Examining IoT-Enhanced for Current Developments in Face Image Authentication (FIA) Methods and Their Drawbacks / Review article

Marwa Jamal Hadi[1] and Emaan Ouudha Oraby[2]
1 Fine Arts Institutes for Girls, Baqubah-Diyala / Iraq
2 General Directorate of Education in Al-Qadissiyah Government, Ministry of Education / Iraq
e-mail1: marwajmal178@gmial.com
e-mail2: eman.iraq2017@gmail.com

دراسة تقنيات إنترنت الأشياء المحسنة للتطورات الحالية في أساليب مصادقة صورة الوجه (FIA) وعيوبها ـ دراسة مرجعية

مروة جمال هادي[1] و إيمان عودة عرابي[2]
1 معاهد الفنون الجميلة للبنات، بعقوبة \ ديالى - العراق
2 المديرية العامة للتربية في محافظة القادسية -
وزارة التربية والتعليم \ العراق

Abstract

The quick development of IoT and facial image manipulation (FIM) algorithms, as well as the growth of their user-friendly applications, highlight the pressing need for manipulation detection methods. These techniques need to demonstrate how face photos have been altered and validate their legitimacy. The scientific community has recently taken notice of the phrase "DeepFakes" and methods for detecting them. Take note of the latest methods for identifying watermark-based face image modification as well. The important thing to remember is that every one of these methods has its own set of drawbacks. This study provides a brief introduction to face image modification detection methods, emphasizing both watermarking-based and deep learning-based methods. Afterwards, the paper offers instances that demonstrate their use, stressing a comparison between deep learning. The paper then goes on to give examples of how they might be used, with a focus on comparing deep learning and watermarking-based methods for detecting tampering. Research recommendations and insights into possible future advancements in this fascinating field of study are included in the paper's conclusion. For scholars actively involved in or interested in this particular field of study, the review in this article is regarded as an essential resource.

Keywords: IoT (Internet of Things), Face Image Authentication (FIA), DeepFakes.

المستخلص

يُبرز التطور السريع لإنترنت الأشياء وخوارزميات التلاعب بصور الوجوه (FIM)، بالإضافة إلى نمو تطبيقاتها سهلة الاستخدام، الحاجة المُلحة لأساليب كشف التلاعب. يجب أن توضح هذه التقنيات كيفية تعديل صور الوجوه والتحقق من صحتها. وقد انتبه المجتمع العلمي مؤخرًا إلى مصطلح "التزييف العميق" وطرق كشفه. انتبه أيضًا إلى أحدث الطرق لكشف تعديلات صور الوجوه القائمة على العلامات المائية. من المهم تذكر أن لكل طريقة من هذه الطرق عيوبها. تُقدم هذه الدراسة مقدمة موجزة عن أساليب كشف تعديل صور الوجوه، مُركزةً على كلٍّ من الأساليب القائمة على العلامات المائية والتعلم العميق. بعد ذلك، تُقدم الورقة أمثلةً تُوضح استخداماتها، مُشددةً على مُقارنة بين التعلم العميق والتعلم العميق. ثم تُقدم الورقة أمثلةً على كيفية استخدامها، مُركزةً على مُقارنة أساليب التعلم العميق والعلامات المائية للكشف عن التلاعب. وتضمنت خاتمة الورقة توصيات بحثية ورؤىً حول التطورات المُستقبلية المُحتملة في هذا المجال الدراسي المُثير للاهتمام. للباحثين المهتمين أو النشطين في هذا المجال الدراسي، تُعدّ المراجعة الواردة في هذه المقالة مرجعًا أساسيًا.

الكلمات المفتاحية: إنترنت الأشياء (IoT)، مصادقة صورة الوجه (FIA)، التزييف العميق. (Deepfakes).

