International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique
https://doi.org/10.1007/s11196-023-10030-1

Digital Face Forgery and the Role of Digital Forensics

Manotar Tampubolon[1]

Accepted: 12 July 2023
© The Author(s), under exclusive licence to Springer Nature B.V. 2023

Abstract

Advancements in digital technology have made it easy to alter faces using editing software, posing challenges for industries in verifying photograph authenticity. Digital image forensics, a scientific method, is employed to gather data and determine the veracity of faces. This study assesses the effectiveness of digital image forensics in detecting fake digital faces using tools such as Foto Forensics, Forensically Beta, and Opanda IExif. Foto Forensics analyzes JPEG picture compression levels to detect image edits, revealing metadata differences compared to the original photo. Forensically Beta examines digital characteristics like color and noise levels to identify alterations. Opanda IExif scrutinizes image metadata, disclosing information about the camera used and subsequent changes. All three forensic methods effectively identify fake digital faces. Analyzing metadata differences and contrast variations between the original and altered faces proves to be an effective method for spotting alterations. Digital image forensics enhances legal and investigative processes, serving as a valuable tool for identifying digital face manipulation. Stronger digital security measures, including improved encryption, authentication, and legal regulations, are needed to protect against facial photograph manipulation. Updating legal and regulatory frameworks for digital security is vital to address increasingly sophisticated techniques used in facial photograph editing. As digital technology advances, continuous development and improvement of forensic techniques are crucial to detect digital face fabrication. Given the growing complexity of digital editing tools and the ease with which facial images can be altered, reliable methods are essential. Digital image forensics provides a systematic approach to gather data and verify the authenticity of digital photographs.

Keywords Digitaltechnology · Facefabrication · Fotoforensics · Forensicallybeta · Opanda IExif

✉ Manotar Tampubolon
manotar.tampubolon@uki.ac.id

[1] Universitas Kristen Indonesia, Jakarta, Indonesia

Published online: 06 August 2023

1 Introduction

Due to rapid technological advancements, the global consumption of digital media has significantly increased. Digital media has become an indispensable tool in various aspects of our lives, including company marketing and social media platforms. It plays a crucial role in the entertainment industry, particularly in the creation of special effects and editing. However, these advancements have also led to the emergence of digital face fabrication, commonly known as deepfakes. Lavrence, and Cambre [1] define deepfakes as a method of editing digital content to create realistic-looking but entirely fake visuals. Deep learning algorithms are utilized to alter a person's voice, facial expressions, and body movements, resulting in films that appear authentic but are actually entirely fabricated.

The potential misuse of digital face forgeries is a major concern for individuals and organizations alike. It can be used to manipulate public opinion, tarnish reputations, and even coerce individuals. The ability to create a video that seemingly depicts someone engaging in activities they have never actually done can have devastating effects on people's perceptions of their own capabilities [2]. In recent years, there has been a significant rise in the proliferation of deepfake videos online. While some of these videos are created for entertainment purposes, others are crafted with malicious intent. As a result, there is an increased demand for professionals with expertise in digital forensics to assess the authenticity of these recordings.

The analysis of digital devices and data is referred to as "digital forensics," which aims to gather evidence for use in legal proceedings. In the field of digital forensics, experts employ various methods to examine digital materials and determine if data have been manipulated [3]. When it comes to deep fakes, digital forensics experts can investigate the information, audio, and visual components of a video to assess its authenticity. According to Ross et al. [4], digital forensics experts play a crucial role in verifying the authenticity of deepfake videos. Given the increasing prevalence of nefarious deepfake usage, it is imperative to have professionals who can identify and analyze such videos. Professionals in the field of digital forensics provide vital evidence during legal processes to combat the spread of false information. This article delves into the growing issue of digital face forgery, exploring the role of digital forensic professionals in investigating various types of videos. The article examines the processes involved in creating deepfakes, the potential societal impact of deepfakes, and the challenges faced by digital forensic professionals in researching these videos.

The first part of this article introduces digital face fabrication, covering topics such as the processes involved in creating deepfakes and their potential impact on individuals and businesses. In the following section, we explore the role of digital forensic professionals in investigating deepfakes, along with the tools and procedures used to analyze digital materials. The third section focuses on the challenges faced by digital forensic experts when researching deepfakes, including the need for specialized training and the difficulties in recognizing and verifying digital data. In the final part of the publication, recommendations are provided to enhance the examination of deepfakes, such as fostering collaboration among experts from different fields and developing new tools and methods for analyzing digital materials. In today's increasingly digital landscape, the proliferation of digital face manipulation has become a pressing issue. The ability to create synthetic videos that appear authentic has the potential to significantly impact individuals and organizations. Digital forensic experts play a crucial role in analyzing these videos, providing crucial evidence for legal proceedings and combating the spread of misinformation. This paper offers a comprehensive overview of digital face forgery and the role of digital forensic professionals in investigating movies containing such manipulations.

