Review of Recent Trends in Face Image Authentication (FIA) Techniques and Their Limitations

Asmaa Hatem Jawad[*], Rasha Thabit[**], Khamis A. Zidan[***]

[*] Department of Computer Engineering, Al-Iraqia University, Baghdad, Iraq
Email: asmaahatem876@gmail.com
https://orcid.org/0009-0008-7637-0135

[**] Department of Computer Engineering, Al-Iraqia University, Baghdad, Iraq
Email: rasha.thabit@aliraqia.edu.iq
https://orcid.org/0000-0003-4141-5723

[***] Vice Rector of Al-Iraqia University for Scientific Affairs, Al-Iraqia University, Baghdad, Iraq
Email: khamis_zidan@aliraqia.edu.iq
https://orcid.org/0000-0002-3739-7270

Abstract

The rapid advancement of face image manipulation (FIM) algorithms and the proliferation of their user-friendly applications underscore an urgent need for manipulation detection techniques. These methods should be capable of revealing modifications in face images and substantiating their authenticity. Recently, the term "DeepFakes" and their detection techniques have attracted the attention of the research community. In addition, pay attention to the most recent techniques for detecting facial image manipulation that utilize watermarks. It's crucial to note that each of these techniques comes with its own set of limitations. This research aims to critically evaluate recent developments in face image authentication (FIA) methods, considering the widespread and user-friendly applications of FIM algorithms and their rapid growth. This study focuses on the urgent necessity for effective manipulation detection methods that can reliably identify and verify modifications in facial images, particularly with the rise of sophisticated DeepFakes. It explores two primary detection approaches: deep learning (DL) techniques, which leverage large datasets to detect subtle manipulations, and watermarking-based methods, which embed verification data into images to safeguard authenticity. The findings showcase the positive aspects and the limitations of these methods. DL techniques are powerful in detecting complex alterations but require substantial computational resources and data for training.
Conversely, watermarking offers a proactive solution for verifying image integrity but may be vulnerable to advanced manipulation tactics and can impact image quality. The review emphasizes the importance of ongoing innovation, advocating for hybrid approaches that integrate the benefits of both DL and watermarking to overcome their shortcomings. This paper serves as a crucial reference for researchers, presenting a detailed overview of current trends, challenges, and future directions in face image manipulation detection (FIMD), underscoring the need for continuous development to keep pace with advancing manipulation technologies.

Keywords- Face image authentication (FIA), Face image manipulation (FIM), Face image manipulation detection (FIMD), DeepFakes.

I. INTRODUCTION

Digital images can now be effortlessly shared for various purposes as technology advances [1]–[3]. Nowadays, technology users find it highly convenient to store their photos and private data in the cloud, allowing them to access it whenever needed. However, users' primary concerns revolve around security and data integrity [4], [5]. Various methods and security frameworks, including watermarking, steganography, and cryptography, have been implemented to guarantee the security of digital images and shared data [6]–[8].

One of the most significant categories of digital images is the face image shared online for various purposes such as social media, face recognition applications, celebrity and fame intentions, and identity discrimination in biometric systems (i.e., security and access control) [9]. The use of face images extends to many more applications [10]–[12].

Digital face manipulation methods, algorithms, and applications have become widely accessible in recent years owing to the rapid advancement of technology [13]–[17]. Techniques for manipulating facial images can be broadly categorized into two groups: intentional attacks, which involve harmful intentions during the manipulation process, and unintentional attacks, which entail innocent intentions such as beautifying the face, adjusting lighting, adding amusing stickers, etc. Both manipulation techniques result in alterations to the facial image content (i.e., changing its features) [18].

The field of data security has witnessed a surge in interest concerning face image manipulation (FIM) methods and their impact on data security systems. The term "DeepFakes" has captured the attention of the research community in recent years, leading to the emergence of a thriving field of study [19]–[24]. Deep learning (DL) techniques have been employed to generate fabricated digital content, commonly known as DeepFakes. In 2017, a machine learning algorithm called DeepFakes was developed to replace celebrity faces in pornographic videos [25]. Various harmful purposes, including financial fraud, the spread of fake news, and the creation of explicit content, have exploited the capabilities of DeepFakes [26]. In efforts to enhance media forensics in general, researchers have focused on developing face manipulation detection algorithms [27]–[32].

The field of manipulated facial image generation is still in its early stages of development. Many papers provide a thorough examination of the methods used to create images of manipulated faces, with a particular emphasis on deepfakes and emerging techniques for detecting fake images [33].

In the realm of digital image processing, the authenticity and integrity of facial images have become paramount due to the rise of sophisticated manipulation techniques. The emergence of DeepFakes and other advanced manipulation methods has underscored the critical need for robust face image authentication (FIA) techniques to combat the spread of deceptive content. In this context, Pepper's research topic holds significant importance as it aims to explore recent advancements in FIA methods and address the challenges posed by the widespread use of FIM algorithms.

The problem at hand revolves around the vulnerability of facial images to malicious alterations, whether for deceptive purposes or innocent beautification. The significance of this issue lies in the potential consequences of manipulated images, ranging from misinformation and identity theft to privacy breaches and reputational damage. As such, developing effective FIA techniques is crucial to safeguarding the authenticity and trustworthiness of facial images in various applications, including social media, forensics, and biometric systems.

Key concepts and terminology central to this research include FIM techniques, intentional and unintentional attacks on facial images, DeepFakes, watermarking-based FIM detection, and DL algorithms. Understanding these terms is essential for grasping the nuances of face image manipulation and the detection methods employed to mitigate its risks.

The primary objectives of this review paper are to critically examine recent trends in FIA techniques, identify the limitations of existing approaches, and propose avenues for enhancing the capabilities of manipulation detection algorithms. By delving into the distinctions between image tampering, manipulation, and forgery, the research aims to shed light on the complexities of detecting and mitigating digital face manipulations. Furthermore, the proposed approach will involve exploring the potential of DL-based techniques, developing comprehensive manipulation detection algorithms, and forecasting future directions to advance the field of FIA. In summary, the paper seeks to address the pressing need for robust FIA techniques in the face of evolving manipulation methods, emphasizing the importance of authenticity and trust in facial images across various domains. By elucidating the challenges and opportunities in this field, the research endeavours to contribute to the ongoing efforts to combat digital face manipulation and safeguard the integrity of visual content.

The next section summarises the recently published review papers in the field of FIM and its detection techniques. To current date no review paper has focused on the recent FIA schemes. Therefore, this paper presents a review of recent trends in FIA techniques and their limitations. The rest of the paper is organized as follows: section II presents a summary of some review papers that are related to the FIM and FIMD schemes; section III presents the types of FIM techniques; section IV presents a review of face image manipulation detection (FIMD) techniques; section V presents a comparison between DL-based and watermarking-based FIMD techniques; and section VI presents the conclusions and suggestions for future researches.

II. REVIEW PAPERS SUMMARY

Studies have investigated various aspects of FIA, exploring the effectiveness of DL and watermark-based for detecting tampering. Researchers emphasize the need for robust manipulation detection algorithms to combat sophisticated DeepFakes and advanced manipulation tactics. Recent research focuses on using large datasets, novel algorithms, and innovative frameworks to enhance the accuracy and reliability of facial image authentication systems.

The study in this section will summarise recently published review papers related to the field of FIM and FIMD, including references, year of publication, and initial contributions, as shown in Table 1.