1. Introduction

As technology develops, digital photos and IoT may now be shared easily for a variety of reasons [1]–[3]. These days, people who utilize technology find that storing their private information and images in the cloud is really convenient because they can access it anytime they need to. However, security and data integrity are the main issues that users are worried about [4], [5]. To ensure the security of digital photos, the Internet of Things, and shared data, a number of techniques and security frameworks have been put into place, such as watermarking, steganography, and cryptography [6]–[8 Face images, which are shared online for a variety of reasons, including social media, face recognition apps, celebrity and fame aspirations, and identity discrimination in biometric systems (i.e., security and access control), are among the most important types of digital images and IoT [9]. There are several other uses for face photographs [10]–[12]. Because of the speed at which technology is developing, digital face editing techniques, algorithms, and applications are now readily available [13]–[17]. Intentional attacks, which involve malicious intent during the manipulation process, and unintentional attacks, which involve harmless intentions like beautifying the face, adjusting lighting, adding humorous stickers, etc., are the two main categories into which techniques for manipulating facial images can be divided. The content of the face picture is changed (i.e., its features) as a result of both modification approaches [18]. Interest in FIM techniques and how they affect data security systems has increased in the data security community. A vibrant field of study has emerged as a result of the scholarly community's attention being drawn to the term "DeepFakes" in recent years [19]–[24]. Known as DeepFakes, deep learning techniques have been used to create fake digital material. To substitute the faces of celebrities in pornographic movies, a machine learning system known as DeepFakes was created in 2017 [25]. DeepFakes' capabilities have been utilized for a number of detrimental objectives, such as financial fraud, the dissemination of false information, and the production of sexual content [26]. Researchers have concentrated on creating face modification detection systems in an attempt to improve media forensics generally [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]. The next section presents a summary of the recently published review papers in the field of face image manipulation and its detection techniques. To date, no review paper focuses 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 deep-learning based and watermarking based FIMD techniques; and section VI presents the conclusions and suggestions for future researches.

2. Literature Survey

The study in this section will present a summary of 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 and IoT techniques and examined the opportunities and risks associated with each group. - A framework was established for successfully addressing the risks of deepfakes.
[13], [34]	2020	- Conducted a comprehensive analysis of contemporary face manipulation techniques, encompassing deepfakes and IoT, and explored methods for detecting them. - Classified these techniques into four major categories based on their prevalent use in facial manipulation. - Examined public`cly 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 deep learning-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 deep learning. - 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.

Ref.	Year	Contributions
[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 deep learning 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 deep learning. - Identifying obstacles, addressing unanswered research questions, and forecasting future directions contribute to the advancement of digital face manipulation generation and detection.

Due to the rapid advancements in the field of FIA, this paper is presented to review recent trends in FIA technologies and their limitations. Additionally, it aims to compare technologies based on deep learning and watermarking.

3. 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 research [13], [18]–[20], [22], [26], [47]–[50]. Several FIM techniques exist, and new manipulation methods are constantly being introduced through improved applications. Nevertheless, the majority of research has focused on the manipulation methods depicted

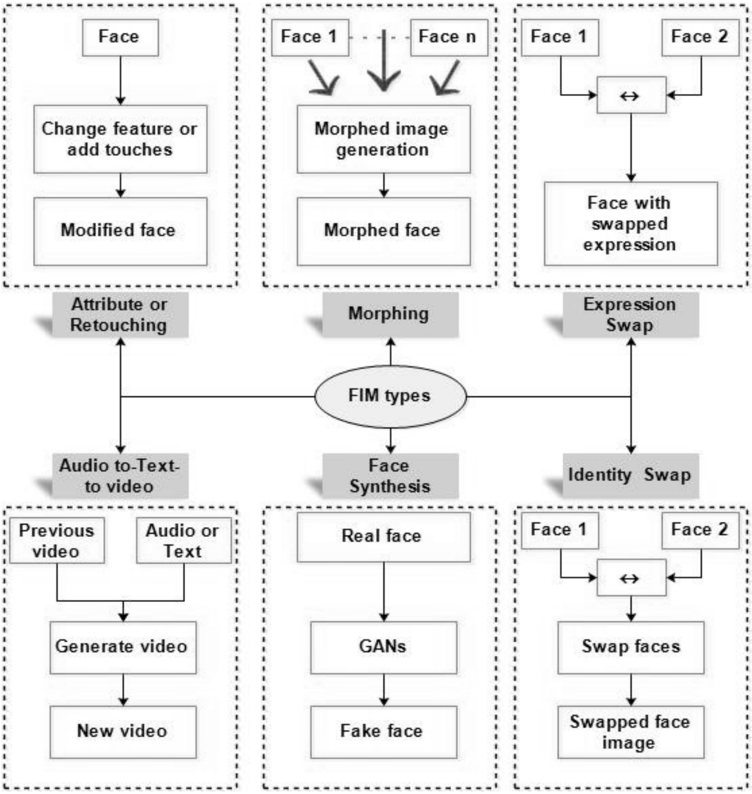

Fig. 1: Common types of FIM techniques [111].

in Table 2, which provides a brief explanation of the common manipulation types. Fig. 1 presents the classification of the FIM.

