A Systematic Literature Review on Face Morphing Attack Detection (MAD)

Mary Ogbuka Kenneth, Bashir Adebayo Sulaimon, Shafii Muhammad Abdulhamid, and Laud Charles Ochei

Abstract Morphing attacks involve generating a single artificial facial photograph that represents two distinct qualities and utilizing it as a reference photograph on a document. The high quality of the morph raises the question of how vulnerable facial recognition systems are to morph attacks. Morphing Attack Detection (MAD) systems have aroused a lot of interest in recent years, owing to the freely available digital alteration tools that criminals can employ to perform face morphing attacks. There is, however, little research that critically reviews the methodology and performance metrics used to evaluate MAD systems. The goal of this study is to find MAD methodologies, feature extraction techniques, and performance assessment metrics that can help MAD systems become more robust. To fulfill this study's goal, a Systematic Literature Review was done. A manual search of 9 well-known databases yielded 2089 papers. Based on the study topic, 33 primary studies were eventually considered. A novel taxonomy of the strategies utilized in MAD for feature extraction is one of the research's contributions. The study also discovered that (1) single and differential image-based approaches are the commonly used approaches for MAD; (2) texture and keypoint feature extraction methods are more widely used than other feature extraction techniques; and (3) Bona-fide Presentation Classification Error Rate and Attack Presentation Classification Error Rate are the commonly used performance metrics for evaluating MAD systems. This paper addresses open issues and includes additional pertinent information on MAD, making it a valuable resource for researchers developing and evaluating MAD systems.

M. O. Kenneth (✉) · B. A. Sulaimon
Department of Computer Science, Federal University of Technology, Minna, Nigeria
e-mail: kenneth.pg918157@st.futminna.edu.ng

B. A. Sulaimon
e-mail: bashirsulaimon@futminna.edu.ng

S. M. Abdulhamid
Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
e-mail: shafii.abdulhamid@futminna.edu.ng

L. C. Ochei
Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria
e-mail: laud.ochei@uniport.edu.ng

S. Misra and C. Arumugam (eds.), *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, Lecture Notes on Data Engineering and Communications Technologies 109, https://doi.org/10.1007/978-3-030-93453-8_7

Keywords Face morphing · Morphing attack detection · Systematic literature review · Feature extraction techniques · Performance metrics

1 Introduction

Biometric characteristics such as face, iris, voice and fingerprint are natural tool in carrying out identification task such as in border control, e-Government application, law enforcement, surveillance, e-commerce applications, user verification in mobile phones and many more [1–3]. Face as a biometric characteristics are regularly used as a means of identification because of the noninvasive nature of its capture process and consumer usability [4]. Face as a means of identification are presented for many forms of documentation worldwide, including, voters card, national identity card, international passports and driving licenses. Face recognition systems are commonly used for automatic recognition of individuals by observing their facial biometric characteristics [5–7].

The deployment of face recognition systems are on the rise due to its accurate and reliable face recognition algorithms, hence the attacks on these systems become more creative [8–10]. Examples of attacks faced by face recognition systems includes the presentation attack [11] such as spoofing that presents a copy of an individual characteristics in order to impersonate that individual [12], and concealed face attacks that aim to disable face recognition using physical objects. Another form of attack identified by Seibold [13] is the face morphing attack. This attack aims to present one face comparison picture which is automatically matched successfully to more than one individual and by human experts [14, 15].

Face morphing can present a serious security threat when these morphed photographs are used in identification or passports, enabling multiple individuals (subjects) to verify their identity with that linked to the presented paper [15–17]. This defective connection of multiple subjects with the document could result in a variety of illegal activities such as human trafficking, financial transaction, and illegal immigration [8]. A targeted offender would morph his face photograph with another of the lookalike partners in a real-life situation of a face-morphing attack. If the partner requests an e-passport with the transformed face photograph, he/she will obtain a legitimate e-passport configured with document security features that match. Both the partner (accomplice) and the criminal could be authenticated against the morphed image stored in the e-passport with success. This means that the offender can use the e-passport granted to the accomplice to pass through the Automatic Border Control gates or maybe even pass through the human inspections at the gate [18]. Hence automatic detection of this face morphing attack is of great importance.

In the previous years, there have been few authors who have worked on detection of face morphing attacks. In 2014 Ferrara [19] introduced the face morphing attack which was called the magic passport. The viability of attacks on Automated Border Control (ABC) systems using morphed face images was examined and it was

concluded that when the morphed passport is presented; if the passport is not substantially different from the applicant's face, the officer will recognize the photograph and release the document. And thus the released document passes all authenticity checks carried out at the gates. Raghavendra [20] carried out a novel research on how this face morphing attack can be detected. The research was conducted using facial micro-textures retrieved via statistically independent filters which are trained on natural photographs. This variation in micro-texture was extracted using Binarized Statistical Image Features (BSIF) and classification had been made via Support Vector Machine (SVM). This was the first research done towards detection of face morphing attacks.

Later in 2017 Seibold [21] aimed to detect face morphing attack using deep neural network. Three Convolutional neural network architecture were trained from scratch and using already trained networks for the initialization of the weights. Pretrained networks was noticed to outperform the networks trained from scratch for each of the three architecture. Hence it has been concluded that the features acquired for classification tasks are also useful for MAD. In 2018 and 2019 researchers such as Singh [22] and Wandzik [23] proposed MAD using deep decomposed 3D form and diffuse Reflectance and a General-Purpose Face Recognition System, respectively. Peng [22] did not just stop at detecting face morphing attack but went further to de-morph the morphed face image using generative adversarial network to rebuild facial image of the accomplice.