1.1 Explanation of Digital Face Forgery

Digital face fabrication, commonly known as "deepfake,“ has garnered significant attention and skepticism in recent years. This form of synthetic media utilizes artificial intelligence (AI) and deep-learning techniques to generate highly realistic computer-generated representations of human faces [5]. Deepfake technology represents a significant advancement in digital manipulation, surpassing previous methods in complexity and realism. Its applications span various fields, including entertainment, research, and unfortunately, even criminal activities. As noted by Seibold et al. [6], deepfake technology relies on Generative Adversarial Networks (GANs). GANs consist of a generator and a discriminator, with the discriminator determining the authenticity of images or videos and the generator responsible for producing fake visuals. Through the collaborative efforts of these networks, deepfakes achieve an astonishing level of credibility and lifelikeness.

To create a deepfake image or video, the generator network is trained using a vast dataset of the target's photos and videos. Through artificial intelligence (AI), the system learns the person's facial expressions, intonation, and other characteristics, enabling the generation of visually convincing content [7]. The generated media is then evaluated against the original by the discriminator network, which provides feedback to the generator for further improvement [8]. This iterative process continues until the generated image or video closely resembles the original, which is the objective of deepfake generators. While the technology behind deepfakes is still evolving rapidly [9], it is becoming increasingly accessible and user-friendly thanks to advancements in AI. Consequently, concerns have been raised regarding the potential misuse of deepfakes, such as the spread of misinformation and cyberbullying. One particularly significant concern revolves around the impact of deepfakes on politics and society. Deepfake-generated fake news and misinformation have the potential to greatly influence public opinion and even elections. If convincing recordings of public officials show them saying or doing things they never actually did, it can severely undermine the public's trust in these leaders and the organizations they represent. Additionally, deepfakes can be used for malicious purposes such as cyberbullying and the creation of revenge pornography.

Fake photos and videos can have detrimental effects on a person's reputation and mental well-being. The erosion of trust in the authenticity of digital media can lead to far-reaching implications. The entertainment industry is also not immune to the impact of deep fake technology. By creating convincing images or videos using deepfakes, it becomes possible to replace human actors or celebrities in media productions [10]. This poses significant challenges for businesses and raises questions about the integrity of their content. While deepfake technology represents a significant advancement in the digital media field, it also gives rise to serious concerns. Its misuse can have profound consequences for governments, cultures, and creative industries [11]. It is crucial, therefore, to address these concerns and implement measures to prevent their exploitation. This involves increasing awareness of the potential dangers associated with deepfakes, conducting further research on detecting and preventing deepfakes, and promoting responsible use of this technology.

1.2 Importance of Digital Forensic in Investigating Deepfakes

Deepfake technology is becoming more widely used, and with it, there is a need for digital forensic specialists to look into and spot fake media. The act of gathering, analyzing, and interpreting electronic data to find and protect legal evidence is known as digital forensics. Digital forensics is essential for the investigation of deep fakes and may help locate the producers and sources of fake material [12]. One of the main reasons digital forensics are essential for analyzing deep fakes is their capability to establish the veracity of digital materials [6]. To ascertain whether the material has been changed or altered, experts in digital forensics may check the metadata, file formats, and other aspects of the media using a range of tools and procedures. Investigators may use this information to identify the source and purpose of fraudulent media.

Specialists in digital forensics may utilize their knowledge and skills to identify the methods and equipment used to produce deep fakes. Future research on cutting-edge techniques for identifying and preventing deep fakes can use these data. Deepfake offenders may be located using digital forensics, which can also provide evidence presented in court [13]. Another crucial role of digital forensics in the study of deepfakes is to help victims. Deepfakes have the potential to seriously injure a person, causing mental pain, and harming their reputation. Digital forensics can help victims by locating the source of fake media and providing evidence that may be used in court. It may also help victims by determining how to obtain bogus material off the Internet and stop it from spreading.

Deepfakes may stop spreading through digital forensics. By locating the source of deep fakes and the methods used to create them, digital forensic experts can establish new ways to detect and prevent deep fakes [14]. Halting the spread of false information and deception may defend people and organizations against harm. However, there are several challenges to researching deep fakes. According to Paul Joseph, and Norman [15], experts in digital forensics face several difficulties when examining deepfakes. The need for specific knowledge and experience was one of the most significant barriers. Digital forensic experts must have a thorough understanding of the tools and technology used to produce deep fakes, as well as the methods for detecting and preventing them.

Identification and authentication of digital media are challenging tasks for forensic digital experts. Because deep fakes are becoming increasingly sophisticated, can be challenging to tell whether a video or image is real or fake [16]. Digital forensic specialists must inspect the material and look for any signs of manipulation or change using specific tools and techniques [13]. When examining deepfakes, digital forensic experts must address the lack of funding. The investigation of deepfakes involves specific tools and technologies that are costly and difficult to obtain. Thus, digital forensic experts only have limited access to resources, which might make it difficult for them to thoroughly evaluate deep fakes.