TABLE 2. The common types of FIM techniques

No.	Manipulation type	Explanation
1	Entire face synthesis	Utilizes Generative Adversarial Networks (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 [51] and b) deep learning-based techniques [52].
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‖ [53]. 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 [54]–[58].
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 color of individuals' hair or skin, their age, gender, the addition of a beard or glasses, and so on [59]–[61]. 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 [62].
5	Expression Swap	The process of replacing an individual's facial expressions in a video clip with those of another individual [59], [60].
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 [63]–[65].

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].

4. FIMD techniques

The face recognition system (FRS) is a subset of biometric security software that also includes voice recognition, fingerprint recognition, and iris recognition [55], [78], [79]. The FIM process affects image quality, which can influence acceptance or rejection decisions in FRS [80]–[85]. 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 [86]–[89], political conflict as a result of fake news [66], [67], [90]–[92], financial fraud, and others.

Since the number of harmful FIM applications is rapidly increasing, the researchers have directed their efforts towards presenting manipulation detection techniques that can distinguish fake face images from authentic images [14], [66], [74], [93]–[95]. 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 [96]–[102]. 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 [40], [102]–[106].

Currently, four types of FIMD schemes are available:

A. FIMD based on texture analysis

The study focuses on assessing the susceptibility of face recognition systems 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 deep learning or artificial intelligence

According to its definition, Deepfakes is a deep learning-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 deep learning.

D. FIMD face detection and image watermarking

Another FIMD method that employs facial identification and picture watermarking algorithms was just released. Following the identification of the face region, the picture blocks are divided into two categories: those connected to the face region and those that are not. This categorization is achieved by creating a binary mask picture. Information is extracted from blocks in the face region and inserted into blocks outside of it using Slantlet-based picture watermarking, as the modification procedure demonstrates [107], [108]. Table 5 highlights some of FIMD's restrictions based on watermarking.

A Multi-Task Cascaded Neural Network (MTCNN) is used in a new FIA scheme to identify and choose the face region, after which output adjustments are made. Following the identification of the face region, a binary mask image is produced, which makes it easier to divide image blocks into two categories: face blocks and non-face blocks. The mean of every block from the face region is used to derive the tamper localization data. The recovery data from the face region is then produced using the Bicubic Interpolation (BI) algorithm. The system embeds the generated binary sequence into the non-face blocks using a content-based embedding algorithm that can embed binary bits in the High-Low (HL) and Low-High (LH) sub-bands of the Slantlet transform (SLT) coefficients of the block. When manipulations are present, the system. The system embeds the generated binary sequence into the non-face blocks using a content-based embedding algorithm that can embed binary bits in the High-Low (HL) and Low-High (LH) sub-bands of the Slantlet transform (SLT) coefficients of the block. The system consistently detects tampered blocks in the face region and restores the original face region when manipulations are present [109]–[111]. A comparison of the sender and recipient sides of the FIMD and FIA schemes is provided in Figures 3 and 4. The original face data cannot be recovered by the FIMD scheme, which is intended to identify and detect tampering. However, the FIA scheme is able to recover the original face region in addition to detecting and locating tampering.