Other researchers were able to perform review of image morphing and face morphing attacks in a general scope but no related works were found that conducted a SLR of face morphing attack. A gap in the domain of biometric systems that needs filling is the lack of existing literature that provides systematic knowledge regarding MAD with the ability to further research, given vital information. The aim of this paper is thus to review the current literatures on MAD techniques in a systematic way.

The paper's primary contributions are to:

1. Present a novel taxonomy of feature extraction techniques used in face morphing attack detection (MAD).
2. Present information on commonly used approaches for morph attack detection, feature extraction techniques, and performance evaluation measures for evaluating morphing attack detection systems.
3. Present open issues and challenges of face morphing attack detection.

The remainder of this paper is structured according to: a summary of previous works on MAD was presented in Sect. 2. The Review method used in carrying out the study is presented in Sect. 3. Section 4 shows the results obtained after review and the presented results were discussed. Section 5 presents the Parametric used in MAD. Taxonomy of MAD techniques are presented in Sect. 6. Section 7 presents open issues and future directions in the field of MAD. In Sect. 6 conclusions were drawn and Appendix A presents a list of the primary studies identified.

2 Previous Related Surveys

Face Recognition (FR) systems were found vulnerable to morphing attacks. Based on this vulnerability, Korshunov [24] focused on assessing the vulnerability of FR systems to deep fake videos where actual faces are replaced by an adversarial generative network that generates images trained on two subjects/people's faces. Two existent FR algorithm based on Facenet and VGG neural networks were evaluated and it suggests that both algorithms were susceptible to deep morphed video as they do not differentiate morphed videos from the actual videos with a Detection Equal Error Rate (D-EER) of up to 95.00%. It was also observed that baseline detection algorithms based on the image quality measurements with SVM classifier could identify high quality deep morph videos with a D-EER of 8.97%.

Scherhag [25] conducted review of the currently proposed morphed facial image detectors regarding their robustness across various databases. The aim of this survey was to identify reliable algorithms for detection. It was concluded that the majority of current detection techniques do not appear to have great performance across various databases showing that morph detectors on a single database could cloud the overall appearance of the real detection results.

Kramer [26] conducted four different experiments to investigate the performance of humans and computers with high quality facial morphs. These four experiments include morph detection using computer simulation, using live-face matching, induced morph detection and tips, and finally research based on Robertson [17] replication using morphs of higher quality. Based on these tests, it was discovered that humans were extremely susceptible to error when detecting morph and also human training on MAD did not yield change. In a live matching experimentation, morphs were also acknowledged as bona fide images; and poses a major concern for security agencies, therefore this demonstrated that identification was again prone to error. Finally, it was established that a simple computer model outperformed the human participants. Ultimately it was established that the human participants were outperformed by a simple computer model.

Makrushin [27] conducted a survey on recent developments in the assessment and mitigation of face morphing attack. It was discovered that the identification of morphed facial images at the human and automated facial recognition systems level was needed to mitigate morph assault It was also found that existing MAD algorithms still have significant high error rates and that the performance of these MAD algorithms severely degrades with images that are re-digitalized and manipulated anti-forensically. It was also proposed that extensive work on the limitations of the MAD techniques should be carried out.

Scherhag [28] conducted a study on facial recognition systems under morphing attacks. This survey was based on conceptual categorization and metrics for an assessment of MAD techniques and a rigorous survey of related literature, in addition open issues and challenges based on Face morph attacks in face recognition systems was carried out. In this survey three steps of morphing process of face images was identified. The first step was determination of the correspondence between the

Table 1 Related survey overview

S/No	References	Number of cited references	Scope of time covered
1	Scherhag [28]	124	1986–2018
2	Makrushin [27]	46	1998–2018
3	Scherhag [25]	22	2004–2018
4	Kramer [26]	39	1993–2019
5	Korshunov [24]	22	2014–2019

contributing samples. Secondly warping which entails distortion of both images to achieve geometrically alignment between sample images and the third step called blending which deals with merging the color values of the warped images. Based on their survey the quality of the created face morphed images can be accessed based on the image quality, morphing artifacts, plausibility of face morph and human insight of morphed images. Lastly drawbacks of studies related to face morphing and MAD were identified which are lack of automatic creation of high-quality face morphs, no available measures for susceptibility of FR systems with respect to morphing attacks and lastly MAD were prone to over fitting. Overview of the related survey is depicted in Table 1.

3 Review Method

Performing SLR in a specific field is necessary to define research issues, as well as to explain potential work in that area [29, 30]. SLR was selected as the tool of inquiry. This study uses SLR guidance, which is a method of secondary analysis that uses consistent and well-defined measures to classify, analyze and interpret all existing evidence relevant to a specific research question [31]. The SLR procedure aims to be as fair as possible by being auditable and repeatable [29]. The SLR process aims at being verifiable and repeatable as equally as possible [29]. The aim of SLR, based on Soledad [32], is to have a potential list of all research that are relevant to a particular subject area. Whereas, general reviews attempt to sum up findings from a variety of studies. The SLR cycle consists of three consecutive phases of preparation, executing, and reporting. The preparation process also known as the planning phase is conducted in this section which involves identifying the research questions as well as how the analysis is conducted [32].

3.1 Review Design

The review design outlines the basis of this analysis by identifying the research questions for the SLR and keywords for search.

