190 of the Code of Criminal Procedure romulgated by Royal Decree No. M/2 dated p H 1435/01/22

[18] Mapp v. Ohio, 367 U.S. 643 (1961).

the recording, its use was considered to be compatible with fair trial guarantees[19].

It should be noted that this balancing approach is consistent with the trend that can be deduced from the texts of the Saudi Evidence Law, which does not prescribe an automatic penalty for the mere existence of a procedural defect, but rather leaves the court with the authority to assess the authenticity of the evidence in light of the circumstances of the case, reflecting a shift towards the logic of substantive justice

2**. The Authenticity and Technical Integrity of the Evidence**

In addition to the legality of obtaining evidence, the authenticity and technical integrity of the visual evidence is an essential condition for its admissibility in criminal evidence, as it must be verified that the evidence presented is the same as the original evidence without alteration or distortion. The U.S. Federal Rules of Evidence regulate this issue, as Rule 901 stipulates that sufficient evidence must be established to prove the attribution of evidence to its true source, in order to ensure that it is protected from forgery or manipulation[20]

The authenticity of the visual evidence is achieved through various technical means, most notably metadata analysis, hash value, and the use of specialized technical expertise[21], which aim to ensure the technical integrity of the evidence and maintain its reliability in the digital environment. These controls are becoming increasingly important in light of the rapid development of deepfake technologies, which enable the production of highly realistic visual content that is difficult to distinguish from the truth.

In the Saudi Evidence Law framework, Article (60) of the Evidence Law emphasizes the need to present the digital evidence in its original form or in a way that allows verification of its content, which reflects the requirement of the technical integrity of the evidence and that it is not subject to modification, and makes the technical examination a necessary element for the visual evidence to acquire its evidentiary value.

At the judicial level, the case of Lorraine v. Markel American Insurance Co. is one of the most prominent precedents that established the criteria for the admissibility of digital evidence, as the court affirmed that the admissibility of this type of evidence depends on proving its authenticity, technical integrity and reliability, in accordance with modern legal and technical requirements. It is inferred from this judgment that the authenticity of visual evidence is not absolute, but depends on the extent to which it meets the technical and legal controls that ensure its technical integrity against tampering or alteration[22].

3**. Chain of Custody Assurance**

The principle of chain of custody is one of the essential procedural guarantees in the field of criminal evidence, as it aims to document the path of evidence from the moment it is seized until it is presented to the court, in a way that ensures its integrity and prevents the possibility of tampering with or modifying it. The importance of this principle is not limited to formal documentation, but extends to enabling the judiciary to verify the technical integrity of the evidence and its source, thereby enhancing confidence in its evidentiary value[23].

This concept is consistent with Article 61 of the Saudi Evidence Law, which provides for a procedural penalty represented in the loss of the right of the litigant to invoke the evidence if he refrains from enabling the court to verify its authenticity, which indicates that the technical integrity of the evidence is closely linked to its traceability and examination. Article (62) also reflects a flexible approach, as the court has been granted the authority to assess the authenticity of evidence when it cannot be verified for a reason beyond the control of the parties, thus distinguishing between what affects the admissibility of the evidence and what falls within the scope of estimating its weight.

In this context, the criminal evidence system in modern systems is based on the principle of the judge's freedom to form his conviction, so that the evidence does not have a prior mandatory value, but is subject to the court's discretion in light of the circumstances and circumstances of the case. However, visual evidence raises a particular problem, as it is often presented as a direct reflection of reality, while jurisprudential and judicial analysis reveals that its argument is not derived from its apparent nature, but from the extent to which it meets the technical and legal controls, especially the technical integrity of the chain of custody, the authenticity of the evidence, and the possibility of Verification of its content, which is in line with the direction adopted by the Saudi Evidence Law in regulating digital evidence.

This trend finds echoes in jurisprudence and comparative justice, especially in the American system, where proof of the integrity of the chain of custody is required to ensure the admissibility of the evidence, and any interruption in it results in raising doubts about its reliability, which may lead to its exclusion or diminishment of its evidentiary weight[24].

It is clear from the above that the evidentiary value of visual evidence in forensic evidence does not stand on

[19] Schenk v. Switzerland, European Court of Human Rights, Application no. 10862/84, Judgment of 12 July 1988.

[20] Federal Rules of Evidence, Rule 901

[21] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Burlington: Academic Press, 2011), 40–45.

Bill Nelson, Amelia Phillips, and Christopher Steuart, Guide to Computer Forensics and Investigations, 5th ed. (Boston: Cengage Learning, 2019), 85–92..

[22] Lorraine v. Markel American Insurance Co., U.S. District Court, District of Maryland (2007).

[23] Casey, Digital Evidence and Computer Crime, at 55..