TABLE 1. REVIEW PAPERS SUMMARY

Ref.	*Year*	*Contributions*
[24]	2020	- Explained what a deepfake is and provided a rundown of the core technologies. - Categorized deepfake techniques and examined the opportunities and risks associated with each group. - A framework was established for successfully addressing the risks of deepfake.
[13], [34]	2020	- Conducted a comprehensive analysis of contemporary face manipulation techniques, encompassing deepfakes, and explored methods for detecting them. - Classified these techniques into four major categories based on their prevalent use in facial manipulation. - Examined publicly accessible datasets and essential benchmarks for detecting manipulated faces and assessing face manipulation techniques.
[35]	2020	- Conducted a comprehensive analysis of prevalent image forgery techniques. - Provided an overview of publicly available data sources for research on the identification of image manipulation. - Emphasized a primary focus on DL-based methods for detecting image manipulation.
[36]	2020	- Conducted an in-depth investigation to detect alterations in both photos and videos. - Emphasized the newly identified deepfake phenomenon from a forensic analyst's perspective. - Outlined the limitations of the latest forensic software, addressed pressing issues, examined imminent challenges, and proposed avenues for new lines of inquiry.
[37]	2020	- Reviewed the recent advancements and applications of semantic manipulation and face synthesis based on DL. - Discussed future perspectives aimed at further enhancing face perception through continued development and innovation.
[38]	2020	- Outlined the distinctions and interrelations among image tampering, image manipulation, and image forgery. - Provided justifications for various tampering detection techniques, highlighting their unique strengths and applications. - Investigated prevalent benchmark datasets commonly used in the assessment of tampering detection methods.
[39]	2021	The study investigates various state-of-the-art neural networks, such as MesoNet, ResNet-50, VGG-19, and Xception Net, with a specific emphasis on addressing complex issues posed by deepfakes generated through neural networks. To identify the most effective outcomes, the paper includes comparisons among the aforementioned methods.
[40]	2021	- Investigated the most recent techniques for creating and identifying deepfake photos. - Focused on summarizing and scrutinizing the architectures of methods for both generating and detecting deepfakes. - Presented future directions aimed at enhancing the architecture of deepfake models.
[41]	2021	- Aimed to present the latest findings in the identification and production of deepfake videos. - Evaluated the generalization and robustness of deepfake video generation and detection models. - Outlined the existing benchmarks for deepfake video creation.
[42], [43]	2021, 2022	A comprehensive analysis of deepfake detection using DL techniques: - Conventional neural network (CNNs)-based techniques. - Generative adversarial networks (GANs)-based techniques. - Recurrent Neural Network (RNN). - Long short-term memory (LSTM). - Autoencoder-based techniques.
[44]–[46]	2021, 2022	- Explored the latest techniques in the creation and detection of deepfakes. - Presented current datasets related to deepfake technology. - Examined prevalent issues and patterns associated with the production and identification of deepfakes.
[33]	2023	- Categorizes and discusses the latest research on face manipulation detection and generation. - Covering over 160 studies, it provides a comprehensive discussion of the subject. - The primary focus of the paper is on the creation and detection of deepfake content using DL. - Identifying obstacles, addressing unanswered research questions, and forecasting future directions, contribute to the advancement of digital face manipulation generation and detection.
[34]	2024	- Introduction of a novel FIA scheme utilizing image watermarking and Cohen–Daubechies–Feauveau (CDF) wavelets to detect manipulations in face images and recover the original face region post-manipulation localization. - Demonstrate the scheme's effectiveness in generating high-quality watermarked images, detecting various manipulations, localizing manipulated blocks in the face region, and successfully recovering the face region with good visual quality.

Despite the progress made in facial image authentication research, there remain limitations and gaps in existing literature despite the progress made in facial image authentication research. The challenges with FIMD techniques that rely on DL include (a) the need for large and high-quality datasets, which can be difficult to obtain, (b) algorithms are only effective when test images are similar to the training dataset. Otherwise, the error rates are significant, (c) limited generalization in available DL-based techniques, (d) high time complexity, where training can take days to complete. Watermarking-based FIMD techniques solved the previous problems of DL-based techniques but suffered from the following problems: (a) they cannot detect and identify various manipulation locations in facial images with 100% accuracy. However, it is unable to retrieve the original face. (b) It can recover the original facial region but suffers from poor embedding ability, which limits the number of images that can be protected.

Our review approach aims to build on and improve existing solutions in facial image authentication by addressing limitations and gaps identified in the literature. By synthesizing insights gained from previous research, we intend to propose innovative methodologies, hybrid approaches, and advanced frameworks that enhance tampering detection algorithms' accuracy, efficiency, and robustness. Through a comprehensive analysis of the field's current state, our review seeks to contribute to the ongoing development of facial image authentication and tampering detection and provide practical insights and advances for future research endeavours.

III. TYPES OF FIM TECHNIQUES

As previously stated, the process of FIM has become a prevalent topic in the last few years, especially after the term "DeepFakes" was recently distributed and highlighted by state-of-the-art researchers [13], [18]–[20], [22], [26], [47]–[50].

Several FIM techniques exist, and new manipulation methods are constantly introduced through improved applications. Nevertheless, most research has focused on the manipulation methods depicted in Table 2, which briefly explains the common manipulation types. Figure 1 presents the classification of the FIM.

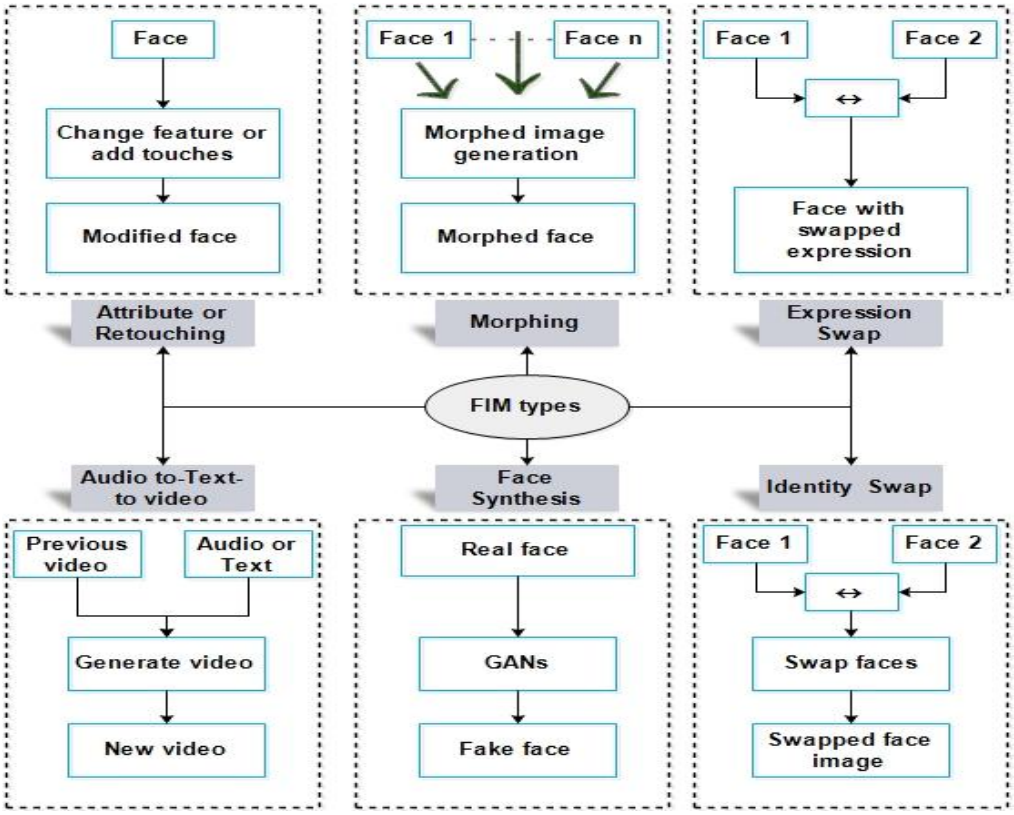

Figure 1. Common types of FIM techniques [111].