3.1.1 SLR Research Questions

Very few researchers have performed face morphing attack identification over the years. Hence the SLR research questions that this study aims to address are:

1. Which approaches are used for detection of face morphing attacks?
2. What feature extraction techniques are used for detection of face morphing attack?
3. Which performance metric are used to evaluate face morph attack detection algorithms?

3.1.2 Search Strategy

The SLR focuses on looking for relevant books or technical papers in the academic repositories. This paper used nine (9) repositories to do the search process for SLR. The following are the repositories used:

1. Scopus (www.scopus.com)
2. Google Scholar (www.scholar.google.com)
3. IEEE Xplore (www.ieeexplore.com)
4. Semantic Scholar (www.semanticscholar.org)
5. ScienceDirect (www.sciencedirect.com)
6. ACM Digital Library (dl.acm.org)
7. Springer link (link.springer.com)
8. Taylor & Francis (taylorandfrancis.com)
9. International Scientific Indexing (isindexing.com).

The repositories were selected because they provide important and maximum impact full-text articles and conference papers, typically covering the areas of MAD.

The search keywords used to locate specific studies in the title of the document, keywords and abstract are as follows: "face morphing" OR "face image modification" AND "face morphing attack" OR "face alteration attack" AND "face morphing attack detection".

3.2 Review Conduction

This segment on review conduction specifies the evaluation process for performing the SLR. The SLR evaluation protocol refers to the review structure and rules [33].

Table 2 Inclusion and exclusion criteria

Inclusion criteria	Abstract and title are written in English Full-text article Study that concentrated on face morphing attack detection
Exclusion criteria	Study that does not address face morphing attack detection Duplicate article Short paper Study not written in English

3.2.1 Inclusion and Exclusion Criteria

This SLR used the parameters for inclusion and exclusion set out in Table 2. On the basis of Table 2, papers which do not focus on the detection of face morphing attacks have been omitted. SLR also removes duplicate papers of the same report.

3.2.2 Study Selection

Study selection was achieved using the below processes [34]:

1. Database search using the search keywords to find relevant studies.
2. Exclude studies based upon the criteria for exclusion.
3. Exclude any insignificant study based on the examination of their titles and abstracts.
4. Assessing the selected studies based complete reading and quality checklist.
5. Extracting responses relating to study issues.
6. Obtain Primary studies.

3.2.3 Quality Assessment

As per Okoli [35] SLR guidelines Quality Assessment (QA) questions must be well-defined to evaluate the credibility of the research paper and also provide a quantitative measure among them. The rating methods are Y (Yes), P (Partially) and N (No). The checklist/questions for quality assessments described in this SLR are shown in Table 3.

3.2.4 Data Extraction

The data collection tools that were used to perform an in-depth analysis for all selected primary studies is presented in Table 4.

Table 3 Quality assessment: checklist

S/No	Question	Score
1	Are the data collection methods adequately described	a. Yes: it explicitly describes the methods used to collect the face morph images b. Partially: it only mentioned the data collection method without further explanation c. No: Data collection method was not listed or clarified
2	The used techniques are they clearly described and their selection justified?	a. Yes: it either clearly describes the techniques used to detect face morphing attack b. Partially: it only gave a peripheral explanation of the techniques c. No: it neither described nor mentioned the techniques for face morphing attack detection
3	How precisely were the limitations to the research documented?	a. Yes: It clearly clarified the proposed algorithm's restriction b. Partially: The restrictions were stated but it did not clarify why c. No: The restriction was not stated
4	Were the discoveries credible?	a. Yes: The analysis has been clarified methodologically so the result can be trusted b. Partially: the analysis has been clarified in methodological terms but not in depth c. No: The research wasn't clarified methodologically

Table 4 Extracted data form

S/No	Data extracted	Description	Type
1	Bibliographic references	Authors, publication year, title and the publishing source	General
2	Study type	conference paper, Text, journal, lecture paper, workshop paper	General
3	Approaches for detection of face morphing attacks	Description of the approaches of face morphing attack detection	Research question (RQ)
4	Feature extraction techniques	Description of the feature extraction techniques for MAD	RQ
5	The performance metric	Performance metric are used to evaluate face morph attack detection algorithms	RQ
6	Findings/contribution	Displaying research results and feedback	General

3.2.5 Synthesis

Analytical results via SLR showed 102 studies for further deliberation. The selected 102 studies were thoroughly reviewed but only 33 publications were left which could address the study question of this SLR. Those 33 publications have therefore been selected as primary studies. Figure 1 Displays the number of studies per systematic procedure.

Figure 2 Displays the number of primary studies by published year. All 33 publications selected have been published from 2016, 2017, 2018, 2019 and 2020. It can be seen that 2018 has the highest selected papers with 15 articles compared to the other years

4 Results and Discussion

This segment reports the findings and discussion after conducting the SLR for answering the defined question of SLR research. Furthermore, the responses to the SLR questions which were obtained from selected primary studies based on specified forms of data extract are discussed.