1.3 Purpose of this Study

The objective of this study is to offer readers a comprehensive understanding of digital face forgeries and the crucial role played by digital forensics in detecting deepfakes. This essay investigates the techniques and tools employed in creating deepfakes and explores their potential consequences on individuals and society. The research emphasizes the importance of digital forensics in identifying, preventing, and investigating deepfakes, while also addressing the challenges faced by experts in this field. Moreover, this research article seeks to contribute to the ongoing discourse on the societal impacts of digital media manipulation and provides recommendations for future research and advancements in this field.

2 Literature Review

Globally, people and businesses face substantial challenges due to the spread of deep fake technology. Digital information that has been altered or synthesized to falsely reflect reality is referred to as a "deepfake" [17]. Artificial intelligence (AI) algorithms are routinely used to produce convincing fake photos or movies. According to Lin et al. [18], research on digital face forgeries and the role of digital forensics in identifying and preventing deep fakes is becoming increasingly important as the underlying technology develops. The technology and procedures used to construct them are subject to deep fake research [19]. Machine learning algorithms that can mimic a person's facial expressions, intonation, and mannerisms have been used to make many deepfakes. These algorithms may produce convincing deepfakes that are difficult to discern from real footage, because they can be trained on vast datasets of pictures or videos of the person being impersonated.

The second crucial area of study focuses on the possible impact of deep fakes on people and society. Deepfakes can be used to spread false information, sway public opinion, and damage the reputation of people and businesses [20]. They may also be used for cyberbullying, revenge pornography, and fraud. Deepfakes may be dangerous, which is why there are calls for more regulations and remedies to prevent them from spreading. Another key research area is the value of digital forensics in identifying and examining deep fakes [20]. Experts in digital forensics use diverse tools and techniques to find manipulations or alterations in digital media, including file formats, metadata, and data abnormalities. According to Pan, and Chen [21], by using specialized tools and software such as those that analyze facial movements or find discrepancies in audio or visual data, experts in digital forensics can also identify deepfakes. Digital forensics can be used to identify and examine deep fakes; however, challenges remain. The lack of defined techniques for identifying deep fakes poses a challenge. The methods used to create and identify deep fakes also advance with the technology that produces them [22]. This makes it challenging for digital forensic specialists to remain current with the latest methods and tools.

Another barrier is the challenge of authenticating digital materials. Deepfakes may be constructed to seem genuine, making it challenging to distinguish them from real media. According to Kiruthika and Masilamani [23], digital forensic specialists must inspect materials and identify signs of manipulation or change using specific tools and techniques. Not all investigators have the specialist knowledge and experience required for this. The ethical and legal ramifications of deep fakes are also important areas of study. Deepfake creation and dissemination may have detrimental effects on people and organizations, including damaging their reputations, causing psychological pain, and financial losses [24]. Consequently, there is a growing demand for ethical standards and regulatory frameworks to control the use of deepfakes and guarantee that they are not used for evil [25].

One method for tackling deep-fake causes is the creation of countermeasures. These include methods for identifying and preventing deep fakes, as well as tools for authenticating digital media. An example of a countermeasure is the use of blockchain technology to create tamper-proof digital materials. Blockchain can be used to build a safe and transparent digital ledger that tracks the origin of information, making it more difficult to produce untraceable deep fakes [26]. This literature review focused on the importance of further studies on digital face forgeries and the function of digital forensics in identifying and preventing deep fakes. The assessment also notes important potential difficulties in this area, including the need for standardized techniques for spotting deepfakes, the creation of barriers to stop them from spreading, and the ethical and legal ramifications of deepfake technology.

2.1 Digital Face Forgery

Digital face forgery, commonly referred to as deep faking, uses digital media to synthesize or manipulate false or deceptive information. To create convincing imitation photos or videos, deep fakes employ machine learning algorithms to assess and imitate the motions, facial expressions, and mannerisms of a person. Several methods, such as image and video editing tools, generative adversarial networks (GANs), and autoencoders, can be used to produce deep fakes [27]. Because they require the training of two neural networks, a generator and discriminator, to produce realistic images or videos, GANs are a popular method for producing deepfakes. The discriminator is trained to determine whether a picture or video is genuine or phony, whereas the generator is trained to produce fake images or videos [28]. The generator learns to produce deeper fakes that become increasingly possible through this iterative process.

Digital face fabrication has important consequences, as deep fakes may be used to distribute false information, sway public opinion, and harm people's and organizations' reputations. Deepfakes are used to fabricate news reports, pose politicians, and influence market prices [29]. Deepfakes can also be used for evil intentions such as fraud, cyberbullying, and revenge pornography. Digital forensic professionals face difficulties in identifying and avoiding deep fakes [30]. Digital forensic specialists use a variety of methods, such as reviewing metadata, evaluating file formats, and spotting data abnormalities, to find indications of tampering or changes in digital material. However, as deep-fake technology develops, so do the strategies are being employed in their production and detection. Therefore, it may be difficult for digital forensic professionals to stay current with new methods and equipment.