[24] Nelson et al., Guide to Computer Forensics and Investigations, 88–90..

its own, but depends on the extent to which it meets a set of legal and technical controls that ensure its technical integrity and reliability. However, the rapid technical development, especially in the field of deepfakes, has created new challenges that threaten the reliability of this type of evidence, and raise questions about the adequacy of traditional controls in confronting it, which calls for examining and analyzing this problem in the second section.

Second Topic

The Impact of Deepfakes on the Authenticity of Visual Evidence and Ways to Counter It

The field of forensic evidence is witnessing a qualitative transformation in light of the rapid development of digital technologies, where the problem is no longer limited to the legality or technical integrity of the evidence, but has extended to the extent of the reliability of the evidence itself in the face of advanced technologies capable of simulating reality with a high degree of accuracy. In this context, what are known as deepfake techniques are highlighted, which represent a real challenge to the authenticity of visual evidence, due to their ability to produce content that is difficult to distinguish from real recordings, which can lead to misleading the court or questioning the correct evidence. Therefore, this paper aims to analyze the impact of deepfakes on the reliability of visual evidence, and to show the adequacy of traditional controls in confronting it, through two requirements:

The first requirement: The effect of deepfakes on the reliability of visual evidence.

Second Requirement: Technical and Statutory Mechanisms to Enhance the Authenticity of Visual Evidence in the Face of Deepfakes

The first requirement

Impact of deepfakes on the reliability of visual evidence.

While traditional controls have established a theoretical framework to ensure the authenticity of visual evidence, the emergence of deepfakes raises the question of the adequacy of these controls in achieving judicial certainty and ensuring the fairness of the proceedings

The impact of these techniques is no longer limited to the technical aspects of the evidence, but extends to the legal foundations on which its admissibility is based, foremost of which is the legality of the evidence, the extent to which it is able to achieve judicial certainty, and the possibility of its examination before the court. Therefore, it is necessary to examine the impact of deepfake manipulation on these three pillars, as they constitute the main pillars of the reliability of visual evidence in criminal evidence.

1. The Impact of Deepfakes on the Legality of the Evidence:

The spread of deepfakes has complicated the question of the legality of visual evidence in forensic evidence, as legality is no longer limited to the integrity of the procedures for obtaining evidence, but has extended to verifying the nature of the content itself and the extent to which it relates to reality. This problem is even more pronounced when distinguishing between filming in private places and filming in public places, as each has an impact on assessing the legality of the evidence.

The principle of legality is one of the basic principles governing the search for evidence in criminal proceedings, as evidence must be obtained in accordance with legitimate procedures that ensure the preservation of human dignity and respect for his privacy, otherwise the evidence will be considered illegitimate and invalid to be invoked whenever it was obtained in a way that violates the sanctity of private life. This rule is supported by the Basic Law of Government, which stipulates in Article 26 the State's obligation to protect human rights in accordance with Islamic Sharia, and Article 40 affirms the inviolability of correspondence, conversations and private means, and that they may not be viewed or monitored except in the cases specified in the law. It follows that any evidence obtained in contravention of these safeguards is contrary to the principle of legality.

In this context, visual evidence, and in particular photographs and recordings, occupy a prominent place in forensic evidence, because of its ability to convey and embody reality, when it is free from distortion or manipulation. However, its use in evidence may infringe on an inherent human right, namely the right to privacy, which imposes the need to adhere to regulatory controls when relying on it[25].

With regard to photographing in private spaces, determining the nature of the place is an essential element in assessing the legality of obtaining the evidence, as it is related to the protection of private life, and refers to places where a person expects a reasonable amount of privacy, such as closed homes and offices. Jurisprudence has established that filming in these places without permission or legal justification is a violation of the sanctity of privacy, and it results in the exclusion of the evidence. This is confirmed by contemporary legal studies, where research indicates that digital evidence obtained in ways that violate privacy raises the issue of serious problems related to the extent of its judicial admissibility, given that it entails infringement on the fundamental rights of individuals[26], which may lead to its exclusion due to its illegality. Registration in private places without a legal basis is also

[25]Ahmed Shawqi Shawahneh, The Authenticity of the Evidence Derived from the Surveillance Camera in Evidence before the Criminal Judge, Master's Thesis, Arab American University, Palestine (2023): 69

[26]Danielle Keats Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review 107, no. 6 (2019): 1753–1819, at 1774.

an attack on the right to privacy[27], which weakens the authenticity of the visual evidence and makes its admissibility questionable, especially in light of the technological development that allows the production of visual content that is difficult to verify

This trend has been exemplified in comparative justice, as in Schenk v. Switzerland[28], where the European Court of Human Rights has dealt with the use of a recording made without the knowledge of one of the parties, and has emphasized that the admissibility of evidence must be assessed in the light of the fairness of the proceedings as a whole, taking into account the protection of the right to privacy, which reflects the importance of balancing the requirements of proof with the guarantees of fundamental rights.