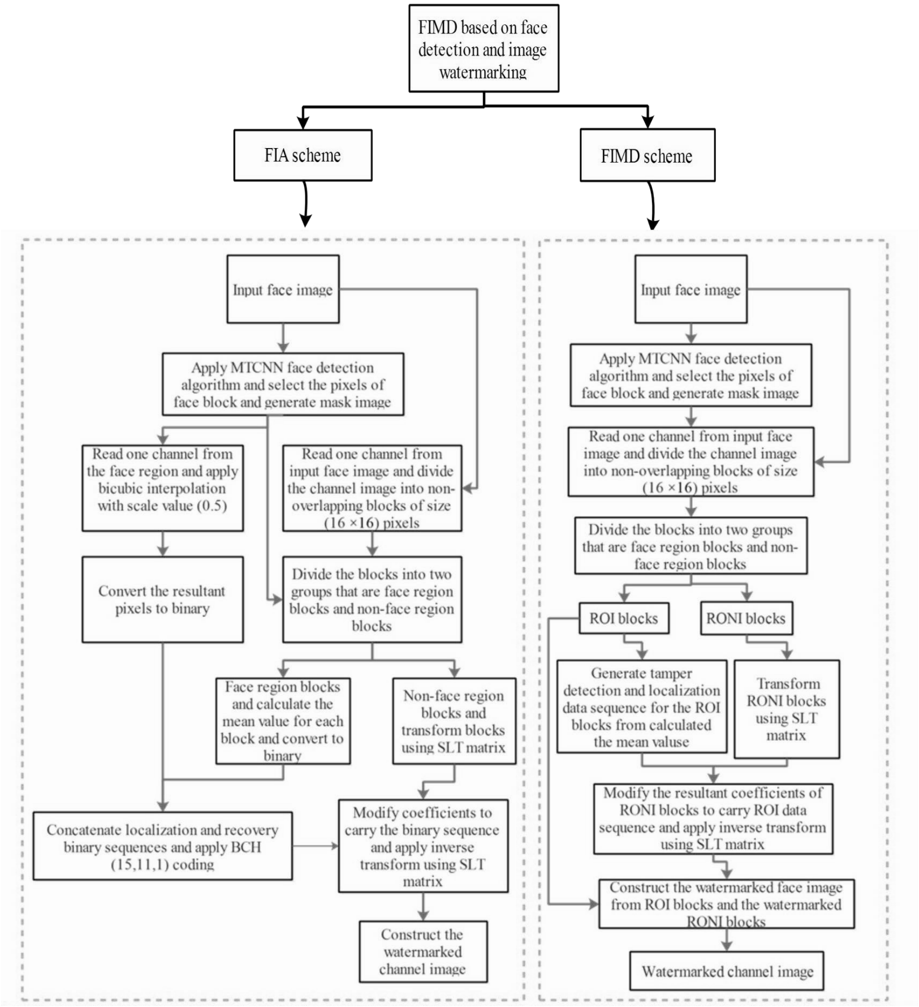
FIMD based on face detection and image watermarking
FIA scheme
FIMD scheme
Input face image
Apply MTCNN face detection algorithm and select the pixels of face block and generate mask image
Read one channel from the face region and apply bicubic interpolation with scale value (0.5)
Read one channel from input face image and divide the channel image into non-overlapping blocks of size (16 ×16) pixels
Convert the resultant pixels to binary
Divide the blocks into two groups that are face region blocks and non-face region blocks
Face region blocks and calculate the mean value for each block and convert to binary
Non-face region blocks and transform blocks using SLT matrix
Concatenate localization and recovery binary sequences and apply BCH (15,11,1) coding
Modify coefficients to carry the binary sequence and apply inverse transform using SLT matrix
Construct the watermarked channel image
Input face image
Apply MTCNN face detection algorithm and select the pixels of face block and generate mask image
Read one channel from input face image and divide the channel image into non-overlapping blocks of size (16 ×16) pixels
Divide the blocks into two groups that are face region blocks and non-face region blocks
ROI blocks
RONI blocks
Generate tamper detection and localization data sequence for the ROI blocks from calculated the mean valuse
Transform RONI blocks using SLT matrix
Modify the resultant coefficients of RONI blocks to carry ROI data sequence and apply inverse transform using SLT matrix
Construct the watermarked face image from ROI blocks and the watermarked RONI blocks
Watermarked channel image

Fig. 3: Comparison of FIMD and FIA schemes on the sender side of a single channel [108], [110].