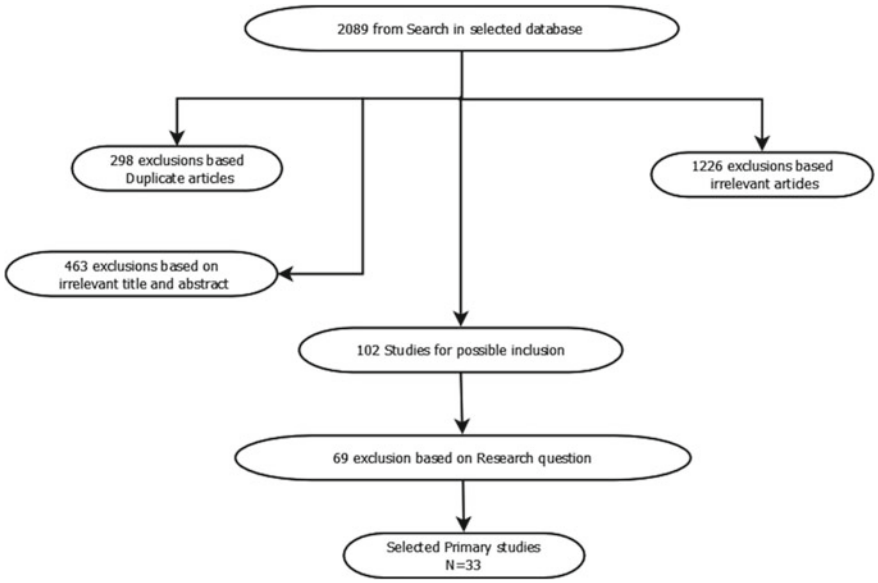

Fig. 1 Procedure for finding primary study

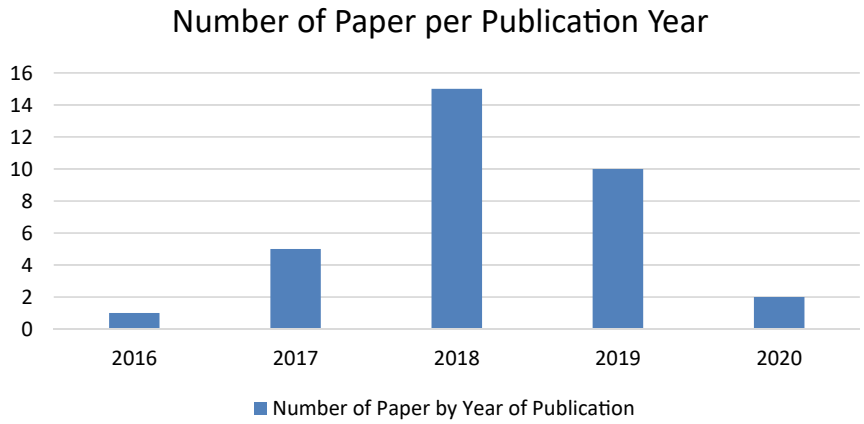

Fig. 2 Number of paper per publication year

4.1 Result

This section includes the results of the SLR research questions.

4.1.1 Finding Research Questions

RQ1: Which approaches are used for detection of face morphing attacks?

Studies were analyzed to answer this question, and as a result, two approaches to MAD was identified. This two approaches are reflected in Table 5. Table 5 provides the list of primary studies which address the MAD approaches described. Approach (1) has 16 papers dealing with approach, and two papers address approach (2).

RQ2: What feature extraction techniques are used for detection of face morphing attack?

The feature extraction techniques identified for face morphing attack detection are displayed in Table 6. In Table 6 technique (1), (5), (7), (8), (9), (10), (17) and (18) are used by one paper respectively, technique (2), (6), (11), (15), (16) and (19) are used by two papers respectively, technique (3) and (14) are used by five papers,

Table 5 Number of primary study addressing the identified approaches

S/N	Approaches	Number of papers	Study identifiers
1	Single image-based	30	P32, P33, P28, P12, P25, P1, P13, P2, P5, P3, P16, P23, P27, P11, P18, P9, P8, P30, P7, P19, P20, P21, P14, P17, P10, P15, P22, P24, P26, P29, P31
2	Differential image-based	4	P4, P6, P22, P20

Table 6 Number of preliminary survey addressing the identified feature extraction techniques

S/N	Feature extraction techniques	Number of papers	Study identifiers
1	Steerable pyramid	1	P14
2	Binarized statistical image features (BSIF)	2	P2 and P18
3	Local binary pattern (LBP)	5	P2, P15, P5, P13, P8
4	Deep neural networks	9	P2, P17, P12, P3, P16, P11, P1, P8, P7
5	Histogram of oriented gradients (HOG)	1	P2
6	Photo response non-uniformity (PRNU)	2	P10, P9
7	Scale invariant feature transform (SIFT)	1	P2
8	Regressing local binary features (LBF)	1	P6
9	Distance based	1	P4
10	Local phase quantization (LPQ)	1	P8
11	Benford features	2	P19, P32
12	FAST	4	P29, P26, P24, P29
13	AGAST	3	P24, P26, P29
14	SURF	5	P22, P23, P24, P27, P29
15	Sobel & canny	2	P29, P24
16	Discrete fourier transform	2	P29, P31
17	Shi Tomasi	1	P26
18	Laplacian pyramid	1	P28
19	Oriented BRIEF (ORB)	2	P29, P24

technique (4) has the highest number of papers with nine papers, technique (12) is used by four paper and finally technique (13) is used by three papers.

RQ3: Which performance metric are used to evaluate face morph attack detection algorithms?

Table 7 depict the identified performance metric and the number of papers that addresses them. In Table 7, 17 papers evaluate using (1), 29 papers evaluate using (2), 30 papers evaluate using (3), 1 paper evaluates using (4) and lastly 2 papers evaluate using (5).