Digital forensic professionals can employ specialized equipment and software in addition to deep fake detection to identify the origin of a deep fake. This may include investigating additional forensic evidence, such as network logs, as well as the metadata and equipment of the media file that produces the material [31]. Another crucial area of study is the prevention of deep fakes from spreading. Creating techniques for authenticating digital materials, including the use of blockchain technology that generates a tamper-evident digital ledger that traces the origin of information, is a countermeasure to stop the proliferation of deep fakes [32]. Other responses include launching educational efforts to increase awareness of the dangers posed by deep fakes, and designing algorithms that can identify indications of manipulation or change in digital media.

Digital face fabrication, often known as deep fake fabrication, is a rapidly developing technology that presents serious difficulties for both people and companies [33]. Specialized tools and techniques, knowledge, and expertise are necessary to identify and prevent deep fakes [31]. Digital forensic professionals must remain current with the most recent methods and instruments to identify and stop the spread of deepfake technology as it continues to advance. We can contribute to protecting people and organizations from the potentially detrimental effects of digital media manipulation by addressing the issues raised by deep fakes.

3 Techniques used to Create Deepfakes

Deepfakes are digital forgeries that employ artificial intelligence and machine learning methods to produce convincing films, pictures, or audio recordings. These fakes are produced by editing existing materials and faking the target person's voice and facial features to produce a fake media file. Deepfakes are often produced using one of the most well-known methods: generative adversarial networks (GANs) [1]. To create fresh data, GANs combine the neural networks of generators and discriminators. Although the discriminator attempts to distinguish real and fake images, the generator creates fake images or videos. The generator continues to produce increasingly realistic pictures or videos as it gains knowledge from the discriminator feedback [34]. Additionally, a class of neural networks called autoencoders is used to compress and reconstruct the data. Autoencoders are taught to recognize the most crucial aspects of a picture to compress it into a smaller amount of data. The original image is recreated from the compressed data using autoencoders. Autoencoders may be used in the context of deep fakes to recognize a target person's facial traits and then utilize this knowledge to produce a fake picture or video.

Moreover, Deep Neural Networks (DNNs) have been used to produce deep fakes. After training on large face datasets, DNNs may learn to produce new faces that are similar to those in the training set. A single photograph can be used to train DNNs to create 3D representations of a person's face [35]. Realistic movies of subjects can then be produced using these 3D models [4]. A method called Facial landmark detection involves recognizing a person's main facial characteristics such as the eyes, nose, and mouth. This method can be used to project the facial characteristics of a target person onto an existing video or picture. Thus, a deep fake that precisely mimics the facial expressions and body language of the target may be produced. Additionally, a voice synthesis technique was employed to produce synthetic audio recordings that mimicked the voice of a target individual. This method uses a large dataset of audio recordings of the speech of a target person to train a machine-learning model. The model utilizes these data to produce a synthetic voice that closely resembles the intended speaker. In addition, software for manipulating images and video deep fakes may be produced using applications for image and video editing, such as Adobe Photoshop and Premiere Pro [2]. Users of these software tools can modify photos and movies to produce a wide range of effects. However, these methods often lack the effectiveness of those developed utilizing machine learning.

3.1 Potential Impact of Deepfakes on Individuals and Organizations

Deepfakes can seriously injure people and organizations by weakening confidence, disseminating false information, and facilitating fraud. Deepfakes may be used to harm people's reputations at personal and professional levels. A deepfake video or picture might give the impression that someone is talking or doing something they are not; public disgrace, job loss, or even legal repercussions might result from this. For instance, a deepfake video of a politician making incendiary words can spark indignation from the public and harm their image. Furthermore, deepfakes can taint political elections by discrediting candidates or disseminating false information [10]. An election's result may be affected by a deep-fake video or picture that negatively portrays a political candidate. For example, a deep fake video depicting a candidate taking a bribe may persuade people to support their opponents instead of that candidate.

Deepfakes can be used to commit financial fraud by possessing people or entities. An employee or shareholder may be persuaded to transfer money or divulge-sensitive information using a deep fake video of the CEO [36]. In speech synthesis, deep fakes may be used to mimic a person's voice and persuade others to engage in dishonest behaviors. Deepfakes may also propagate false information and disinformation, because they make it difficult to distinguish what is genuine from what is fake. Public misunderstanding and distrust of dependable sources of information may have resulted from this. For example, a deepfake video showing a well-known person making false statements about a health emergency may spread fear and uncertainty.

Deepfakes may endanger national security by undermining the authorities or disseminating misleading information [37]. For instance, a deepfake video depicting a military commander delivering erroneous instructions may result in security breaches or wars. Deepfakes may also be employed by foreign actors to sway public opinion or affect election results [13]. Deepfakes can cause moral and legal problems. It may be challenging to identify both those responsible for producing and disseminating deep fakes, and those responsible for the damage they create. Deepfakes may also breach someone's right to privacy and be used maliciously, as in revenge porns.