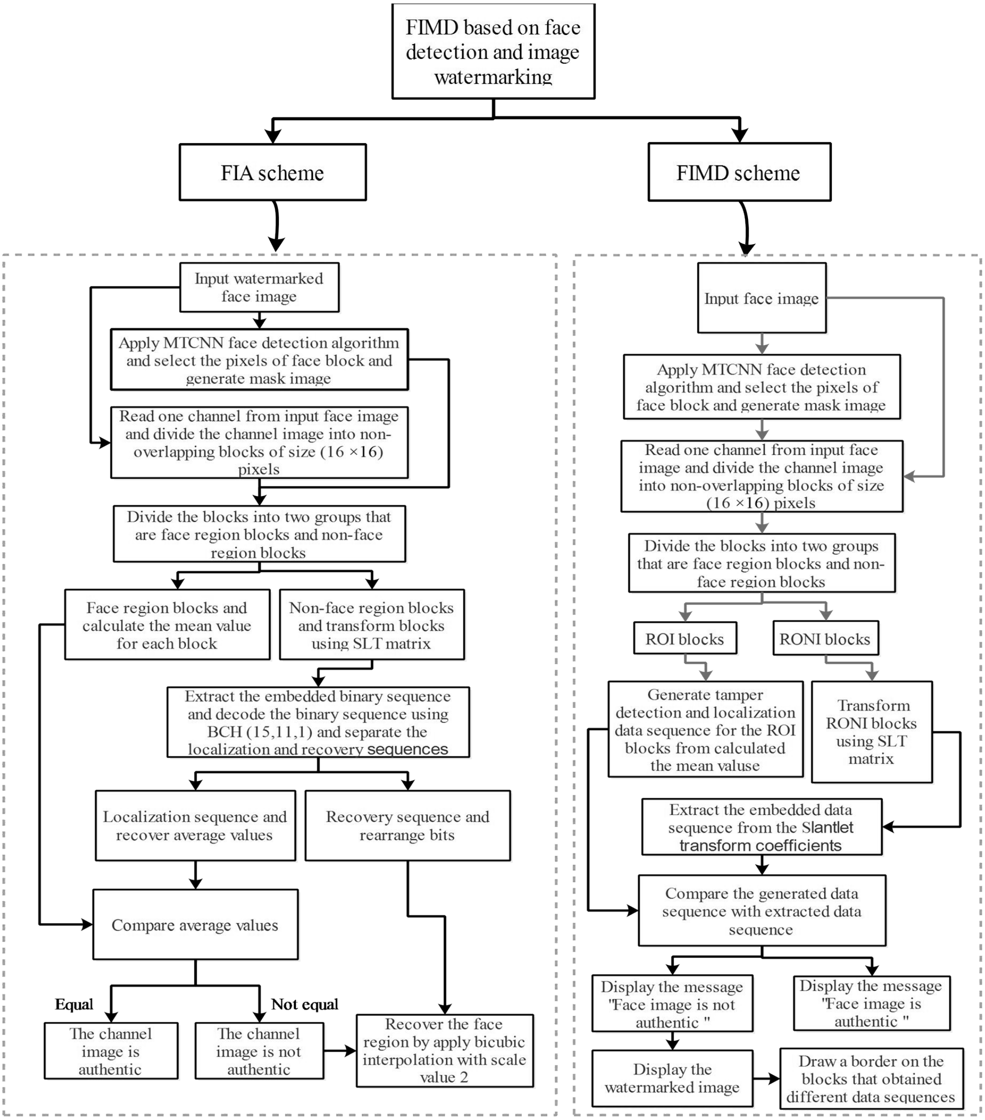
FIMD based on face detection and image watermarking
FIA scheme
FIMD scheme
Input watermarked face image
Apply MTCNN face detection algorithm and select the pixels of face block and generate mask image
Read one channel from input face image and divide the channel image into non-overlapping blocks of size (16 ×16) pixels
Divide the blocks into two groups that are face region blocks and non-face region blocks
Face region blocks and calculate the mean value for each block
Non-face region blocks and transform blocks using SLT matrix
Extract the embedded binary sequence and decode the binary sequence using BCH (15,11,1) and separate the localization and recovery sequences
Localization sequence and recover average values
Recovery sequence and rearrange bits
Compare average values
Equal
Not equal
The channel image is authentic
The channel image is not authentic
Recover the face region by apply bicubic interpolation with scale value 2
Input face image
Apply MTCNN face detection algorithm and select the pixels of face block and generate mask image
Read one channel from input face image and divide the channel image into non-overlapping blocks of size (16 ×16) pixels
Divide the blocks into two groups that are face region blocks and non-face region blocks
ROI blocks
RONI blocks
Generate tamper detection and localization data sequence for the ROI blocks from calculated the mean valuse
Transform RONI blocks using SLT matrix
Extract the embedded data sequence from the Slantlet transform coefficients
Compare the generated data sequence with extracted data sequence
Display the message "Face image is not authentic "
Display the message "Face image is authentic "
Display the watermarked image
Draw a border on the blocks that obtained different data sequences

Fig. 4: Comparison of FIMD and FIA schemes on the receiver side of a single channel [108], [110].

TABLE 4. Summary of some limitations in deep-learning based FIMD.