Table 7 Number of primary study addressing the identified performance metrics

S/N	Performance metrics	Number of papers	Study identifiers
1	Detection-equal error rate (D-EER)	17	P23, P25, P27, P13, P2, P3, P10, P9, P12, P30, P33, P1, P8, P17, P7, P22, P28
2	Bona fide presentation classification error rate (BPCER)/false rejection rate (FRR)	29	P13, P2, P19, P20, P14, P5, P3, P9, P12, P1, P8, P7, P6, P16, P11, P27, P29, P30, P18, P17, P4, P22, P23, P24, P25, P28, P31, P33, P21
3	Attack presentation classification error rate (APCER)/false acceptance rate (FAR)	30	P32, P19, P20, P21, P13, P2, P27, P14, P5, P23, P24, P25, P3, P9, P12, P29, P1, P31, P8, P7, P6, P16, P11, P18, P17, P4, P22, P28, P30, P33
4	True positive rate	1	P32
5	Accuracy (ACC)	3	P11, P15, P26

4.2 Discussion

Discussion about this SLR is provided in this section. The discussion is based on the research problem set out in Sect. 4.1.1.

4.2.1 Approaches to Face Morphing Attack Detection

Single Image-Based

The existence of morph alterations is identified here on a single image, like the identity passport provided to the officer at the time of registration or the face picture read from an e-document during authentication at the gate [36, 37]. This means that the single given image is processed by the detector and classified as either morph or bona-fide without any reference image [4]. There are two types of single image-based approach. These are the print-scan attack detection and digital attack detection.

1. **Print-Scan Attack Detection**

   The original images be it morphed or bone-fide are first printed a printer and then scanned with a scanner. This method of printing/scanning alters the image content, eliminating most of the fine details (that is, digital artefacts) which might help identify morphing [38]. Literatures that addressed morphing attack detection based on print-scan images are P14, P17, P10, P15, P12, P25, P28, P33 and P1.
2. **Digital Attack Detection**

   Here the digital copy of the bona fide and morphed images captured by the camera is being used without having to undergo any kind of post-processing

like print-scan. This is the most commonly used approach in the literatures. Literatures that adopted this approach includes P30, P13, P24, P27, P2, P5, P3, P16, P11, P21, P10, P23, P32, P18, P9, P33, P20, P8, P19, P31, P29, P26, P25, P22 and P7.

Differential Image-Based (Image-Pair Based Approach)

This approach deals with the contrast between a live image (for example, the image obtained at the gate) and the one stored on the electronic record in order to perform MAD [38]. Recently, some works have explored differential image-based detection approach. These researches has indicated that introducing a bone fide reference image permits for a whole new set of techniques [39].

In P4 research the angles and distances between the passport's facial landmarks and the bona fide picture are compared. The angle comparison gives the best results, but the classification error rates are not yet small enough for real-world use. Hence in future work the technique can be combined with a texture based technique to achieve small classification error rate.

To examine MAD involving a bona fide probe image, P6 created a repository of paired images between the reference images investigated (whether morphed or bona fide) and the probe images (assumed to be live captures). Each reference image is matched with similar images. The probe photographs, however, are the frontal face photographs captured by the very same users in different sessions than the reference images. Consequently P6, P4, P20 and P22 used differential image based technique.

4.2.2 Face Morphing Attack Detection Feature Extraction Techniques

Steerable Pyramid

Steerable Pyramid developed by Simoncelli & Freeman's [40] is a sequential multiple scales, multiple oriented image decomposition that offers a good front-end for computer vision and image processing applications [40, 41]. This could be seen as a selective alignment variant of the Laplacian pyramid, during which a steerable filter bank is used at each pyramid level instead of a single Laplacian or Gaussian filter. P14 used these techniques to remove scale-space features (morphed or bona-fide) from pictures. The scale-space is essentially a collection of directed filters synthesized as a linear combination of the fundamental functions. This technique has been described as being successful in morphing attack section since the extracted texture features can easily reflect visual distortion throughout the image.

Binarized Statistical Image Features (BSIF)

It is a local feature descriptor built by binarizing the reactions to linear filters but, in contrast to previous binary descriptors, the filters are learned from natural images utilizing independent component analysis [42]. This feature extraction technique was used by P2, P18, P22, P23 and P27.

Local Binary Pattern (LBP)

Local binary patterns (LBP) is a form of visual descriptor which is used in computer vision classification [7, 43]. LBP is indeed a type of gray scale that supports the local contrast estimate of an image within the reach of the texture measure. LBP is originally specified in an eight-pixel neighborhood, and the center pixel gray value is set as a threshold. All neighbors having values greater or equal to the center pixel value are given a value of 1, otherwise they are set as 0 [1]. The values upon thresholding (notably 0 or 1) will increase with the corresponding pixel weight, respectively, and their multiplicative result will be the LBP value [44]. One drawback of LBP found by [44] is its vulnerability to changes in noise and lighting. The following literatures used this extraction technique for MAD: P22, P23, P27, P28, P15, P2 and P5. P13 made use of the LBP pyramid, an extension of LBP. The features of the Pyramid-Local Binary Component (P-LBP) were being used to efficiently measure residual noise, as it has been proven by literatures to be effective in modeling the residual noise. P20 and P21 used LBP histogram.