However, deepfakes add a more complex dimension, as the danger is no longer limited to illegal photography, but has extended to the possibility of creating visual recordings that give the illusion that the filming takes place in private places without actually existing, which raises the question of the extent to which the appearance of evidence can be relied upon to assess its legitimacy without verifying its authenticity and technical integrity.

As for filming in public places, the origin is legality, because there is no legitimate expectation of privacy[29], which makes the visual evidence derived from it more acceptable, when the conditions of authenticity and technical integrity are met. However, this presumption is no longer absolute in the light of deepfake technology, as recordings can be produced that suggest that events took place in public places that did not take place in the first place, leading to misleading the judiciary about the source and legality of obtaining the evidence.

Thus, it is clear that deepfakes have not only affected the content of the visual evidence, but its impact has extended to the legal basis for the legality of obtaining it, so that the standard of place itself is no longer sufficient, but it has become necessary to support this with a technical verification of the authenticity and technical integrity of the evidence, to ensure that it reflects a real fact and not artificial content.

2. Examination of Evidence:

The principle of examining evidence is one of the basic guarantees for the achievement of criminal justice, as it requires that the evidence be presented before the court and discussed in the presence of the litigants, enabling each party to examine its content, interrogate its source, and verify the method of obtaining it and the extent to which it adheres to the requirements of legality. A breach of this principle would prejudice the right to a defence and undermine the foundations of a fair trial, especially if evidence is relied on that the parties could not discuss or verify.

However, the advent of deepfake techniques has increasingly complicated the process of discussing visual evidence, as the debate is no longer limited to the content of the recording, but has extended to verifying its technical authenticity and proving that it is free from manipulation. With the ability to produce high-resolution videos that are difficult to distinguish from reality, it is impossible for a judge – and sometimes even an expert – to distinguish between real and fake evidence without the use of advanced technical analysis tools[30].

As a result, the examination of visual evidence is no longer a formality, but has become a complex technical process that requires the submission of specialized expert reports and the analysis of technical data associated with the registration, including verification of its source and the integrity of its digital structure, which increases the burden of proof on the litigants and enhances the role of technical expertise in guiding the court's conviction[31].

In this context, it is not enough to simply provide a visual recording to invoke it, but it must be subjected to an objective, legal and technical examination that ensures an accurate interpretation of its content, and verifies the legality of obtaining it and its technical integrity. Jurisprudential studies have emphasized the need to preserve procedural safeguards when dealing with digital evidence, especially in light of the possibilities of forgery provided by modern technologies, stressing that the authenticity of visual evidence does not derive from its apparent form, but from the extent to which it is subject to examination and analysis before the judiciary[32].

3. Certainty of proof:

The requirement of certainty of proof is one of the main pillars for the admission of visual evidence in criminal evidence, as the evidence must be clear and conclusive in a way that allows the judge to rely on it to form his conviction and make his judgment. It is not enough for evidence to be merely a recording or photograph of a particular incident, but it must be able to remove doubt and reach a degree of acceptable judicial certainty, reflecting the objective truth of the incident in dispute.

However, the advent of deepfakes has cast a shadow over this requirement, as visual evidence no longer has the same certainty value that was traditionally assumed, as it can produce high-resolution visual content that mimics reality to a degree that makes it difficult to distinguish between real and fake. Recent studies have suggested that these techniques may be used to produce clips that appear highly realistic, which can lead to

[27] Tal Z. Zarsky, "Privacy and Data Collection in the Digital Age," Harvard Law Review Forum, Vol. 127 (2013), p. 209

[28] Schenk v. Switzerland.op. cit ,

[29] András Koltay, "Photographing People in Public and the Protection of Privacy," Central European Journal of Comparative Law, Vol. 3, Issue 2 (2022), p. 96.

[30] M. Hydara, A. Abayomi-Alli, S. Misra, and R. Damaševičius, "Deepfake Detection: Challenges and Future Directions," IEEE Access, Vol. 12 (2024), pp. 6

[31] Hydara et al., "Deepfake Detection," p. 7

[32].149–146Shawahneh, op. cit., pp.

misleading the court if their authenticity is not verified before they are submitted to court[33].

The technical literature also confirms that deepfakes' ability to accurately simulate facial features and voices makes it difficult for a judge – and even experts – to differentiate between real and fake content without the help of advanced analysis tools[34].