As a result, deepfakes can seriously hurt both people and organizations. Deepfake effects may vary from risk to national security and harm one's reputation in personal and professional life. Therefore, it is critical to provide efficient methods for identifying and halting the spread of deep-fake technologies as they continue to advance [18]. In addition, it is crucial to encourage the responsible use of digital media and inform the public about the potential dangers of deep fakes. By addressing these issues, we can preserve the credibility of digital media and safeguard people and organizations from any possible damage caused by deep fakes.

4 Role of Digital Forensic in Investigating Deepfakes

The process of collecting, analyzing, and storing digital evidence for forensic purposes is referred to as "digital forensic.“ This involves employing forensic techniques to examine digital data and equipment such as computers, mobile devices, and networks, among other types of digital media and hardware [38]. Digital forensics is used in many different fields, including law enforcement, corporate investigations, and cybersecurity, to name just a few of them [25]. The use of digital forensics has made the investigation of deep fakes an increasingly important issue over the last several years.

4.1 Tools and Techniques used to Examine Digital Media

Experts in the field of digital forensics examine digital evidence using a wide array of techniques and approaches in order to search for signs of any alterations that may have been made. Data recovery software, hash analysis tools, and forensic imaging software are only a few digital forensic investigation instruments that are regularly used [39]. Experts can examine digital media files using these technologies and identify any anomalies or irregularities that may indicate that the files have been altered or tampered with [26]. In addition to the tools listed herein, digital forensic experts have examined digital evidence using a wide range of investigative methods. Image, audio, and video analyses are a few approaches that fall within this category. Image analysis involves looking at the pixels, colors, and lighting of a photograph to search for indicators in which the image was manipulated in any way [18]. Through audio analysis, a search was conducted using the sound waves included in an audio file to identify any indicators of modification or change. During video analysis, the frames and pixels of a video file are inspected for possible inconsistencies or anomalies that may have occurred.

4.2 Importance of Digital Forensic Experts in Investigating Deepfakes

Digital forensic professionals are required to conduct accurate investigations of deep fakes. The use of deepfake technology is becoming increasingly prevalent, making it increasingly difficult to recognize and differentiate deepfake content. Digital forensics professionals are equipped with the skills and resources necessary to detect and investigate digital media files [31]. This allows professionals to determine whether a media file has been modified. When investigating deep fakes, one of the primary responsibilities of digital forensic specialists is to search media files for any inconsistencies or artifacts that might be present [40]. Deepfake evidence often consists of minute artifacts that are difficult to observe with the naked eye. Digital forensic professionals have the education and practical experience necessary to spot these artifacts and study them to establish whether a media file has been manipulated.

The origin of a deep fake can be tracked by digital forensic professionals if they have the necessary information [41]. Through the analysis of metadata and other digital trails, specialists can determine the source of a deepfake as well as the person who created it. Without this information, it is impossible to hold individuals responsible for the creation and dissemination of profound bogus content [30]. Moreover, in cases involving deep fakes, digital forensic professionals may testify in court as witnesses. Forensic studies that fully disclose their findings may be used as evidence for legal proceedings to establish responsibility for the production and dissemination of deep fake media. Consequently, it is necessary to have experts in digital forensics in hand when investigating deep fakes. They were equipped with the skills and tools necessary to examine digital media assets and identify instances of possible tampering. By recognizing the inconsistencies and anomalies in deep-fake content, digital forensic specialists can determine whether a media file has been modified. They can also establish the source of a deep fake and provide supporting evidence when deep fakes are involved. It is essential to continue creating and improving digital forensic methods as deepfake technology continues to evolve to stay ahead of people who seek to abuse deepfake content for bad motives. This allows one to remain one step ahead of these individuals.

4.3 Challenges Faced by Digital Forensic Experts in Investigating Deepfakes

Owing to the proliferation of deep fakes, digital forensic experts face a variety of challenges when attempting to investigate and identify changed materials. This is because it is difficult to locate deep fakes. One of the most significant challenges that digital forensic experts must overcome is the complex technology employed in the production of deep fakes. The algorithms used for deep fakes are becoming increasingly complicated, making it more difficult to identify fake news [26]. In addition, new deep-fake algorithms are continually being developed, making it difficult for digital forensic experts to keep pace with current advancements in the field. Verifying whether the material in question is original is an additional challenge. Because deepfake creators frequently base their manipulations on real media, it can be difficult to determine whether the original media are authentic. When it is not feasible to analyze the source material, the significance of this issue increases.