Deep Neural Networks (Convolutional Neural Network)

The convolutional neural network (CNN) [45] is among the most popular feature extraction techniques used for MADs. This technique is also used for extracting profound features from images. CNN is a multilayer network of neurons; each layer consist of multiple 2D surfaces, and each plane consist of multiple independent neurons [46, 47]. CNNs comprises of many connections, and the architecture is composed of different types of layers, including pooling, convolution and fully-connected layers, and realize form of regularization [48]. CNN makes use of deep architecture to learn complicated features and functions that can represent high-level abstractions. P20, P25 and P21used CNN architecture for feature extraction, P16 used scratched and pre-trained alextNet, googleNet and VGG19 architecture for extraction and analysis. It was noted that pre-trained VGG19 achieved the best result. P3, P11, P12 and P33 used pre-trained AlexNet architecture, P33, P8 and P1 used VGG architecture, faceNet a popular model for face recognition and verification [49] was used by P17 for MAD while P2, P7 and P22 used the OpenFace Model.

Histogram of Oriented Gradients (HOG)

The histogram of oriented gradients (HOG) is a feature descriptor centered on the gradient approximation used for object recognition purposes in computer vision and image processing. HOG descriptor method counts gradient orientation instances in localized portions of an image identification window, or region of interest (ROI). Because HOG is invariant to photometric and geometric transformations, it is very well adapted for human detection [50]. HOG was implemented for MAD by P2, P22, P23 and P27 given the fact that the morphing process decreases the variations in high frequencies and thus the steepness of the gradients is reduced which improves MAD.

Photo Response Non-uniformity (PRNU)

The PRNU is a distortion-like pattern, which originates from small differences between individual pixels during the digital photo sensor transformation of photons into electrons. It forms an intrinsic part of those sensors, while this weak signal is incorporated in any image they capture [51–53]. P9, P10 and P30 used PRNU for MAD as all image sensors exhibit PRNU. PRNU exists in each image irrespective of the scene content, except fully dark or over-exposed images, and PRNU survives, gamma correction, filtering, loss compression and several other processing method [54, 55].

Scale Invariant Feature Transform (SIFT)

SIFT is a computer vision Keypoint extractor algorithm used for the identification and definition of local features in images [56]. By using a staggered filtering technique, the scales-invariant features are well defined. In the early stage, key locations are identified by looking for positions with a difference of Gaussian function that are maximum or minimum [57]. A character vector that defines the sampled region of the local image relative to its scale space frame is then used for each point [58]. SIFT Keypoint extractors were used for P2, P22, P23, P24, P27 and P29 as morphed photos are assumed to comprise of fewer key locations, which are described as maxima and minima resulting from the difference in function of Gaussians. This keypoint identification is used as descriptive function for MAD.

Regressing Local Binary Features (RLBF)

The detector proposed by Ren [59] is a landmark detector. Where a variety of local binary characteristics and a local theory have been used to learn these features. Lowe [58] proposes that each facial landmark learn independently of a set of highly discriminatory local binary features, then use them to learn a linear regression together for

the final mark detection result. P6 used a characteristic extractor for MAD based on an approach focused on differential images.

Distance Based

In a differential image scenario, this method was used by P4 for MAD. The landmarks of both the image of bona fide and the morphed images were evaluated by the predictor of the facial landmark of dlib [60]. The landmarks are standardized to a range between 0 and 1 to achieve a scalable-robust method. Next the Euclidean distance between bona fide and morphed images, which results in a 2278 long vector known as the distance characteristics, is determined for each landmark's relative location. The results obtained by P4 are not appropriate for operational deployment but is an initial step to MAD based on reference.

Local Phase Quantization (LPQ)

Initially, Ojansivu [61] proposed the LPQ operator which is a texture descriptor. LPQ focuses on the Fourier component spectrum's blurring invariance property. It uses the local phase data extracted using the transformation of 2-D Short Term Fourier (STFT), measured on each pixel of the image over a rectangular district [61]. Due to the robustness of the image, LPQ was adopted by P8.

Benford Feature

The rule of Benford states: in a set of natural numbers, the first digits distribution is a logarithmic [62]. That is it is a likelihood distribution for the probability of the very first digit in a set of numbers. Benford characteristics can be used in natural data sets for pattern or pattern loss detection [63]. The use of Benford's features for pattern detection has led Fu [64] to suggest it in JPEG format compressed images for tamper detection. Hypothesis behind applying Benford's characteristics by P19 for MAD is that the naturally produced data are in accordance with Benford law and the altered data infringes the law. P32, also used Benford's rule for morphed face image detection.

Features from Accelerated Segment Test (FAST)

FAST is an existing algorithm for the identification of interest points in an image originally introduced by Rosten and Drummond [65]. FAST uses one variable which is the threshold of intensity between the middle pixel and the ones in a circular ring around the middle [66]. FAST is measured easily and quickly to match. The precision is pretty good, too. FAST does not represent a scale-space detector, so the detection of the edges at the particular scale can produce much more than a scale-space technique like SIFT [67]. P24, P26 and P29 used FAST descriptor for MAD.

Adaptive and Generic Accelerated Segment Test (AGAST) Features

AGAST has been designed to address the limitation of the FAST algorithm that includes: FAST needs to learn from an image dataset in the context in which it operates, and then generate a decision tree to identify each center pixel as a function or not. However, this approach cannot guarantee that every pixel combination will be discovered, and this can yield inaccurate results [68, 69]. Additionally, each time the working context shifts, the FAST feature detector must be trained from scratch [68]. AGAST is founded on the same criteria of Accelerated Segment Test feature as FAST, but utilizes another decision tree. AGAST is trained on the basis of a set of data with all possible 16 pixel combinations on the circle included. This guarantees that the decision tree is working in any setting. AGAST performance increases for random scenes, and AGAST operates with no training steps in any arbitrary environment [65]. P24, P26 and P29 used AGAST descriptor for MAD.