In this context, it is important to develop technical and legal mechanisms to verify visual evidence, most notably metadata analysis, traceability of digital content, and the use of deepfake detection tools, in order to ensure the reliability of evidence in judicial proceedings[35]. Recent studies also suggest that any flaw in verifying the authenticity of the recording undermines a judge's ability to rely on it with certainty[36].

From a jurisprudential point of view, the certainty of proof is measured by the extent to which the evidence is close to the objective truth, which is expressed in criminal jurisprudence by the rule that "proof by conclusion takes precedence from proof by suspicion", as visual evidence – when it meets the conditions of reliability and clarity – is supposed to rise to the level of strong evidence in proof, and not to be a source of doubt or probability[37].

This problem has been embodied in practice in judicial applications, most notably the case of Mendones v. Cushman & Wakefield, where videos generated using artificial intelligence techniques were presented as evidence, but the court revealed technical indications of forgery, including a mismatch of mouth movement with voice, and a malfunction in digital data (metadata), which led it to dismiss the lawsuit and impose procedural sanctions[38].

Some practical incidents, such as the "Polvoron Video" (2024) incident, also reveal the danger of relying on visual content without verifying its authenticity, as the video has been proven to be fabricated using advanced technical analysis tools, which reinforces the need for visual evidence to be subject to technical examination before it can be considered as proof[39].

Thus, it is clear that deepfake technology has not only affected the certainty of visual evidence, but has also extended to its legality, authenticity and admissibility, which has undermined the traditional assumption of credibility of this type of evidence and made it subject to the need for rigorous technical verification, so that certainty can only be achieved through a combination of judicial evaluation and specialized technical analysis. In view of this shift in the nature of visual evidence and the consequent legal and practical problems, there is a need to develop technical and statutory mechanisms capable of confronting it These new challenges reaffirm reliability of visual evidence and enhance its admissibility in forensic evidence.

The second requirement

Technical and statutory mechanisms to enhance the authenticity of visual evidence in the face of deepfakes

In light of the problems created by deepfake technology that affect the reliability of visual evidence, it is no longer enough to rely on traditional means of proof, but it has become necessary to adopt modern technical and statutory mechanisms that enhance the authenticity of this evidence and reduce the risks of tampering with it. Accordingly, this requirement deals with these mechanisms and ways to activate them in the framework of criminal evidence.

First: Technical Mechanisms for Protecting Visual Evidence

In light of the escalation of deepfake capabilities and the complexity of its methods, there has been a need to develop advanced technical means capable of detecting the manipulation of visual content, in a way that contributes to verifying the authenticity of the evidence and supporting its reliability before the judicial authorities. The most prominent of these methods can be described as follows:

1. Detection using deep learning algorithms

Deep learning algorithms are one of the most prominent techniques used in deepfake detection, as they rely on training advanced AI models to analyze images and videos and detect abnormal patterns resulting from artificial generation processes. Neural Networks (CNNs) are often used to analyze facial features and extract subtle features that the human eye may not notice, such as pixel differences or asymmetries in facial details. Studies have proven that these models can achieve high levels of accuracy in detecting deepfake manipulation, which contributes to enhancing the

[33] Matthew Freeman, "Threat of Deepfakes to the Criminal Justice System: A Systematic Review," Crime Science, Vol. 13, 2024, p6

[34] Ebrima Hydara, Masashi Kikuchi & Takayuki Ozono, "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence," IEEE Access, Vol. 12, 2024, pp4

[35] Casey, Digital Evidence and Computer Crime, 45–47. Stephen Mason and Daniel Seng, Electronic Evidence, 5th ed. (London: Institute of Advanced Legal Studies, 2017), 72–74.

[36] Francesco Marra et al., "Detection of GAN-Generated Fake Images over Social Networks," Forensic Science International: Reports, Vol. 7 (2023), NO. 100262.

[37] Mohamed Karima, Forensic Evidence: Its Rules and 225–223Fikr, 2015), -Types (Cairo: Dar Al

[38] Mendones v. Cushman & Wakefield, Alameda County Superior Court (California), 2025, reported in: NBC News, 2025.

[39] Deepfake Video Circulates Against Philippine President," The Philippine Star, 2024

reliability of the visual evidence and supports the court's conviction of its technical integrity against tampering[40].

2- Digital forensic analysis of visual media

Modern technical methods in detecting deepfakes rely on digital forensic analysis of visual media, which examines the technical characteristics of videos and images to detect the effects of digital manipulation. These methods include digital noise analysis, file compression effects, frequency analysis in images and videos using the frequency range, tracking discrepancies in sequential frames and detecting abnormal changes in facial movement or asymmetry between audio and image. This type of analysis contributes to the detection of hidden indicators of manipulation. This enhances the ability to verify the technical integrity of visual evidence and supports the confidence of judicial authorities that it is free from deepfake manipulation [41].