Digital forensic professionals often face challenges related to shortages of time, money, and equipment. Under other circumstances, forensic specialists may not have access to the necessary resources or an appropriate level of expertise to accurately evaluate deep fake content. Because of this constraint, their ability to spot and investigate deep fakes may be significantly hindered [25]. In addition, deep fakes sometimes entail the illegal use of people's voices or photos, which may give rise to significant privacy concerns. Therefore, forensic experts are required to strike a balance between the need to identify and investigate deepfakes and respect the rights of individuals to their own privacy. Digital forensic experts face a significant obstacle in the lack of criteria for analyzing deep fakes, which is not the least problematic [42]. Currently, there is no internationally accepted standard for the study and identification of deep fake media, making it impossible for forensic specialists to compare their findings with those of other investigators. Despite these challenges, digital forensic professionals are investing significant effort to remain one step ahead of those who make deep fakes and protect individuals and organizations from any possible damage caused by manipulated media [43]. To address the challenges presented by this cutting-edge technology, researchers are collaborating with experts from various fields to develop novel approaches and tools to detect and investigate deep fakes.

4.4 Need for Specialized Training

Owing to the complex nature of deepfake technology and the fact that it is constantly evolving, individuals working in digital forensics need to receive specialized training to identify and investigate deepfakes. This study covers all the most current deepfake methods and technologies, methodologies for detecting manipulated media, and best practices for obtaining and storing evidence. One of the most significant challenges that digital forensic specialists must overcome is staying current with the latest deepfake tactics and technologies [44]. The algorithms used by Deepfake are constantly updated, and new techniques are being developed to make forgeries more convincing [34]. Experts in digital forensics need to stay abreast of the most current developments in deepfake technology if they are to maintain their track record of success in their investigations.

Professionals in the field of digital forensics require extensive specialized training that includes instructions on how to recognize corrupt content. This training must include a wide range of methodologies including image, audio, and video analyses. It is essential for experts working in digital forensics to be able to differentiate between authentic and false data, although doing so is becoming increasingly challenging as deepfake technology advances. Additionally, specialized training should include instructions on the most effective practices for the collection and storage of evidence [45]. When collecting and analyzing evidence, professionals in the field of digital forensics are required to adhere to a stringent set of rules to guarantee that the evidence is admissible in court. In addition, they must be knowledgeable about a wide range of digital media types and have the ability to retrieve data that have been lost or damaged [30]. In addition to acquiring technical capabilities, digital forensic specialists need to develop "soft skills" such as collaboration and communication in order to be successful in their investigations of deepfakes. They must be able to collaborate effectively across disciplinary lines and communicate their findings to other members of the investigative team, particularly those who specialize in law enforcement and the legal system.

5 Recommendations for Improving the Investigation of Deepfakes

Digital forensic professionals face huge difficulties because of the proliferation of deep fakes. For digital forensic professionals to operate, defined standards for the analysis of deep fakes can be created. Standardization may make it easier to compare forensic specialist results with those of other investigators and guarantee that they use a uniform technique. Additionally, to create new methods and instruments for detecting and examining deep fakes, digital forensic specialists should work with specialists from other disciplines, such as artificial intelligence, machine learning, and computer science. By keeping up with the most recent advancements in deepfake technology, collaboration may assist forensic specialists in remaining a step ahead of deepfake makers. Digital forensic professionals may create new methods and tools for locating and analyzing deep fakes with the aid of more money and resources. This may include investing in R&D and granting access to cutting-edge equipment.

Deepfake detection and investigation should be the focus of training for digital forensic professionals. The most recent deep fake tools and techniques should also be covered, along with the finest methods for assessing digital materials. Additionally, creating public awareness campaigns can assist people and organizations in realizing the dangers posed by deep fakes. In addition, by encouraging people to report suspected deep fakes, these campaigns can provide forensic experts with more information. Experts in digital forensics must strike a compromise between the necessity of locating and examining deep fakes and the protection of people's privacy rights. Forensic specialists can guarantee that their investigations respect people's rights by creating standards and best practices for handling privacy issues.

6 Conclusion

The proliferation of deepfakes poses significant challenges for digital forensic specialists in identifying and examining manipulated materials. Forensic professionals face difficulties due to the advanced technology used to create deepfakes, the challenge of authenticating original content, limited resources, privacy concerns, and the absence of standardized practices. However, by continuously developing new methods and tools, fostering interdisciplinary collaborations, and providing specialized training, digital forensic professionals can enhance their ability to detect and analyze deepfakes. It is crucial for individuals, businesses, and governments to recognize the potential impact of deepfakes and take proactive measures to prevent their malicious use. This includes investing in the development of detection tools and methodologies, educating digital forensic specialists, and establishing industry-wide standards for deepfake investigations. As technology evolves rapidly, digital forensic specialists must remain vigilant and proactive in their efforts to combat deepfakes. By staying ahead of deepfake creators, digital forensic specialists can play a crucial role in safeguarding individuals and organizations from the significant harm caused by manipulated media.