TABLE 2. THE COMMON TYPES OF FIM TECHNIQUES

No.	*Manipulation type*	*Explanation*
1	Entire face synthesis	Utilizes GANs to generate virtual human faces that closely resemble real human faces. The generated faces can be used in various applications such as email, games, teleconferences, chat rooms, and various other contexts [16], [17].
2	Identity swap	This manipulation process involves replacing the person's face image with another face image, which can be used in a variety of applications, including the film industry, financial fraud, and video fabrication. The identity swap manipulation methods are divided into two categories: a) classical computer graphics-based techniques [35] and b) DL-based techniques [36].
3	Morphing	In this type of manipulation, a single morphed image is created by combining images from two or more people using specific software tools such as "Face Morph", "Face Swap Online", and the "morphed thing" [37]. The process of face morphing is focused on creating fake samples for photos, not for video. Furthermore, the front view of the face is usually considered in the process of manipulation [38]–[42].
4	Attribute manipulation	This manipulation process, also known as "face editing" or "face retouching" is used to change images based on attributes such as the colour of individuals' hair or skin, their age, gender, the addition of a beard or glasses, and so on [43]–[45]. In most cases, this type of manipulation is considered an unintentional attack and is used to improve image quality. One example of this type of manipulation is the popular 'Snapchat' mobile application [46].
5	Expression Swap	The process of replacing an individual's facial expressions in a video clip with those of another individual [43], [44].
6	Audio-to-Video and Text-to-Video Swap	This type of manipulation is based on artificial intelligence (AI) techniques, and certain aspects must be considered, such as sounds, 3D face pose, expression, and scene light [47]–[49].

The FIM can be used for a variety of purposes, both harmless and harmful [14], [66][13]. Table 3 provides a brief description of the applications in which the FIM can be utilized.

TABLE 3. DESCRIPTION OF FIM EXAMPLE APPLICATIONS

No.	*FIM Application*	*Description*
1	Spread Fake News	Images and videos are manipulated and edited to spread fake news on internet websites, magazines, and social media [67].
2	Digital Communication	Images are used in a variety of communication applications, including online registration and social media friendship [68].
3	Security Applications	Services include identity verification, online access control, identification, and authentication [69].
4	Entertainment	The FIM is used in entertainment to create videos, advertisements, and other content. Some companies specialize in creating amusing cartoons from still images using lip-syncing technology [70]–[72].
5	Film Industry	Deepfakes have been used in the film industry for a variety of purposes, including changing the identity of the person in the recorded video and lowering costs by generating characters with AI tools [32], [73]–[75].
6	E-Commerce	Retailers have used deepfake technology to create tools that allow customers to swap their faces with digital models in virtual changerooms, potentially increasing online sales. Furthermore, ideal fake models generated using AI technology are used for advertisements at a significantly lower cost than real models [76].
7	E-Learning	Deepfake technology has the potential to improve children's education in a variety of ways, including swapping the teacher's face with their parents to help them coalesce and reinforce learning [66]. On the other hand, instructors can use the text and previous videos to create new video courses [77].

IV. FIMD TECHNIQUES

The face recognition system (FRS) is a subset of biometric security software that also includes voice recognition, fingerprint recognition, and iris recognition [39], [50], [51]. The FIM process affects image quality, which can influence acceptance or rejection decisions in FRS [52]–[57]. When a fake image is accepted in FRS, it poses a threat to the entire security system and is viewed as a significant challenge to privacy control. On the other hand, intentional FIM attacks can lead to a variety of issues, including identity theft [58]–[61], political conflict as a result of fake news [62]–[66], financial fraud, and others.

Since the number of harmful FIM applications is rapidly increasing, researchers have directed their efforts toward presenting manipulation detection techniques that can distinguish fake face images from authentic images [14], [62], [67]–[70]. In recent years, several FIMD algorithms have been presented, which can be broadly classified into two types: differential-based algorithms and no-reference-based algorithms [71]–[77]. The differential detection algorithms require two images: the original image (the reference image) and the test image. These algorithms demonstrated their effectiveness in detecting manipulation; however, in traditional image forensics, there is only one video or image. Several studies have been directed toward detecting tampering when the trusted reference image is not available [77]–[82].
Currently, four types of FIMD schemes are available:

A. FIMD based on texture analysis

The study focuses on assessing the susceptibility of FRS to morphing attacks and proposes a novel technique for detecting such attacks. The suggested approach combines multiple Multi-scale Block Local Binary Patterns (MB-LBP). The study emphasizes that training and evaluating face morphing attack detection algorithms depend on robust morphing detection algorithms and the utilization of diverse databases [102].

B. FIMD based on digital forensics

The study investigates the impact of face retouching on face recognition and proposes a detection method based on Photo-Response Non-Uniformity (PRNU) for retouched face photos. The research assesses biometric performance both before and after retouching, coupled with a qualitative evaluation of beautification apps. The findings suggest that facial retouching only marginally decreases comparison scores. However, accurate identification of retouched face photos is crucial for upholding laws against Photoshop manipulation [103].

C. FIMD based on DL or AI

According to its definition, Deepfakes is a DL-based method that replaces a person's face with another person's face to produce fake videos. The method creates realistic images and videos using GANs that can be exploited for financial fraud, fake news, and other malicious activities [14], [31], [40], [66], [104], [105]. Table 4 summarizes some limitations of FIMD based on DL.

D. FIMD based on face detection and image watermarking

Another FIMD technology has recently been presented, which involves the utilization of face detection and image watermarking algorithms. Upon identifying the face region, the image blocks undergo classification into two groups: those associated with the face region and those that are not. This classification is achieved by generating a binary mask image. The manipulation process unveils the application of Slantlet-based image watermarking, which is employed to extract data from blocks within the face region and embed it into blocks that are outside of this region [107], [108]. Table 5 summarizes some limitations of FIMD based on watermarking.

A new FIA scheme employs a Multi-Task Cascaded Neural Network (MTCNN) for detecting and selecting the face region, followed by output adjustments. Subsequently, a binary mask image is generated based on the identified face region, facilitating the categorization of image blocks into two groups: face blocks and non-face blocks. Tamper localization data is derived by calculating the mean of each block from the face region. Then, the Bicubic interpolation (BI) algorithm is applied to generate recovery data from the face region. Using a content-based embedding algorithm capable of embedding binary bits in the High-Low (HL) and Low-High (LH) subbands of the Slantlet transform (SLT) coefficients of the block, the system embeds the generated binary sequence into the non-face blocks. In the presence of manipulations, the system reliably identifies tampered blocks within the face region and restores the original face region [109]–[111]. Figures 3 and 4 offer a comparison of the FIMD and FIA schemes on both the sender and receiver sides. The FIMD scheme is designed to detect and locate tampering, but it cannot recover the original face data. On the other hand, the FIA scheme not only detects tampering and identifies its location but also can retrieve the original face region.