3- Facial biomarker analysis

Facial and video biomarker analysis is one of the latest techniques in detecting deepfakes, as it relies on the study of natural biological characteristics of humans that are difficult for deepfake techniques to accurately simulate. These signals include eyelash rate, skin discoloration due to blood flow (Photoplethysmography), subtle facial movements, and the coordination between facial expressions and voice. One study showed that many manipulated videos fail to mimic these vital signals naturally, which enables analysis systems to detect deepfake manipulation even in high-quality clips, enhance the reliability of the examination results and support the authenticity of the visual evidence before the courts[42].

4- Analyze the temporal consistency of the video

Temporal Consistency Analysis (CL) is an effective tool in detecting deepfakes, as it focuses on studying the relationship between sequential frames and subtle changes in facial movement and expressions. Even advanced techniques in deepfakes often fail to maintain the consistency of movement between frames or between lip movement and voice, creating indicators that can be detected by advanced analysis tools. One study showed that checking the frame chronology helps detect subtle errors in expressions face, which is a technical indicator that enhances the technical integrity of visual evidence and supports its reliability in forensic evidence[43].

5. Hybrid models for deepfake detection

The recent research trend tends to develop hybrid models that combine deep learning techniques with digital forensics techniques to improve the accuracy of deepfake detection. These models are one of the most advanced, as they rely on combining several analytical tools into a single framework, such as combining bypass neural networks (CNNs) and repetitive neural networks (RNNs) or combining them with performance enhancement techniques such as PSO.

Studies show that this integration enables models to recognize deepfakes even in high-quality clips, and contributes to reducing error rates compared to relying on a single technique, due to its ability to analyze visual, temporal and physiological characteristics in an integrated manner, enhancing the reliability of detection results and supporting the authenticity of visual evidence in forensic[44] evidence.

It is clear from the above that the fight against deepfakes is no longer based on a single technology, but is based on an integrated system that includes deep learning algorithms, digital forensics, biosignal analysis, and video chronological coordination analysis, in addition to hybrid models that combine these methods, which contribute to enhancing the reliability of visual evidence and supporting its authenticity in forensic evidence.

However, the effectiveness of these technical tools remains limited unless they are supported by a statutory framework that regulates their use and ensures their admissibility before the courts, which requires a review of the complementary statutory mechanisms.

Second: Statutory Mechanisms to Enhance the Authenticity of Visual Evidence

The statutory mechanisms to enhance the authenticity of visual evidence are to enable the judge to exercise his discretion in evaluating the digital evidence. Therefore, the assessment of the ability of technical means to preserve and secure the data of the digital evidence and its admissibility in evidence falls within the discretion of the judge, who examines and verifies the digital

[40] L. Gong and X. Li, "A Contemporary Survey on Deepfake Detection: Datasets, Methods, and Challenges," Electronics (2024): 5. Tolosana et al., "Deepfakes and Beyond," at 140.

[41] S. M. Qureshi et al., "Deepfake Forensics: A Survey of Digital Forensic Methods for Multimodal Deepfake Identification," PeerJ Computer Science 10 (2024): 6.

[42] D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks and Physiological Signals," Journal of Visual Communication and Image Representation 74 (2021): 6.
Y. Li and S. Lyu, "Exposing DeepFake Videos by Detecting Face Warping Artifacts," IEEE International Conference on Multimedia and Expo (ICME) (2019): 5.

[43] Zahid Akhtar, "Deepfakes Generation and Detection: A Short Survey," Journal of Imaging 9, no. 1 (2023): 7–8

[44] Momina Masood et al., "Deepfakes Generation and Detection: State-of-the-Art, Open Challenges, Countermeasures, and Way Forward," Applied Intelligence 53 (2023): 3974–4026, at 3981–3983.
A. Al-Adwan et al., "Detection of Deepfake Media Using a Hybrid CNN–RNN Model and Particle Swarm Optimization Algorithm," Computers 13, no. 4 (2024): 6–7.

evidence by discussing it in the judicial session to highlight its admissibility and evidentiary value[45].

Thus, the judge is not bound by the expert opinion or the technical findings they provide but rather appreciates the strength of these clues within the discretion granted to him, taking into account the rest of the evidence and the circumstances surrounding the case. This discrepancy reflects a difference in the view to which the adoption of digital evidence is mandatory versus the persuasive power that the judge gives to digital evidence, which is a fundamental focus of recent studies on digital forensics in the Saudi Law.

In furtherance of this discretion, the technical examination carried out by specialists using advanced digital analysis tools contributes to the detection of any illegal modifications, installations or manipulations that may have been made to the visual material. If this examination proves the integrity of the visual recording from forgery or manipulation, it acquires the strength of the proof as a technical presumption that the judge can rely on within the body of evidence presented in the case, as confirmed by studies on the authenticity of existing digital evidence on artificial intelligence technologies[46].