Ref.	Detected features	Limitations
[50], [112], [113]	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.
[114]	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.
[115], [116]	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.
[117]	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.
[104], [118]– [123]	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.
[95]	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.
[124]– [126]	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
[107], [108]	FIMD	The original face region cannot be recovered after the manipulation-revealing process, although the watermarking-based technique can detect various manipulations.
[109]–[111]	FIA	The primary drawback of this scheme is considered to be its strict embedding capacity. Large face regions in the image can result in generating 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.

I. Comparison between deep-learning-based and watermarking-based FIMD techniques

Watermark-based FIMD and FIA techniques have proven efficiency and advantage over deep learning-based FIMD techniques. Table 6 presents a comparison of deep learning-based and watermarking-based techniques.

TABLE 6. Comparison between deep-learning based and watermarking-based FIMD techniques

Deep-learning-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 [50], [113]–[116], [127] .	Capable of identifying various forms of manipulation and do not reliant on knowledge of the processes involved in producing manipulated or fake images.

Deep learning-based schemes require large datasets for training, and optimal detection performance is achieved when the input image closely matches the training set [120], [128].	**It can be applied to any type of image, and training is not required.**
The majority of methods employ labor- and time-intensive supervised networks for detection [129]– [131].	**The system is superior in terms of time and effort savings as it operates in a fully automated manner.**
Results of false detections have been documented, particularly in cases where the input image deviates from the training dataset [120], [128], [132], [133]. For example, the maximum accuracy values are 84.7%, 99.3%, 87.5%, and 81.6%, respectively [120], [132].	**There are no false detections, and the system exhibits high detection accuracy.**

5. Conclusion

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 deep learning-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, and 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.

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 Devipriya,‖ *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 Undermines Truth and threaten democracy,‖ in *TEDSummit*, TED official website, 2019. [Online].

[22]. Available: https://www.ted.com/talks/danielle_citron_how_deepfakes_undermine_truth_and_threaten_democracy

[23]. P. Korshunov and S. Marcel, —DeepFakes: a New Threat to Face Recognition? Assessment and Detection,‖ *ArXiv*, vol. abs/1812.0, 2018.

[24]. 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

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. X. Ju, —An Overview of Face Manipulation Detection,‖ *J. Cyber Secur.*, vol. 2, no. 4, pp. 197–207, 2020, doi: 10.32604/jcs.2020.014310.

[36]. R. Thakur and R. Rohilla, —Recent advances in digital image manipulation detection techniques: A brief review,‖ *Forensic Sci. Int.*, vol. 312, p. 110311, 2020.

[37]. L. Verdoliva, —Media Forensics and DeepFakes: An Overview,‖ *IEEE J. Sel. Top. Signal Process.*, vol. 14, no. 5, pp. 910– 932, Aug. 2020, doi: 10.1109/JSTSP.2020.3002101.

[38]. M. Abdolahnejad and P. X. Liu, —Deep learning for face image synthesis and semantic manipulations: a review and future perspectives,‖ *Artif. Intell. Rev.*, vol. 53, no. 8, pp. 5847–5880, Dec. 2020, doi: 10.1007/s10462-020-09835-4.

[39]. X. Zheng, Y. Guo, H. Huang, Y. Li, and R. He, —A Survey of Deep Facial Attribute Analysis,‖ *Int. J. Comput. Vis.*, vol. 128, no. 8–9, pp. 2002–2034, Sep. 2020, doi: 10.1007/s11263-020-01308-z.

[40]. S. Pashine, S. Mandiya, P. Gupta, and R. Sheikh, —Deep Fake Detection: Survey of Facial Manipulation Detection Solutions,‖ Int. Res. J. Eng. Technol., vol. 8, no. 8, pp. 4441–4449, 2021, [Online]. Available: http://arxiv.org/abs/2106.12605

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

[42]. P. Yu, Z. Xia, J. Fei, and Y. Lu, —A Survey on Deepfake Video Detection,‖ *IET Biometrics*, vol. 10, no. 6, pp. 607–624, Nov. 2021, doi: 10.1049/bme2.12031.

[43]. A. M. Almars, —Deepfakes Detection Techniques Using Deep Learning: A Survey,‖ *J. Comput. Commun.*, vol. 09, no. 05, pp. 20–35, 2021, doi: 10.4236/jcc.2021.95003.