Shi Tomasi Features

The Shi Tomasi is an angle/corner detector entirely based on the detection of Harris corner [70]. A small change in a selection criterion, however, has enabled this detector to perform even better than the initial. Also, the Shi Tomasi can be characterized as an enhancement on the Harris technique, using only the lowest eigenvalues for discrimination, thus significantly streamlining the computation [71]. Shi Tomasi was used for MAD by P26.

Oriented FAST and Rotated BRIEF (ORB) Features

ORB is a mixture of the famous FAST key point descriptor with some modification of the Binary Robust Independent Elementary Feature (BRIEF) descriptor [72]. ORB is a simple binary descriptor founded on the BRIEF, which is noise tolerant and rotation invariant [66]. These techniques provide good performance and have low cost [72]. Firstly, ORB utilizes FAST to identify the key points. A Harris corner formula for locating top N points is then added. FAST is not used for orientation calculation, and is a variant to rotation. Hence it used to measure the intensity weighted centroid with center corners located [73]. The rotation matrix is calculated by utilizing the patch orientation, and the orientation of the BRIEF descriptors is steered [67]. ORB was used by P24 and P29 for MAD.

Discrete Fourier Transform (DFT)

DFT is a technique for signal processing [74]. It is a transform dealing with a countable discrete-time signal and a discrete amount of frequency [75]. DFT translates a signal for the time domain to its relative frequency domain. This frequency domain depiction of the time domain signal is named the signal frequency spectrum [74]. Hence the spectrum of the signal shows the range of frequencies and their amount

that are present in the time domain signal. Sensor Pattern Noise (SPN) is a deterministic factor which remains almost the same if multiple images are taken from the exact same location. Because of this property, the SPN is present in any image a sensor captures, and can therefore be used to classify the source of the image [76, 77]. P31 used the differences in the Fourier frequency spectrum of the SPN of the images to differentiate between morphed and bona fide images [78]. P29 used the frequency domain representation of the time domain signal as feature for MAD [79].

Speed up Robust Features (SURF)

SURF is a powerful algorithm for image registration and object recognition. SURF describes the local texture features of key points in different directions and scales of the image and it remains invariance to rotation, brightness, and scaling changes [80]. SURF uses the Hessian Blob Detector (HBD) to identify interest points on an image [81, 82]. HBD is based on the scale-space depiction of the Hessian matrix, computed in box filters, so that Hessian matrix elements can be properly measured using integral images at really low computational expense [72, 83]. The SURF descriptor was used by P22, P23, P24, P27 and P29 for MAD.

Canny and Sobel Edge Detection

Edge Detection is an operation finding boundaries that limit two homogeneous image regions that have different brightness levels [84]. The aim of edge detection algorithms is to generate a line drawing of the loaded image. The extracted characteristics could be used to recognize and track objects. The Sobel operator is a discrete differential operator that uses two kernels measuring 3×3 pixels to calculate the gradient [85]. One kernel evaluates the gradient in the x-direction, and the other one evaluates the gradient in the y-direction [86, 87]. The gradient is determined using the formula of Eq. 1:

$$\boldsymbol{G} = \sqrt{\boldsymbol{S_x}^2 + \boldsymbol{S_y}^2} \tag{1}$$

where G: Sobel gradient operator value, S_x: Horizontal gradient and S_y: Vertical sobel gradient.

The Canny Edge Detector is commonly referred to as the optimal detector, developed by John F. Canny in 1986 [88]. The steps involved in canny operator are: firstly, to process the images, a Gaussian filter is introduced to eliminate noise in an image. Secondly the magnitude of the gradient is calculated. Thirdly, non-max suppression is implemented by the algorithm to omit pixels that are not part of an edge. Finally the thresholding of hysteresis is used across the edges [86]. The features from the sobel and canny edge detector were used by P24 and P29 for MAD.

Laplacian Pyramid

The Laplacian pyramid, is a band-pass image decomposition originating from Gaussian Pyramid which is a multi-scale image depiction produced by a recursive reduction of the image set [89]. Laplacian pyramid was used by P28 to remove details from the spatial information by decomposing color space pictures into various scales.

4.2.3 MAD Performance Metric

Five performance metric were adopted by the primary papers in evaluation of face morphing attack detection systems. This five performance measure are as follows.

Bona Fide Presentation Classification Error Rate (BPCER) OR False Rejection Rate (FRR)

This is to be described as the percentage of genuine presentations wrongly classified as presentation attacks in a particular scenario or as the relative quantity of genuine images categorized as morphing attacks [90]. BPCER can also be characterized as the expected percentage of transactions incorrectly rejected with truthful claims of identity (in a positive identity system) [91]. P29, P13, P23, P2, P14, P5, P11, P3, P20, P9, P28, P12, P1, P27, P16, P8, P31, P25, P7, P33, P6, P19, P22, P30, P24, and P18 made use of this performance metric for MAD performance evaluation.

Attack Presentation Classification Error Rate (APCER) OR False Acceptance Rate (FAR)

This is described as the percentage of attacks that use the same presentation attack device species incorrectly classified as true (bone fide) presentations in a particular scenario or it can be described as a relative number of morphing attacks classified as true images [90, 92]. P29, P13, P23, P2, P14, P5, P11, P3, P20, P9, P28, P12, P1, P27, P16, P8, P31, P25, P7, P33, P6, P19, P22, P30, P24, and P18 made use of this performance metric for MAD performance evaluation.