The role of the expert is not limited to conducting the technical examination, but also extends to the preparation of a technical report that clarifies the results in an accurate scientific manner, showing the extent of the authenticity of the clip, its source and the integrity of its digital structure, which enables the court to form a clear perception of the evidence. This technical expertise is an auxiliary element to the judge's discretion, as the judge is guided by the opinion of the specialists without being bound by it, and he appreciates the authenticity of the visual evidence in the light of the technical reports and other evidence of the case presented to him.

In this context, the evidentiary value of visual evidence is its ability to provide accurate information about the facts in dispute, which affects the formation of a judge's conviction. Two main trends have arisen in legal jurisprudence regarding this value, with the first trend arguing that digital evidence has strong evidentiary value when it is proven to be technically sound, which limits the scope of the judge's discretion[47].

The second approach, on the other hand, believes that visual evidence is nothing more than a technical presumption subject to the discretion of the judge, who balances it with other evidence, and does not abide by the results of the technical expertise absolutely, but rather adopts them within the framework of his discretion[48].This confirms that estimating the ability of technical means to preserve and secure the data of the digital evidence and its admissibility in evidence falls within the scope of the judge's discretion, as he examines the digital evidence and verifies it through its discussion during the judicial session, to highlight its admissibility and evidentiary value[49].

In light of the above, the positions of comparative legal systems differ in how the authenticity of visual evidence is regulated. In the American system, the principle of the judge's freedom to form his or her conviction prevails, with a heavy reliance on technical expertise in the evaluation of digital evidence, where expert reports are a pivotal element in verifying the integrity of the evidence and its reliability[50]. In some European systems, regulation tends to be more stringent, by setting strict controls related to the safety of the collection of digital evidence and ensuring that it is not tampered with. In addition to focusing on privacy protection and data integrity, which is reflected in the extent to which the evidence is admissible and evidential[51].

In the Saudi Law, the regulation is based on the principle of the judge's freedom to form his conviction, where the assessment of the integrity of the digital evidence and its evidentiary value falls within the scope of the court's discretion, through its examination and discussion during the hearing of the case, in the light of the technical reports and supporting evidence submitted in this regard. This approach reflects a balance between benefiting from technical development in the means of proof and maintaining statutory safeguards that ensure the fairness of the proceedings and the achievement of judicial certainty.

On the basis of the foregoing, it is clear that enhancing the authenticity of visual evidence in the face of deepfakes is not achieved through technical means alone, but requires an integrated statutory framework based on technical expertise and at the same time subject to the discretion of the judge, while drawing on comparative experience, in order to achieve a balance between technological development and the requirements of criminal justice, and to enhance reliability of visual evidence as an effective means of proof.

Meeting the challenges of deepfakes therefore requires continuous development in both technical means and

[45] Anzi, "The Provisions -Abdulhadi bin Muwafaq Al ence according to the Saudi Evidence of Digital Evid System", Journal of the College of Sharia and Law 28, Volume 3 (2024): 692

[46] Sager Al-Sager, "The Evidentiary Value of Proving Deepfake Technically and Jurisprudentially in Artificial Intelligence Systems," Journal of Social Studies 29, no. 4 (2023): 180–182.

[47]Orin S. Kerr, "Computer Records and the Federal Rules of Evidence," USA Bulletin 49, no. 2 (2001): 4–5.

[48] G. C. Kessler, Judges' Awareness, Understanding, and Application of Digital Evidence, Nova Southeastern University, 2010, p. 25.

[49]Anzi, op. cit., p. 692-Al

[50]Orin S. Kerr, "Digital Evidence and the New Criminal Procedure," Columbia Law Review 105, no. 1 (2005): 279–318, at 283.

[51]Stephen Mason and Daniel Seng (eds.), Electronic Evidence and Electronic Signatures (London: University of London Press, 2021), 236–240.

statutory frameworks, ensuring that visual evidence remains a reliable tool in the achievement of criminal justice.

Conclusion

Finally, with the rise of deepfakes, visual evidence no longer necessarily reflects reality, but is able to simulate it in a way that undermines the traditional assumption of its reliability. This reveals a qualitative shift in the structure of criminal evidence, which necessitates a re-evaluation of its foundations, foremost of which is the legality of obtaining the evidence, its examinability, and the standard of judicial certainty. While the Saudi evidence system has flexibility in assessing digital evidence, addressing these challenges requires strengthening the technical and statutory frameworks in a more specialized manner. Ensuring the reliability of evidence in the age of AI requires adopting an integrative approach that harmonizes law and technology, safeguarding criminal justice from the risks of deepfake manipulation and digital disinformation.