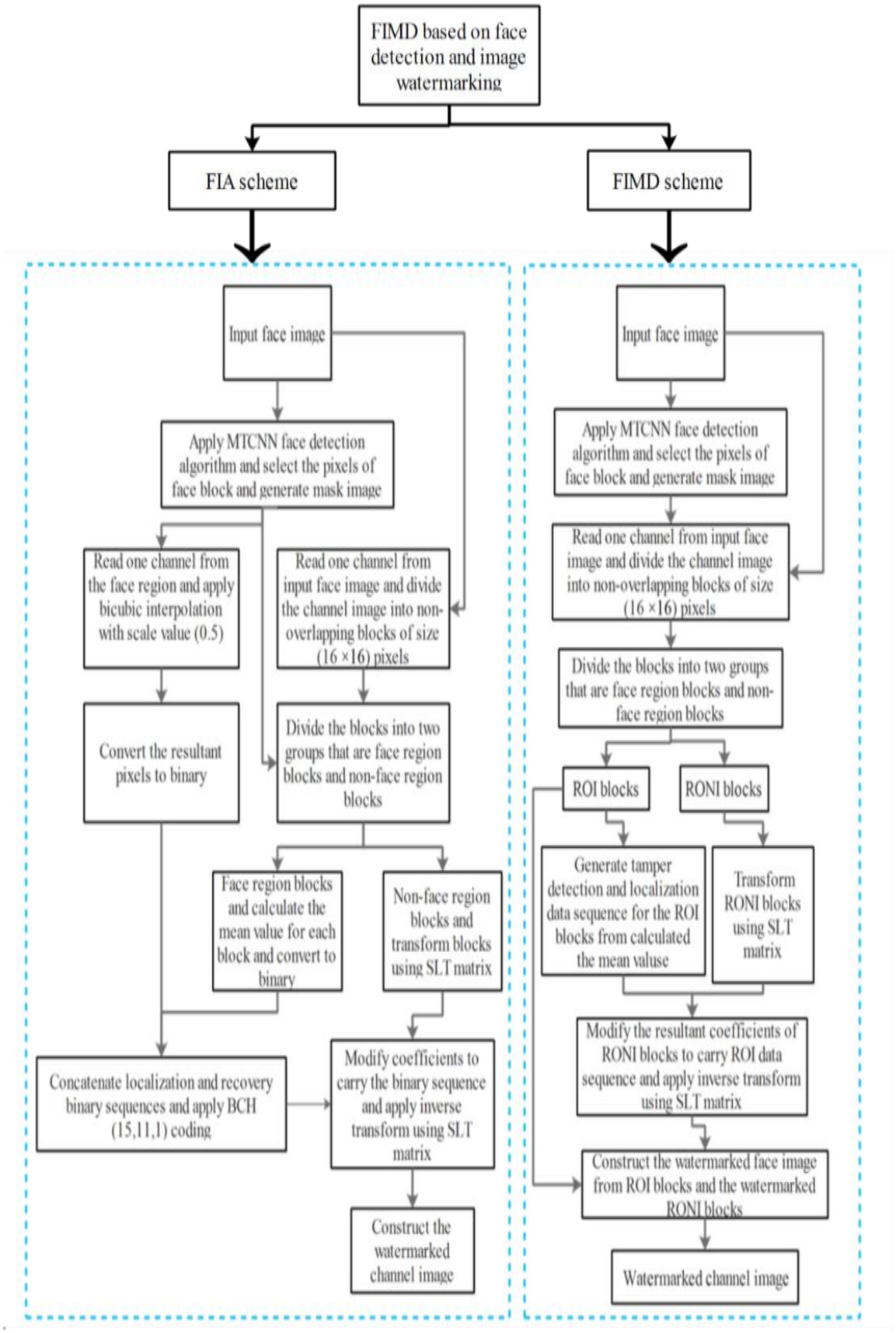

Figure 2. Comparison of FIMD and FIA schemes on the sender side of a single channel [108], [110].

ISSN: 2710-2165

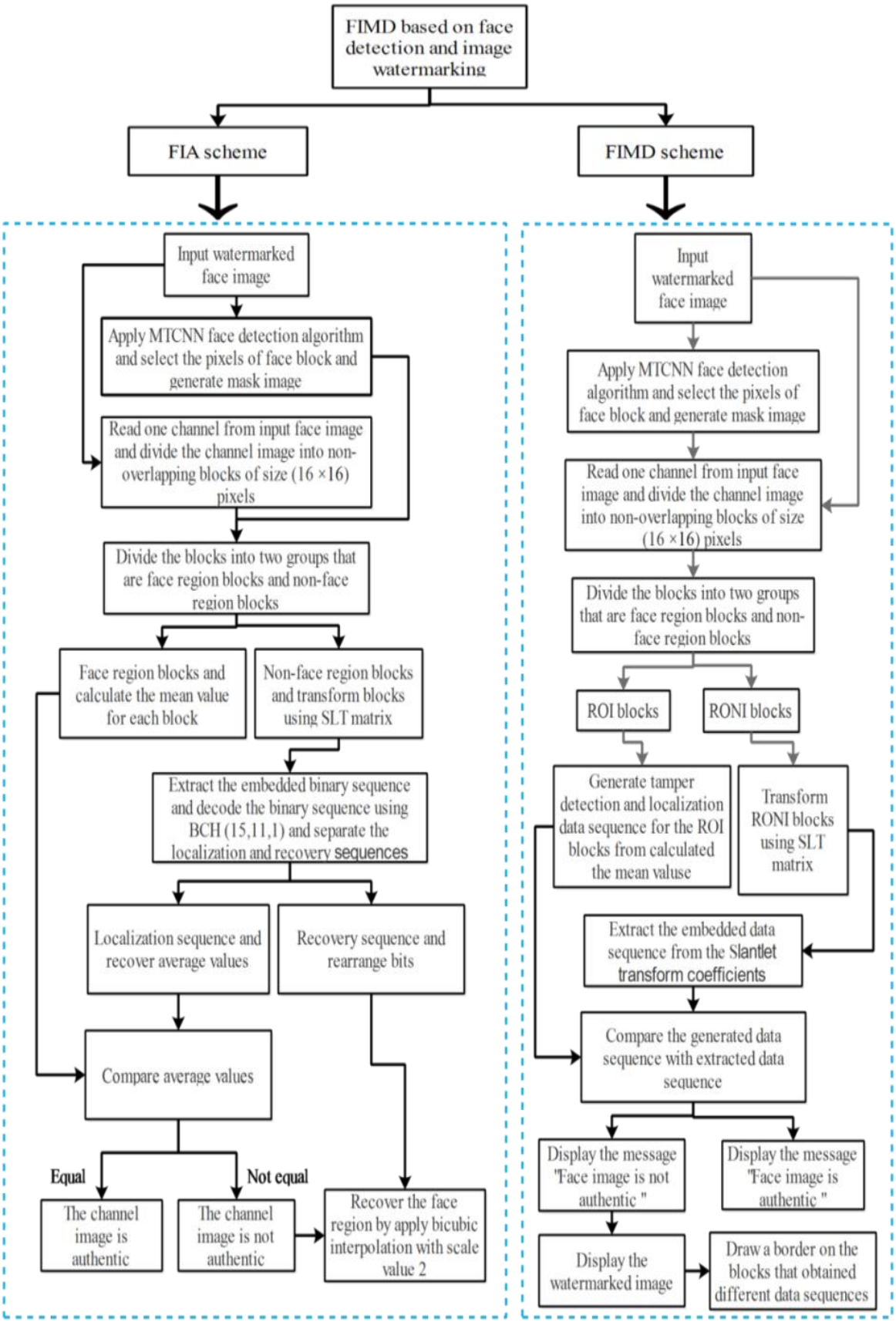

Figure 3. Comparison of FIMD and FIA schemes on the receiver side of a single channel [108], [110].