[44]. L. A. Passos, D. Jodas, K. A. P. da Costa, L. A. S. Júnior, D. Colombo, and J. P. Papa, —A Review of Deep Learning-based Approaches for Deepfake Content Detection,‖ *arXiv:2202.06095v1*. arXiv, 2022. [Online]. Available: http://arxiv.org/abs/2202.06095

[45]. F. Juefei-Xu, R. Wang, Y. Huang, Q. Guo, L. Ma, and Y. Liu, —Countering malicious deepfakes: Survey, battleground, and horizon,‖ *Int. J. Comput. Vis.*, vol. 130, no. 7, pp. 1678–1734, 2022.

[46]. A. Malik, M. Kuribayashi, S. M. Abdullahi, and A. N. Khan, —DeepFake Detection for Human Face Images and Videos: A Survey,‖ *IEEE Access*, vol. 10, pp. 18757–18775, 2022, doi: 10.1109/ACCESS.2022.3151186.

[47]. A. D. and S. B. Wankhade, *Intelligent Computing and Networking*, vol. 146. 2021. [Online]. Available: http://link.springer.com/10.1007/978-981-15-7421-4

[48]. M. Ibsen, C. Rathgeb, D. Fischer, P. Drozdowski, and C. Busch, —Digital Face Manipulation in Biometric Systems,‖ C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, Eds., Cham: Springer International Publishing, 2022, pp. 27–43. doi: 10.1007/978-3-030-87664-7_2.

[49]. I. Papastratis, —Deepfakes: Face synthesis with GANs and Autoencoders,‖ *AI Summer*, 2020, [Online]. Available: https://theaisummer.com/deepfakes/

[50]. D. Siegel, C. Kraetzer, S. Seidlitz, and J. Dittmann, —Media Forensics Considerations on DeepFake Detection with Hand- Crafted Features,‖ *J. Imaging*, vol. 7, no. 7, p. 108, Jul. 2021, doi: 10.3390/jimaging7070108.

[51]. 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.

[52]. M. Kowalski, —FaceSwap,‖ *GetHub official website*. 2021. [Online]. Available: https://github.com/MarekKowalski/FaceSwap

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

[54]. A. Verma, —9 Best Photo Morph Apps for Android & iOS in 2022,‖ *The Unfolder*, 2022.

[55]. [54] G. Wolberg, —Image morphing: a survey,‖ *Vis. Comput.*, vol. 14, no. 8, pp. 360–372, 1998, doi: 10.1007/s003710050148.

[56]. 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.

[57]. 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.

[58]. 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.

[59]. 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.

[60]. 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.

[61]. 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.

[62]. 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.

[63]. I. Snap, ―Snapchat,‖ *App Store Preview*. 2022.

[64]. L. LOIC, ―The 9 Best AI Video Generators (Text-to-Video),‖ *Make Use of Website*. 2021.

[65]. 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.

[66]. F. T. Support, ―Talking Avatar,‖ *Talking avatar website*. 2022.

[67]. 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.

[68]. 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.

[69]. D. Boneh, A. J. Grotto, P. McDaniel, and Ni. Papernot, ―How Relevant Is the Turing Test in the Age of Sophisbots?,‖ *IEEE Secur. Priv.*, vol. 17, no. 6, pp. 64–71, Nov. 2019, doi: 10.1109/MSEC.2019.2934193.

[70]. J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Niessner, ―Face2Face: Real-Time Face Capture and Reenactment of RGB Videos,‖ in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2016, pp. 2387–2395. doi: 10.1109/ CVPR.2016.262.

[71]. R. Salia, ―Top 10 Best Alternatives to Deep Nostalgia App,‖ *Top Ten AI website*. 2021.

[72]. P. Panyatham, ―Deepfake Technology In The Entertainment Industry: Potential Limitations And Protections,‖ *Emerg. Technol.*, vol. 3, no. 10, 2020.

[73]. V. Caron and V. Bergeron, ―WHAT ARE DEEPFAKE'S IMPACTS ON THE MEDIA AND ENTERTAINMENT INDUSTRY?,‖ *CANADA MEDIA FUND*, 2019.

[74]. J. ALDREDGE, ―Is Deepfake Technology the Future of the Film Industry?,‖ *Prem. Beat by shutterstock*, 2020.