Based on the above, the research reached a number of findings and recommendations that would enhance the reliability of visual evidence and develop the efficiency of the criminal system in facing the challenges of artificial intelligence.

First: Results

1. Deepfakes are not just a technical challenge, but rather a structural shift in the nature of visual nce, which has led to the collapse of the evide traditional assumption based on the conformity of the image to reality, which is reshaping the epistemological basis on which forensic evidence is based.
2. The evidentiary value of visual evidence is no d from its direct sensory nature, but longer derive has become conditional on the technical verification of its digital structure, shifting the center of trust from "human perception" to technical analysis".
3. Deepfakes have expanded the concept of the e to include the legality of the legality of evidenc content itself, not just the legality of the means of obtaining it, a development that redefines the scope of procedural protection in criminal evidence.
4. Traditional controls for the admissibility of henticityevidence (legality, aut, chain of custody (are no longer sufficient on their own, and are unable to keep pace with highly complex artificial evidence, unless they are supported by advanced .technical mechanisms
5. The principle of examination of evidencehas shifted from a formal procedural guarantee to a complex technical process, in which technical expertise overlaps with judicial evaluation reflecting the changing nature of criminal litigation in the digital environment.
6. Judicial certainty indeepfake casesis no longer based on "clarity of evidence," but on "the degree to which it is verified," leading to a reformulation of the standard of judicial persuasion toward a more technical probabilistic model than traditional .certainty
7. n of reliance on technical expertise The expansio creates a delicate balancing problem, represented by the risk of the transfer of the discretion of evidence from the judge to the expert, which may .affect the essence of the judicial discretion
8. TheSaudi Lawflexible and balanced reflects a trend, but this balance is still in the process of adapting to technical challenges, and needs more statutory developmentspecialized in advanced .digital evidence
9. Confronting deepfakes requires a shift from the "independent evidence" model to the "integrated evidence" model, which is based on the synergy of technical evidence and forensic evidence in building conviction.

Second: Recommendations

1. The theory of forensic evidence in theSaudi Law should be developed to accommodate AI-generated evidence, by adopting the framework of Technologically Augmented Digital Evidence" as " .a benchmark for evaluating visual evidence
2. The Saudi evidence system should require visual evidence to be subject to prior technical inspection e is a possibility of the use of AI whenever ther technologies, and not to be considered as independent evidence without specialized .technical verification
3. Standardized national deepfake detection protocols that acknowledge their judicial admissibilityd, thereby should be adopte standardizing the evaluation of evidence and reducing inconsistency between judgments.
4. There is a need to establish an institutional structure specialized in digital evidence within the Saudi justice system, which enjoys technical nd is integrated with the judicialindependence a authorities.
5. The standard of judicial certainty should be recalibrated and the relationship between the judge and the technical experts should be clarified to ensure that the discretion of the judge remains in the hands of the judge, while requiring him to rely on multi-level technical verification in the evaluation of digital evidence.

Acknowledgment

The author would like to acknowledge the Deanship of Graduate Studies and Scientific Research, Taif University for funding this work.

References

1. Ahmed Shawqi Shawahneh, The Authenticity of the Evidence Derived from the Surveillance Camera in Evidence before the Criminal Judge ,Master's Thesis, Arab American University) (Palestine, 2023).