TABLE 4. SUMMARY OF SOME LIMITATIONS IN DL-BASED FIMD.

Ref.	*Detected features*	*Limitations*
[83]–[85]	Face Asymmetries	1- Small details often go unnoticed. 2- Accurate detection requires high-resolution images, which are challenging to find on social media networks. 3- It involves a high level of computational complexity. 4- It can identify a specific type of manipulation.
[86]	Landmark locations	1- Relying on landmark locations in face photos as a discriminative feature is not always dependable. 2- When sharing images over networks, having the front-face view is not always necessary. 3- It can identify a specific type of manipulation.
[87], [88]	Color features	1- A substantial training set is necessary. 2- It involves a high level of computational intricacy. 3- Abundant computational capacity is required. 4- It can identify a specific type of manipulation.
[89]	Spatial artifacts	1- A sizable training set is necessary. 2- Training takes a considerable amount of time. 3- The computation techniques involved are challenging. 4- The precision and capability of manipulation detection are limited.
[79], [90]–[95]	Different features as inputs to CNN	1- A substantial training set is necessary. 2- Training takes a considerable amount of time. 3- Involves complex computation techniques. 4- The precision and capability of manipulation detection are limited.
[70]	Spectral distribution	1- Errors may occur when utilizing the energy spectral distribution. 2- Training takes a considerable amount of time. 3- Involves a convoluted calculation method. 4- It can identify a specific type of manipulation.
[96]–[98]	Spectral artifacts fitting parameters	1- Intricate computation techniques. 2- It took a significant amount of time to find the fitting parameters during post-processing. 3- Is limited to identifying GAN-based and certain retouching manipulations.

TABLE 5. SUMMARY OF SOME LIMITATIONS IN WATERMARKING-BASED FIMD AND FIA.

Ref.	*Scheme*	*Limitations*
[99], [100]	FIMD	The original face region cannot be recovered after the manipulation revealing process, although the watermarking-based technique can detect various manipulations.
[101]–[103]	FIA	The primary drawback of this scheme is considered to be its strict embedding capacity. Large face regions in the image can generate a significant number of bits for tamper detection, localization, and face region recovery, which require additional embedding space. If there is insufficient embedding capacity, the FIA scheme can not effectively protect the face image.

V. COMPARISON BETWEEN DL-BASED AND WATERMARKING-BASED FIMD TECHNIQUES

Watermark-based FIMD and FIA techniques have proven efficient and advantageous over DL-based FIMD techniques. Table 6 presents a comparison of DL-based and watermarking-based techniques.

TABLE 6. COMPARISON BETWEEN DL-BASED AND WATERMARKING-BASED FIMD TECHNIQUES

DL-based techniques	*Watermarking-based techniques*
Most of these techniques are limited to detecting a single kind of manipulation because they rely on techniques for fabricating or manipulating images for implementation [83], [85]–[88],[104].	Capable of identifying various forms of manipulation and not reliant on knowledge of the processes involved in producing manipulated or fake images [99]–[103].
DL-based schemes require large datasets for training, and optimal detection performance is achieved when the input image closely matches the training set [92], [105].	It can be applied to any type of image, and training is not required [99]–[103].
The majority of methods employ labor- and time-intensive supervised networks for detection [106]–[108].	The techniques are superior in terms of time and effort savings as they operate in a fully automated manner [99]–[103].
Results of false detections have been documented, particularly in cases where the input image deviates from the training dataset [92], [105], [109], [110]. For example, the maximum accuracy values are 84.7%, 99.3%, 87.5%, and 81.6%, respectively [92], [109].	There are no false detections, and the system exhibits 100% detection accuracy [99]–[103].

VI. CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK

This paper has highlighted the increasing significance of FIMD and FIA techniques in the context of digital data security. The emergence of digital face manipulation methods, including the notable development of "DeepFakes," has underscored the need for robust authentication and manipulation detection mechanisms. The limitations of current forensic software and the challenges posed by the rapid advancements in facial image manipulation techniques have been addressed. Furthermore, the paper has provided an

overview of recent trends in FIA techniques and their limitations, emphasizing the need for continued development and innovation in this field. For future work, it is imperative to address the limitations of existing forensic software and to develop more effective manipulation detection techniques capable of differentiating between authentic and manipulated face images. Additionally, further research is needed to enhance the capabilities of FIA schemes, particularly in the context of DeepFakes and other advanced manipulation methods. This may involve exploring the potential of DL-based techniques and the development of more comprehensive and versatile manipulation detection algorithms. Moreover, the paper suggests investigating the distinctions and interrelations among image tampering, manipulation, and forgery, as well as the development of tampering detection techniques with unique strengths and applications. Finally, the paper emphasizes the importance of addressing unanswered research questions and forecasting future directions to advance digital face manipulation generation and detection. By addressing these avenues for future research, the field of FIA and manipulation detection can continue to evolve and effectively mitigate the security risks associated with digital face manipulation methods.

ACKNOWLEDGEMENT

The authors extend their thanks to Al-Iraqia University for supporting this research.

.

REFERENCES

[1] H. Al-Najjar, S. Alharthi, and P. K. Atrey, “Secure image sharing method over unsecured channels,” Multimed. Tools Appl., vol. 75, no. 4, pp. 2249–2274, Feb. 2016, doi: 10.1007/s11042-014-2404-5.

[2] M. E. Hodeish, L. Bukauskas, and V. T. Humbe, “A new efficient TKHC-based image sharing scheme over unsecured channel,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 4, pp. 1246–1262, Apr. 2022, doi: 10.1016/j.jksuci.2019.08.004.

[3] J. Faircloth, “Information Security,” in Enterprise Applications Administration, J. Faircloth, Ed., Boston: Elsevier, 2014, pp. 175–220. doi: 10.1016/B978-0-12-407773-7.00005-3.

[4] M. Devipriya and M. Brindha, “Secure Image Cloud Storage Using Homomorphic Password Authentication with ECC Based Cryptosystem,” Adv. Syst. Sci. Appl., vol. 22, no. 1, pp. 92–116, 2022.

[5] V. L. Schultz, V. V Kulba, O. A. Zaikin, A. B. Shelkov, and I. V Chernov, “Regional Security: Analysis of the Emergency Management Effectiveness Based on the Scenario Approach,” Adv. Syst. Sci. Appl., vol. 17, no. 1, pp. 9–24, 2017.

[6] H. Kaur and S. R, “VLSI Implementation of Lightweight Cryptography Algorithm,” Adv. Syst. Sci. Appl., vol. 16, no. 1, pp. 95–101, 2016.

[7] R. Thabit and B. E. Khoo, “Robust Reversible Watermarking Application for Fingerprint Image Security,” Adv. Syst. Sci. Appl., vol. 22, no. 1, pp. 117–129, 2022.

[8] R. Thabit, “Improved steganography techniques for different types of secret data,” Adv. Syst. Sci. Appl., vol. 19, no. 3, 2019.

[9] S. Kloppenburg and I. van der Ploeg, “Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences,” Sci. Cult. (Lond)., vol. 29, no. 1, pp. 57–76, Jan. 2020, doi: 10.1080/09505431.2018.1519534.