References

1. Lavrence, Christine and Cambre Carolina. 2020. ‘Do I look like my selfie?’: filters and the digital-forensic gaze. Social Media + Society 6(4). https://doi.org/10.1177/2056305120955182.
2. Leone, Massimo. 2021. From fingers to faces: visual semiotics and digital forensics. *International Journal for the Semiotics of Law-Revue Internationale de Sémiotique Juridique* 34 (2): 579–599. https://doi.org/10.1007/s11196-020-09766-x.
3. Saugmann, Rune. 2020. The security captor, captured. Digital cameras, visual politics and material semiotics. *Critical Studies on Security* 8 (2): 130–144. https://doi.org/10.1080/21624887.2020.1815479.
4. Ross, Arun, Banerjee Sudipta, and Chowdhury Anurag. 2020. Security in smart cities: a brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters* 138: 346–354. https://doi.org/10.1016/j.patrec.2020.07.009.
5. Poulsen, Søren. 2021. Face off–a semiotic technology study of software for making deepfakes. *Sign Systems Studies* 49 (3–4): 489–508. https://doi.org/10.12697/SSS.2021.49.3-4.12.
6. Seibold, Clemens, and Samek Wojciech, Hilsmann Anna, and Eisert Peter. 2017. Detection of face morphing attacks by deep learning. In *Digital Forensics and Watermarking: 16th International Workshop. Proceedings 16, 107–120* Magdeburg, Germany: IWDW, August 23–25, 2017. Springer International Publishing.
7. Javed, Abdul and Jalil Zunera. 2020. Byte-level object identification for forensic investigation of digital images. In 2020 *International Conference on Cyber Warfare and Security (ICCWS) 1–4*. IEEE Publications. https://doi.org/10.1109/ICCWS48432.2020.9292387.
8. Al-Khateeb, Haider, Epiphaniou Gregory, and Daly Herbert. 2019. Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger. Blockchain and Clinical Trial: Securing Patient Data 149–168. https://doi.org/10.1007/978-3-030-11289-9_7.
9. Tripathi, Arun. 2022. A proactive improvement toward digital forensic investigation based on deep learning. Deep Learning in Visual Computing and Signal Processing 237.
10. Neubert, Tom. 2017. Face morphing detection: An approach based on image degradation analysis. In *Digital Forensics and Watermarking: 16th International Workshop. Proceedings 16, 93–106* Magdeburg, Germany: IWDW, August 23–25, 2017. Springer International Publishing.
11. Balushi, Al, Shaker Yusra, Hothefa, and Kumar Basant. 2023. The use of machine learning in digital forensics. In *1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, 96–113. Atlantis Press.
12. Khudhair, Zaid, Mohamed Farhan, and Kadhim Karrar. 2021. A review on copy-move image forgery detection techniques. *Journal of Physics: Conference Series* 1892: 1: 012010. IOP Publishing. https://doi.org/10.1088/1742-6596/1892/1/012010.
13. Amjed, Alaa, Mahmood Basim, and Almukhtar Khalid. 2022. Approaches for forgery detection of documents in digital forensics: A review. In *Emerging Technology Trends in Internet of Things and Computing*, *Revised Selected Papers: First International Conference, TIOTC 2021*, Erbil, Iraq, June 6–8, 2021, 335–351. Cham: Springer International Publishing.
14. Patel, Shubham and Singh Rajendra. 2022. Digital forensics: Fundamentals and awareness to society against cybercrime. *Journal of Advancements in Robotics* 9 (2): 37–41.
15. Paul Joseph, D., and Norman, and Jasmine. 2019. An analysis of digital forensics in cyber security. In *First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018*, 701–708. Singapore: Springer.
16. Chaturvedi, Aparna, Awasthi Aashish, and Shanker Surabhi. 2020. Cyber forensic - A literature review. *Trinity Journal of Management IT and Media* 10 (1): 24–29.
17. Englbrecht, Ludwig, Meier Stefan, and Pernul Gunther. 2020. Towards a capability maturity model for digital forensic readiness. *Wireless Networks* 26 (7): 4895–4907. https://doi.org/10.1007/s11276-018-01920-5.
18. Lin, Xiaodong. 2018. *Introductory computer forensics*. Springer International Publishing.
19. Swain, Aanasuya. 2020. Big data challenges and hype digital forensic. Big Data Analytics and Computing for Digital Forensic Investigations *43*.
20. Powell, Ashleigh and Haynes Cyndee. 2020. Social media data in digital forensics investigations. Digital Forensic Education: An Experiential Learning Approach 281–303. https://doi.org/10.1007/978-3-030-23547-5_14.