[75]. C. Rathgeb, A. Dantcheva, and C. Busch, ―Impact and Detection of Facial Beautification in Face Recognition: An Overview,‖

[76]. *IEEE Access*, vol. 7, pp. 152667–152678, 2019, doi: 10.1109/ACCESS.2019.2948526.

[77]. E. Sarkar, P. Korshunov, L. Colbois, and S. Marcel, ―Vulnerability Analysis of Face Morphing Attacks from Landmarks and Generative Adversarial Networks,‖ *ArXiv*, vol. abs/2012.0, 2020.

[78]. C. Gray, ―Add to Cart: Why deepfakes are good for retail,‖ *AdNews Newsl.*, 2020.

[79]. H. Kronk, ―UDACITY DEVELOPED AN AI TO TURN INSTRUCTOR'S SPEECH INTO DEEPFAKE-STYLE VIDEO, BUT HAS NO PLANS TO USE IT,‖ *Elearning Insid.*, 2019.

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

[81]. 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.

[82]. 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.

[83]. 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.

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

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

[86]. 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.

[87]. 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.

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

[89]. 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

[90]. 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

[91]. L. Patel, —The Rise of Deepfakes and What That Means for Identity Fraud,‖ *DarkReading Authentication*, 2020, [Online].

[92]. Available: https://www.darkreading.com/authentication/the-rise-of-deepfakes-and-what-that-means-for-identity-fraud

[93]. 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/

[94]. 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/

[95]. 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.

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

[97]. 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.

[98]. 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.

[99]. 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.

[100]. 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.

[101]. 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.

[102]. 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.

[103]. U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, ―Deep Face Representations for Differential Morphing Attack Detection,‖

[104]. *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3625–3639, 2020, doi: 10.1109/TIFS.2020.2994750.

[105]. 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.

[106]. U. Scherhag, J. Kunze, C. Rathgeb, 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

[107]. 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

[108]. 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.

[109]. 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.

[110]. 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

[111]. 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.

[112]. 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.

[113]. M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, —A New Face Image Authentication Scheme based on Bicubic Interpolation,‖

[114]. *Al-Iraqia J. Sci. Eng. Res.*, vol. 2, no. 2, pp. 1000–1006, Jun. 2023, doi: 10.58564/IJSER.2.2.2023.68.

[115]. M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, —A New Face Region Recovery Algorithm based on Bicubic Interpolation,‖

[116]. *JOIV Int. J. Informatics Vis.*, vol. 7, no. 3, pp. 1000–1006, Sep. 2023, doi: 10.30630/joiv.7.3.1671.

[117]. M. H. Al-Hadaad, R. Thabit, and K. A. Zidan, —Tamper detection , localization , and recovery for digital face images,‖ 2020.

[118]. S. Hu, Y. Li, and S. Lyu, —Exposing GAN-Generated Faces Using Inconsistent Corneal Specular Highlights,‖ in *ICASSP 2021*

[119]. *2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, Jun. 2021, pp. 2500– 2504. doi: 10.1109/ICASSP39728.2021.9414582.

[120]. 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.

[121]. 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.

[122]. 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.

[123]. H. Li, B. Li, S. Tan, and J. Huang, —Detection of Deep Network Generated Images Using Disparities in Color Components,‖

[124]. *ArXiv*, vol. abs/1808.0, 2018.

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

[126]. 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.

[127]. 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.

[128]. 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

[129]. 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.

[130]. Z. Mi, X. Jiang, T. Sun, and K. Xu, —GAN-Generated Image Detection With Self-Attention Mechanism Against GAN

[131]. Generator Defect,‖ *IEEE J. Sel. Top. Signal Process.*, vol. 14, no. 5, pp. 969–981, 2020, doi: 10.1109/JSTSP.2020.2994523.

[132]. 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.

[133]. 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.

[134]. 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.

[135]. 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.

[136]. S. Hu, Y. Li, and S. Lyu, —Exposing GAN-Generated Faces Using Inconsistent Corneal Specular Highlights,‖ in *ICASSP 2021*

[137]. *2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2021, pp. 2500–2504. doi: 10.1109/ICASSP39728.2021.9414582.

[138]. 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.

[139]. 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.

[140]. 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.

[141]. 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.

[142]. I. Amerini, L. Galteri, R. Caldelli, and A. Del Bimbo, —Deepfake video detection through optical flow based cnn,‖ in

[143]. *Proceedings of the IEEE/CVF international conference on computer vision workshops*, 2019, p. 0.

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