[10] J. Galbally, S. Marcel, and J. Fierrez, “Biometric Antispoofing Methods: A Survey in Face Recognition,” IEEE Access, vol. 2, pp. 1530–1552, 2014, doi: 10.1109/ACCESS.2014.2381273.

[11] ISO/IEC JTC1 SC37 Biometrics, “Information Technology-Biometric Presentation Attack Detection-Part 3: Testing and Reporting.,” Int. Organ. Stand., 2017.

[12] S. Marcel, J. Fierrez, and N. Evans, Handbook of Biometric Anti-Spoofing - Presentation Attack Detection and Vulnerability Assessment. Springer Nature Singapore, 2023.

[13] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, “Deepfakes and beyond: A Survey of face manipulation and fake detection,” Inf. Fusion, vol. 64, no. July, pp. 131–148, Dec. 2020, doi: 10.1016/j.inffus.2020.06.014.

[14] L. Verdoliva, “Media Forensics and DeepFakes: An Overview,” IEEE J. Sel. Top. Signal Process., vol. 14, pp. 910–932, 2020.

[15] A. Czajka, W. Kasprzak, and A. Wilkowski, “Verification of iris image authenticity using fragile watermarking,” Bull. Polish Acad. Sci. Tech. Sci., vol. 64, no. 4, pp. 807–819, Dec. 2016, doi: 10.1515/bpasts-2016-0090.

[16] I. J. Goodfellow et al., “Generative adversarial nets,” in Proceedings of advances in neural information processing systems, 2014.

[17] D. P. Kingma and M. Welling, “Auto-encoding variational bayes,” in Proceedings of international conference on learning representations, 2013.

[18] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, “An introduction to digital face manipulation,” in Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, Springer International Publishing Cham, 2022, pp. 3–26.

[19] V. V. V. N. S. Vamsi et al., “Deepfake detection in digital media forensics,” Glob. Transitions Proc., vol. 3, no. 1, pp. 74–79, Jun. 2022, doi: 10.1016/j.gltp.2022.04.017.

[20] R. Cellan-Jones, “Deepfake videos double in nine months,” BBC Tech News. 2019.

[21] D. Citron, “How DeepFake undermine truth and threaten democracy,” in TEDSummit, TED official website, 2019. [Online]. Available: https://www.ted.com/talks/danielle_citron_how_deepfakes_undermine_truth_and_threaten_democracy

[22] P. Korshunov and S. Marcel, “DeepFakes: a New Threat to Face Recognition? Assessment and Detection,” ArXiv, vol. abs/1812.0, 2018.

[23] B. B. C. Bitesize, “Deepfakes: what are they and why would i make one,” BBC Bitesize Articles. 2019. [Online]. Available: https://www.bbc.co.uk/bitesize/articles/zfkwcqt

[24] J. Kietzmann, L. W. Lee, I. P. McCarthy, and T. C. Kietzmann, "Deepfakes: Trick or treat?," Bus. Horiz., vol. 63, no. 2, pp. 135–146, Mar. 2020, doi: 10.1016/j.bushor.2019.11.006.

[25] S. Kolagati, T. Priyadharshini, and V. Mary Anita Rajam, "Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model," Int. J. Inf. Manag. Data Insights, vol. 2, no. 1, p. 100054, Apr. 2022, doi: 10.1016/j.jjimei.2021.100054.

[26] G. Wang, Q. Jiang, X. Jin, and X. Cui, "FFR_FD: Effective and fast detection of DeepFakes via feature point defects," Inf. Sci. (Ny)., vol. 596, pp. 472–488, Jun. 2022, doi: 10.1016/j.ins.2022.03.026.

[27] P. Korus, "Digital image integrity – a survey of protection and verification techniques," Digit. Signal Process., vol. 71, pp. 1–26, Dec. 2017, doi: 10.1016/j.dsp.2017.08.009.

[28] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, "Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics," ACM Comput. Surv., vol. 43, no. 4, Oct. 2011, doi: 10.1145/1978802.1978805.

[29] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 3, pp. 492–506, 2010, doi: 10.1109/TIFS.2010.2053202.

[30] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Trans. Inf. Forensics Secur., vol. 3, no. 1, pp. 101–117, Mar. 2008, doi: 10.1109/TIFS.2007.916010.

[31] D. Cozzolino, A. Rossler, J. Thies, M. Niesner, and L. Verdoliva, "ID-Reveal: Identity-aware DeepFake Video Detection," in 2021 IEEE/CVF International Conference on Computer Vision (ICCV), IEEE, Oct. 2021, pp. 15088–15097. doi: 10.1109/ICCV48922.2021.01483.

[32] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Niessner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in 2019 IEEE/CVF International Conference on Computer Vision (ICCV), IEEE, Oct. 2019, pp. 1–11. doi: 10.1109/ICCV.2019.00009.

[33] M. Dang and T. N. Nguyen, "Digital Face Manipulation Creation and Detection: A Systematic Review," Electronics, vol. 12, no. 16, p. 3407, Aug. 2023, doi: 10.3390/electronics12163407.

[34] M. H. Al-Hadaad, R. Thabit, K. A. Zidan, and B. E. Khoo, "Face Image Authentication Scheme Based on Cohen–Daubechies–Feauveau Wavelets," in International Conference on Robotics, Vision, Signal Processing and Power Applications, Springer, 2024, pp. 553–564.

[35] M. Kowalski, "FaceSwap," GetHub official website. 2021. [Online]. Available: https://github.com/MarekKowalski/FaceSwap

[36] A. Store, "ZAO," Changsha Shenduronghe Network Technology Co., Ltd. 2019. [Online]. Available: https://apps.apple.com/cn/app/id1465199127

[37] A. Verma, "9 Best Photo Morph Apps for Android & iOS in 2022," The Unfolder, 2022.

[38] G. Wolberg, "Image morphing: a survey," Vis. Comput., vol. 14, no. 8, pp. 360–372, 1998, doi: 10.1007/s003710050148.

[39] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, "Is your biometric system robust to morphing attacks?," in 2017 5th International Workshop on Biometrics and Forensics (IWBF), IEEE, Apr. 2017, pp. 1–6. doi: 10.1109/IWBF.2017.7935079.

[40] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "Face Morphing Attack Generation and Detection: A Comprehensive Survey," IEEE Trans. Technol. Soc., vol. 2, no. 3, pp. 128–145, Sep. 2021, doi: 10.1109/TTS.2021.3066254.

[41] Y. Weng, L. Wang, X. Li, M. Chai, and K. Zhou, "Hair Interpolation for Portrait Morphing," Comput. Graph. Forum, vol. 32, pp. 79–84, 2013.

[42] H. Zhang, S. K. Venkatesh, R. Ramachandra, K. B. Raja, N. Damer, and C. Busch, "MIPGAN—Generating Strong and High Quality Morphing Attacks Using Identity Prior Driven GAN," IEEE Trans. Biometrics, Behav. Identity Sci., vol. 3, pp. 365–383, 2021.

[43] E. Gonzalez-Sosa, J. Fierrez, R. Vera-Rodriguez, and F. Alonso-Fernandez, "Facial Soft Biometrics for Recognition in the Wild: Recent Works, Annotation, and COTS Evaluation," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 8, pp. 2001–2014, Aug. 2018, doi: 10.1109/TIFS.2018.2807791.

[44] Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, and J. Choo, "StarGAN: Unified Generative Adversarial Networks for Multi-domain Image-to-Image Translation," in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, IEEE, Jun. 2018, pp. 8789–8797. doi: 10.1109/CVPR.2018.00916.