21. Pan, Weiwei and Chen Guolong. 2016. A method of off-line signature verification for digital forensics. In *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 488–493. IEEE Publications. https://doi.org/10.1109/FSKD.2016.7603222.
22. Yaacoub, Jp, Noura Hassan, and Salman Ola, and Chehab Ali. 2022. Advanced digital forensics and anti-digital forensics for IoT systems: techniques, limitations and recommendations. *Internet of Things* 19: 100544. https://doi.org/10.1016/j.iot.2022.100544.
23. Kiruthika, S., and Masilamani Vedhanayagam. 2023. Image quality assessment based fake face detection. *Multimedia Tools and Applications* 82 (6): 8691–8708. https://doi.org/10.1007/s11042-021-11493-9.
24. Årnes, Andre. 2017. *Digital forensics*. John Wiley & Sons.
25. Tyagi, Shobhit and Yadav Divakar. 2022. A detailed analysis of image and video forgery detection techniques. The Visual Computer 1–21.
26. Feng, Disheng, Lu Xuequan, and Lin Xufeng. 2020. Deep detection for face manipulation. In *Neural Information Processing. Proceedings part V 27: 27th International Conference, ICONIP 2020*, Bangkok, Thailand, November 18–22, 2020, 316–323. Springer International Publishing.
27. Kävrestad, Joakim. 2020. *Fundamentals of digital forensics*. Springer International Publishing.
28. Naick, Doraswamy and Bachalla Neelima. 2016. Application of digital forensics in digital libraries. *International Journal of Library and Information Science (IJLIS)* 5 (2): 89–94.
29. Das, Dolly, Shaw Urjashee, and Medhi Smriti. 2017. Realizing digital forensics as a big data challenge. In *4th International Conference on Computing for Sustainable Global Development, New Delhi*.
30. Bakas, Jamimamul, Naskar Ruchira, and Nappi Michele, and Bakshi Sambit. 2021. Object-based forgery detection in surveillance video using capsule network. *Journal of Ambient Intelligence and Humanized Computing* 12 (1): 1–3.
31. Quick, Darren and Choo Kkwang Raymond. 2016. Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing* 19 (2): 723–740. https://doi.org/10.1007/s10586-016-0553-1.
32. Al-Duwairi, Basheer, Shatnawi Ahmed, Jaradat Hala, Al-Musa Afnan, and Al-Awadat Hamzah. 2022. On the digital forensics of social networking web-based applications. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. IEEE Publications.
33. Khan, Abdulla, Shaikh Aftab Ayub, Laghari Asif Ahmed, Dootio Mazhar Ali, Rind Ali, and Malook, and Awan Shafique Ahmed. 2022. Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics* 14 (2): 124–150. https://doi.org/10.1504/IJESDF.2022.121174.
34. Ferreira, Sara, Antunes Mario, and Correia Manuel. 2021. Forensic analysis of tampered digital photos. In *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, *Revised Selected Papers 25: 25th Iberoamerican Congress, CIARP 2021*, Porto, Portugal, May 10–13, 2021, 461–470. Springer International Publishing.
35. Aggarwal, Ananta. 2021. Critical analysis of digital forensic in criminal justice. *Supremo Amicus* 26: 49.
36. Casino, Fran, Dasaklis Thomas, Spathoulas Georgios, and Anagnostopoulos Marios, et al. 2022. Research trends, challenges, and emerging topics in digital forensics: a review of reviews. *Ieee Access : Practical Innovations, Open Solutions* 10: 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059.
37. Kebande, Victor and Venter Hendrik. 2018. On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences* 50 (2): 209–238. https://doi.org/10.1080/00450618.2016.1194473.
38. Wilson-Kovacs, Dana. 2019. Effective resource management in digital forensics: an exploratory analysis of triage practices in four English constabularies. *Policing: An International Journal* 43 (1): 77–90. https://doi.org/10.1108/PIJPSM-07-2019-0126.
39. Kumari, Shabnam, Tyagi Amit Kumar, and Rekha Gangula. 2021. Applications of blockchain technologies in digital forensics and threat hunting. In *Recent trends in blockchain for information systems security and privacy*, 159–173. CRC Press.
40. Zhu, Xiangyu, Wang Hao, Fei Hongyan, and Lei Zhen, and Li Stan. 2021. Face forgery detection by 3D decomposition. In *Proceedings IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2928–2938. https://doi.org/10.1109/CVPR46437.2021.00295.
41. Vincze, Eva. 2016. Challenges in digital forensics. *Police Practice and Research* 17 (2): 183–194. https://doi.org/10.1080/15614263.2015.1128163.

42. Yang, Ke, Li Da, Guo Qinglei, Wang Hejian, Bai Desheng, and Pan Xiukui. 2022. Research on deep forgery data identification and traceability technology based on blockchain. In *IEEE 2nd International (Ed.) 2022 Conference on Data Science and Computer* Application *(ICDSCA)*, 230–234. IEEE Publications. https://doi.org/10.1109/ICDSCA56264.2022.9988274.
43. Vinolin, V., and M. Sucharitha. 2021. Dual adaptive deep convolutional neural network for video forgery detection in 3D lighting environment. *The Visual Computer* 37 (8): 2369–2390. https://doi.org/10.1007/s00371-020-01992-5.
44. Chen, Guangxuan, Wu Di, Chen Guangxiao, and Hu Bo, and Huang Anan. 2020. *Discussion on the talents cultivation of digital forensics* DOI: https://doi.org/10.38007/Proceedings.0000961.
45. Tembe, Anushree and Thombre Supriya. 2017. Survey of copy-paste forgery detection in digital image forensic. In *International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 248–252. IEEE Publications. https://doi.org/10.1109/ICIMIA.2017.7975613.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.