2. egal Aspects of Hakim, "The L-Rabab Mustafa Al Deepfakes", Journal of Jurisprudential and Legal (2025) Research, Vol. 48.
3. Jabbar, "The Authenticity of-Abdul-Ziad Majed Al Digital Evidence in Proof: A Study in the Saudi Evidence System", Journal of Economic, (2022) Sciences 6, p. 26 Administrative and Legal.
4. Sarah Moussa Mustafa Odeh, "Electronic Video Recordings and Their Authenticity in Jordanian Criminal Evidence", Jerash for Research and (2025) Studies, Volume 25, Volume 2.
5. Anzi, "The Provisions -Abdulhadi bin Muwafaq Al Evidence According to the Saudi of Digital Evidence System", Journal of the College of Sharia and Law 28, Volume 3 (2024).
6. Mohamed Karima, Forensic Evidence: Its Rules (Fikr, 2015-and Types (Cairo: Dar Al.
7. The Saudi Evidence Law, issued by Royal Decree ted 26/5/1443 HNo. (M/43) da.
8. The Saudi Code of Criminal Procedure, issued by Royal Decree No. (M/2) dated 22/1/1435 H.
9. Decision of the General Assembly of the Supreme Court No. 34 dated 24/4/1439 A.H.
10. Akhtar, Zahid. "Deepfakes Generation and Detection: A Short Survey." Journal of Imaging 9, no. 1.(2023)
11. Al-Adwan, A., et al. "Detection of Deepfake Media Using a Hybrid CNN–RNN Model and Particle Swarm Optimization Algorithm." Computers 13, no. 4(2024).
12. Al-Sager, Sager. "The Evidentiary Value of Proving Deepfake Technically and Jurisprudentially in Artificial Intelligence Systems." Journal of Social Studies 29, no. 4 (2023).
13. Altuncu, Enes, Virginia N. L. Franqueira, and Shujun Li. "Deepfake: Definitions, Performance Metrics and Standards, Datasets and Benchmarks, and a Meta-Review." arXiv preprint arXiv:2208.10913.(2022)
14. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed., Burlington: Academic Press, 2011).
15. Citron, Danielle Keats, and Robert Chesney. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." California Law Review 107, no. 6.(2019)
16. Federal Rules of Evidence (2024 ed.), Rule 901.
17. Freeman, Matthew. "Threat of Deepfakes to the Criminal Justice System: A Systematic Review." Crime Science 13, no. 1.(2024)
18. Gong, L., and X. Li. "A Contemporary Survey on Deepfake Detection: Datasets, Methods, and Challenges." Electronics.(2024)
19. Goodfellow, Ian, et al. "Generative Adversarial Nets." In Advances in Neural Information Processing Systems, vol. 27.(2014)
20. Güera, D., and E. J. Delp. "Deepfake Video Detection Using Recurrent Neural Networks and Physiological Signals." Journal of Visual Communication and Image Representation 74 .(2021)
21. Hak, Jonathan W. Image-Based Evidence in International Criminal Prosecutions (Oxford: Oxford University Press, 2024).
22. Hydara, Ebrima, Masashi Kikuchi, and Takayuki Ozono. "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence." IEEE Access 12.(2024)
23. Hydara, M., A. Abayomi-Alli, S. Misra, and R. Damaševičius. "Deepfake Detection: Challenges and Future Directions." IEEE Access 12.(2024)
24. Kerr, Orin S. "Computer Records and the Federal Rules of Evidence." USA Bulletin 49, no. 2.(2001)
25. Kerr, Orin S. "Digital Evidence and the New Criminal Procedure." Columbia Law Review 105, no. 1.(2005)
26. Kessler, G. C. Judges' Awareness, Understanding, and Application of Digital Evidence (Dissertation, Nova Southeastern University, 2010).
27. Kietzmann, Johan, et al. "Deepfakes: Trick or Treat?" Business Horizons 63, no. 2.(2020)
28. Koltay, András. "Photographing People in Public and the Protection of Privacy." Central European Journal of Comparative Law 3, no. 2.(2022)
29. Li, Y., and S. Lyu. "Exposing DeepFake Videos by Detecting Face Warping Artifacts." In IEEE International Conference on Multimedia and Expo (ICME).(2019)
30. Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).
31. Mapp v. Ohio, 367 U.S. 643.(1961)
32. Marra, Francesco, et al. "Detection of GAN-Generated Fake Images over Social Networks." Forensic Science International: Reports 7.(2023)
33. Mason, Stephen, and Daniel Seng. Electronic Evidence (5th ed., London: Institute of Advanced Legal Studies, 2017).
34. Mason, Stephen, and Daniel Seng, eds. Electronic Evidence and Electronic Signatures (London: University of London Press, 2021).
35. Masood, Momina, et al. "Deepfakes Generation and Detection: State-of-the-Art, Open Challenges, Countermeasures, and Way Forward." Applied Intelligence 53.(2023)
36. Mendones v. Cushman & Wakefield, Inc., No. 23CV028772, Superior Court of California, County of Alameda.(2025)
37. Nelson, Bill, Amelia Phillips, and Christopher Steuart. Guide to Computer Forensics and Investigations (5th ed., Boston: Cengage Learning, 2019).
38. Qureshi, S. M., et al. "Deepfake Forensics: A Survey of Digital Forensic Methods for Multimodal Deepfake Identification." PeerJ Computer Science 10.(2024)

39. Schenk v. Switzerland, European Court of Human Rights, Application No. 10862/84, Judgment of 12 July 1988.
40. "Deepfake Video Circulates Against Philippine President," The Philippine Star, Apr. 24, 2024.
41. Tolosana, Ruben, et al. "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection." Information Fusion 64.(2020)
42. Tursun, O., et al. "The Potential Effects of Deepfakes on News Media and Entertainment." AI & Society 40, no. 4.(2025)
43. Westerlund, Michael. "The Emergence of Deepfake Technology: A Review." Technology Innovation Management Review 9, no. 11.(2019)
44. Zarsky, Tal Z. "Privacy and Data Collection in the Digital Age." Harvard Law Review Forum. (2013).