[45] A. Agarwal, R. Singh, M. Vatsa, and A. Noore, "SWAPPED! Digital face presentation attack detection via weighted local magnitude pattern," in 2017 IEEE International Joint Conference on Biometrics (IJCB), IEEE, Oct. 2017, pp. 659–665. doi: 10.1109/BTAS.2017.8272754.

[46] I. Snap, "Snapchat," App Store Preview. 2022.

[47] L. LOIC, "The 9 Best AI Video Generators (Text-to-Video)," Make Use of Website. 2021.

[48] O. Fried et al., "Text-based editing of talking-head video," ACM Trans. Graph., vol. 38, no. 4, pp. 1–14, Aug. 2019, doi: 10.1145/3306346.3323028.

[49] F. T. Support, "Talking Avatar," Talking avatar website. 2022.

[50] P. Korshunov and S. Marcel, "Vulnerability of Face Recognition to Deep Morphing," ArXiv, Oct. 2019, [Online]. Available: http://arxiv.org/abs/1910.01933

[51] U. Anchalia, K. P. Reddy, A. Modi, K. Neelam, D. Prasad, and V. Nath, "Study and Design of Biometric Security Systems: Fingerprint and Speech Technology," in Lecture Notes in Electrical Engineering, 2019, pp. 577–584. doi: 10.1007/978-981-13-7091-5_47.

[52] A. Kamboj, R. Rani, and A. Nigam, "A comprehensive survey and deep learning-based approach for human recognition using ear biometric," Vis. Comput., pp. 1–34, 2021.

[53] U. Muhammad, T. Holmberg, W. C. de Melo, and A. Hadid, "Face Anti-Spoofing via Sample Learning Based Recurrent Neural Network (RNN)," in BMVC, 2019.

[54] G. GencyV, M. K. Chaithanya, and A. F. Majeed, "Face Spoofing Detection: A Survey on Different Methodologies," 2020.

[55] Z. Boulkenafet, Z. Akhtar, X. Feng, and A. Hadid, "Face Anti-spoofing in Biometric Systems," 2017.

[56] E. Fourati, W. Elloumi, and A. Chetouani, "Anti-spoofing in face recognition-based biometric authentication using Image Quality Assessment," Multimed. Tools Appl., vol. 79, pp. 865–889, 2019.

[57] L. Li, P. L. Correia, and A. Hadid, "Face recognition under spoofing attacks: countermeasures and research directions," IET Biom., vol. 7, pp. 3–14, 2018.

[58] A. Snook, "What is Deepfake Identity Theft?," i-Sight website. 2020. [Online]. Available: https://www.i-sight.com/resources/what-is-deepfake-identity-theft/

[59] E. Haller, "The two faces of deepfakes: Cybersecurity & identity fraud," Secur. Mag., 2022, [Online]. Available: https://www.securitymagazine.com/articles/97085-the-two-faces-of-deepfakes-cybersecurity-and-identity-fraud

[60] R. Hendrikse, "How Deepfakes Could Become A Threat To Your Identity," Forbes, 2019, [Online]. Available: https://www.forbes.com/sites/renehendrikse/2019/12/20/how-deepfakes-could-become-a-threat-to-your-identity/?sh=3ce7083e1063

[61] L. Patel, "The Rise of Deepfakes and What That Means for Identity Fraud," DarkReading Authentication, 2020, [Online]. Available: https://www.darkreading.com/authentication/the-rise-of-deepfakes-and-what-that-means-for-identity-fraud

[62] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A Survey of face manipulation and fake detection," Inf. Fusion, vol. 64, pp. 131–148, Dec. 2020, doi: 10.1016/j.inffus.2020.06.014.

[63] H. Allcott and M. Gentzkow, "Social Media and Fake News in the 2016 Election," J. Econ. Perspect., vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.

[64] J. Cote, "DEEPFAKES AND FAKE NEWS POSE A GROWING THREAT TO DEMOCRACY, EXPERTS WARN," News Northeast., 2022, [Online]. Available: https://news.northeastern.edu/2022/04/01/deepfakes-fake-news-threat-democracy/

[65] V. Vieira, "Deepfakes and the intensification of fake news," Inst. Res. internet Soc., 2019, [Online]. Available: https://irisbh.com.br/en/deepfakes-and-the-intensification-of-fake-news/

[66] C. Vaccari and A. Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," Soc. Media + Soc., vol. 6, no. 1, p. 2056305120903408, Jan. 2020, doi: 10.1177/2056305120903408.

[67] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and Detection of Facial Beautification in Face Recognition: An Overview," IEEE Access, vol. 7, pp. 152667–152678, 2019, doi: 10.1109/ACCESS.2019.2948526.

[68] Z. Akhtar, D. Dasgupta, and B. Banerjee, "Face Authenticity: An Overview of Face Manipulation Generation, Detection and Recognition," SSRN Electron. J., 2019.

[69] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face Recognition Systems Under Morphing Attacks: A Survey," IEEE Access, vol. 7, pp. 23012–23026, 2019, doi: 10.1109/ACCESS.2019.2899367.

[70] J. Frank, T. Eisenhofer, L. Schönherr, A. Fischer, D. Kolossa, and T. Holz, "Leveraging frequency analysis for deep fake image recognition," in 37th International Conference on Machine Learning, ICML 2020, in ICML'20, vol. PartF16814. JMLR.org, 2020, pp. 3205–3216.

[71] A. Jain, R. Singh, and M. Vatsa, "On Detecting GANs and Retouching based Synthetic Alterations," in 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, Oct. 2018, pp. 1–7. doi: 10.1109/BTAS.2018.8698545.

[72] R. Raghavendra, K. B. Raja, and C. Busch, "Detecting morphed face images," in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, Sep. 2016, pp. 1–7. doi: 10.1109/BTAS.2016.7791169.

[73] C. Rathgeb, C.-I. Satnoianu, N. E. Haryanto, K. Bernardo, and C. Busch, "Differential Detection of Facial Retouching: A Multi-Biometric Approach," IEEE Access, vol. 8, pp. 106373–106385, 2020, doi: 10.1109/ACCESS.2020.3000254.

[74] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch, Detecting morphed face images using facial landmarks, vol. 10884 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-319-94211-7_48.

[75] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep Face Representations for Differential Morphing Attack Detection," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 3625–3639, 2020, doi: 10.1109/TIFS.2020.2994750.

[76] S.-Y. Wang, O. Wang, R. Zhang, A. Owens, and A. Efros, "Detecting Photoshopped Faces by Scripting Photoshop," in 2019 IEEE/CVF International Conference on Computer Vision (ICCV), IEEE, Oct. 2019, pp. 10071–10080. doi: 10.1109/ICCV.2019.01017.

[77] U. Scherhag, J. Kunze, C. R athgeb, and C. Busch, "Face morph detection for unknown morphing algorithms and image sources: a multi-scale block local binary pattern fusion approach," IET Biometrics, vol. 9, no. 6, pp. 278--289(11), Nov. 2020, [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2019.0206

[78] C. Rathgeb et al., "PRNU-based detection of facial retouching," IET Biometrics, vol. 9, no. 4, pp. 154--164(10), Jul. 2020, [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2019.0196

[79] F. Marra, D. Gragnaniello, D. Cozzolino, and L. Verdoliva, "Detection of GAN-Generated Fake Images over Social Networks," in 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018, pp. 384–389. doi: 10.1109/MIPR.2018.00084.

[80] D. Gragnaniello, D. Cozzolino, F. Marra, G. Poggi, and L. Verdoliva, "Are GAN Generated Images Easy to Detect? A Critical Analysis of the State-Of-The-Art," in 2021 IEEE International Conference on Multimedia and Expo (ICME), 2021, pp. 1–6. doi: 10.1109/ICME51207.2021.9428429.

[81] Y. Mirsky and W. Lee, "The creation and detection of deepfakes: A survey," ACM Comput. Surv., vol. 54, no. 1, pp. 1–41, 2021.

[82] T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, and S. Nahavandi, "Deep Learning for Deepfakes Creation and Detection," CoRR, vol. abs/1909.1, 2019, [Online]. Available: http://arxiv.org/abs/1909.11573

[83] F. Matern, C. Riess, and M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," in 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), IEEE, Jan. 2019, pp. 83–92. doi: 10.1109/WACVW.2019.00020.

[84] S. Hu, Y. Li, and S. Lyu, "Exposing GAN-Generated Faces Using Inconsistent Corneal Specular Highlights," in ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Jun. 2021, pp. 2500–2504. doi: 10.1109/ICASSP39728.2021.9414582.

[85] X. Han, Z. Ji, and W. Wang, "Low Resolution Facial Manipulation Detection," in 2020 IEEE International Conference on Visual Communications and Image Processing (VCIP), 2020, pp. 431–434. doi: 10.1109/VCIP49819.2020.9301796.

[86] X. Yang, Y. Li, H. Qi, and S. Lyu, "Exposing GAN-synthesized Faces Using Landmark Locations," in Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, New York, NY, USA: ACM, Jul. 2019, pp. 113–118. doi: 10.1145/3335203.3335724.

[87] S. McCloskey and M. Albright, "Detecting GAN-Generated Imagery Using Saturation Cues," in 2019 IEEE International Conference on Image Processing (ICIP), 2019, pp. 4584–4588. doi: 10.1109/ICIP.2019.8803661.

[88] H. Li, B. Li, S. Tan, and J. Huang, "Detection of Deep Network Generated Images Using Disparities in Color Components," ArXiv, vol. abs/1808.0, 2018.

[89] L. Nataraj et al., "Detecting GAN generated Fake Images using Co-occurrence Matrices," ArXiv, vol. abs/1903.0, 2019.

[90] M. Barni, K. Kallas, E. Nowroozi, and B. Tondi, "CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis," in 2020 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/WIFS49906.2020.9360905.

[91] H. Dang, F. Liu, J. Stehouwer, X. Liu, and A. K. Jain, "On the Detection of Digital Face Manipulation," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 5780–5789. doi: 10.1109/CVPR42600.2020.00582.

[92] R. Wang, L. Ma, F. Juefei-Xu, X. Xie, J. Wang, and Y. Liu, "FakeSpotter: {A} Simple Baseline for Spotting AI-Synthesized Fake Faces," CoRR, vol. abs/1909.0, 2019, [Online]. Available: http://arxiv.org/abs/1909.06122

[93] A. Jain, P. Majumdar, R. Singh, and M. Vatsa, "Detecting GANs and Retouching based Digital Alterations via DAD-HCNN," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2020, pp. 2870–2879. doi: 10.1109/CVPRW50498.2020.00344.

[94] Z. Mi, X. Jiang, T. Sun, and K. Xu, "GAN-Generated Image Detection With Self-Attention Mechanism Against GAN Generator Defect," IEEE J. Sel. Top. Signal Process., vol. 14, no. 5, pp. 969–981, 2020, doi: 10.1109/JSTSP.2020.2994523.

[95] X. Zhang, S. Karaman, and S.-F. Chang, "Detecting and Simulating Artifacts in GAN Fake Images," in 2019 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, Dec. 2019, pp. 1–6. doi: 10.1109/WIFS47025.2019.9035107.

[96] T. Dzanic, K. Shah, and F. D. Witherden, "Fourier Spectrum Discrepancies in Deep Network Generated Images," in Proceedings of the 34th International Conference on Neural Information Processing Systems, in NIPS'20. Red Hook, NY, USA: Curran Associates Inc., 2020.

[97] R. Durall, M. Keuper, and J. Keuper, "Watch your up-convolution: CNN based generative deep neural networks are failing to reproduce spectral distributions," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2020, pp. 7887–7896. doi: 10.1109/CVPR42600.2020.00791.

[98] N. Bonettini, P. Bestagini, S. Milani, and S. Tubaro, "On the use of Benford's law to detect GAN-generated images," in 2020 25th International Conference on Pattern Recognition (ICPR), IEEE, Jan. 2021, pp. 5495–5502. doi: 10.1109/ICPR48806.2021.9412944.

[99] Z. A. Salih, R. Thabit, K. A. Zidan, and B. E. Khoo, "A new face image manipulation reveal scheme based on face detection and image watermarking," in 2022 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), IEEE, 2022, pp. 1–6.

[100] Z. A. Salih, R. Thabit, and K. A. Zidan, "A New Manipulation Detection and Localization Scheme," J. Eng. Sci. Technol., vol. 18, no. 2, pp. 1164–1183, 2023.

[101] M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, "A New Face Image Authentication Scheme based on Bicubic Interpolation," Al-Iraqia J. Sci. Eng. Res., vol. 2, no. 2, pp. 1000–1006, Jun. 2023, doi: 10.58564/IJSER.2.2.2023.68.

[102] M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, "A New Face Region Recovery Algorithm based on Bicubic Interpolation," JOIV Int. J. Informatics Vis., vol. 7, no. 3, pp. 1000–1006, Sep. 2023, doi: 10.30630/joiv.7.3.1671.

[103] M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, "Tamper detection , localization , and recovery for digital face images," 2023.

[104] S. Hu, Y. Li, and S. Lyu, "Exposing GAN-Generated Faces Using Inconsistent Corneal Specular Highlights," in ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021, pp. 2500–2504. doi: 10.1109/ICASSP39728.2021.9414582.

[105] F. Marra, C. Saltori, G. Boato, and L. Verdoliva, "Incremental learning for the detection and classification of gan-generated images," in 2019 IEEE international workshop on information forensics and security (WIFS), 2019, pp. 1–6.

[106] A. Bharati, R. Singh, M. Vatsa, and K. W. Bowyer, "Detecting Facial Retouching Using Supervised Deep Learning," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 9, pp. 1903–1913, 2016, doi: 10.1109/TIFS.2016.2561898.

[107] C. Kong, B. Chen, H. Li, S. Wang, A. Rocha, and S. T. W. Kwong, "Detect and Locate: A Face Anti-Manipulation Approach with Semantic and Noise-level Supervision," ArXiv, vol. abs/2107.0, 2021.

[108] L. Cao, W. Sheng, F. Zhang, K. Du, C. Fu, and P. Song, "Face Manipulation Detection Based on Supervised Multi-Feature Fusion Attention Network.," Sensors (Basel)., vol. 21, no. 24, Dec. 2021, doi: 10.3390/s21248181.

[109] I. Amerini, L. Galteri, R. Caldelli, and A. Del Bimbo, "Deepfake video detection through optical flow based cnn," in Proceedings of the IEEE/CVF international conference on computer vision workshops, 2019, p. 0.

[110] T. Jung, S. Kim, and K. Kim, "Deepvision: Deepfakes detection using human eye blinking pattern," IEEE Access, vol. 8, pp. 83144–83154, 2020.