Detection-Equal Error Rate (D-EER)

D-EER is an algorithm used to describe the BPCER Threshold values and it's APCER. The common value obtained when the rates are same/equal is called the equal error [90]. The common value indicate that the APCER percentage is the same as the BPCER percentage. This is the position at which BPCER = APCER. It is used as the optimal point during training. The lesser the D-EER, the greater the biometric system's precision. On the basis of the assessed decision threshold (θ), (APCER (θ)

+ BPCER (θ))/2) is used as the detection error. This performance metric was used by P13, P2, P3, P10, P9, P12, P1, P8, P22, P23, P25, P27, P28, P30, P33 and P7.

Accuracy (ACC)

This is described as the percentage of correctly categorized images in relative to all categorized images [93–95]. Accuracy was used by P11 and P26 as a performance measure. The formula for calculating ACC is presented in Eq. 2

$$\text{ACC} = \text{correctly classified images}/\text{all classified images} \tag{2}$$

True Positive Rate (TPR)

TPR also called Sensitivity or Recall estimates the percentage of actual positive categorized as such (for example, the amount of morphed pictures recognized as an attack [93, 94, 96]. This can be calculated using the formula in Eq. 3:

$$\text{TPR} = \text{TruePostiive}/(\text{TruePositive} + \text{FalseNegative}) \tag{3}$$

5 Parametric Discussion

This section presents a tabular discussion of parameters used in Morphing Attack Detection (MAD). The parameters used in MAD are discussed in Table 8.

6 Taxonomy of MAD Techniques

Based on the SLR performed the techniques used for MAD can be grouped into 6 broad taxonomies founded on the detected and extracted image features. This taxonomies is as shown in Fig. 3:

1. **Texture Descriptor**: Texture is an attribute used to separate images into regions of interest and to categorize those regions. Texture includes information regarding the spatial configuration of colors or intensities in an image or selected region of image. It is anticipated that the image morphing process will lead to a change in the textual properties of morphed images which will make it a useful function for differentiating between morph and bona fide images. LBP, LPQ, BSIF and RLBF are the descriptors which fall into this category.

Table 8 Parameters used in MAD

S/No	Parameters	Discussion
1	Training dataset	This are morphed and bona fide images used to train a MAD algorithm. The better the training dataset the better the MAD algorithm. It is mostly 70% of the overall dataset
2	Testing dataset	This are morphed and bona fide images used to test the efficiency of a MAD algorithm after been trained with the training dataset. With the testing dataset an algorithm accuracy can be tested. it is mostly 30% of the overall dataset
3	Landmark-detection	One important parameter used for MAD is landmark detection. This is preprocessing stage used to detect and normalize morphed and bona fide images according to important face features such as the mouth, eyes, and nose. With landmark detection the facial image can be cropped to focus on just the facial features for better MAD
4	Feature extraction	It is a sort of dimension reduction that effectively represents a compact characteristic vector for interesting sections of the images. Features extracted are used to determine whether an image is morphed and bona fide. Example of feature extractors are local binary pattern, steerable pyramid etc.
5	Classification	This is about determining which of a set of groups to which the individual testing data set belongs, based on the training data set whose membership in the category is identified. In MAD there are two category of classification which are bone fide image or morphed image
6	Scenario	Deals with approaches used in MAD. And there are only two scenario which are reference (differential) based scenario and no-reference (single-image) based scenario
7	Post-processing	Deals with parameters that can alter the natural characteristics of a morphed imaged to prevent attack detection. Example of this parameters are image sharpening, print-scan operation and image compression

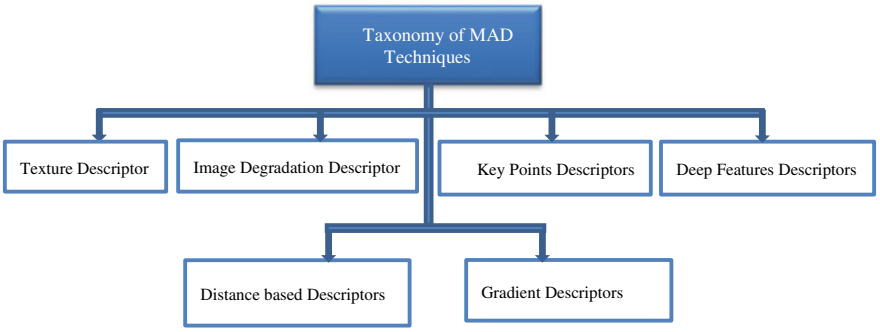

Fig. 3 Taxonomy of feature extraction techniques in MAD

2. **Image Degradation Descriptor**: The descriptors in this category takes advantage of degradations present in images. Image morphing leads to several image degradation due to the artefacts created by morphing process, hence making these degradations important features for MAD. The descriptors in this group includes: PRNU, Laplacian Pyramid, Benford features, DFT and Steerable Pyramids.
3. **Key Points Descriptors**: These descriptors does not just deal with merely 2D locations on the image but with 3D locations on the image scale space. This locations are the x, y and scale coordinates. Key point descriptors are used for MAD, as morphed images are supposed to comprise of fewer key point locations that are described as the maximum and minimal result of Gaussian function difference. Hence the quantity of extracted key points can be used as a useful feature for MAD. The descriptors in this category include: SURF, SIFT, FAST, AGAST, ORB and Shi Tomasi.
4. **Deep Features Descriptors**: A deep attribute is the coherent layer response within a hierarchical structure to an input that gives an answer relative to the final output of the model. Recent researches on face recognition has shown that the use of deep features for object recognition and classification have achieved good performance and easy adaptability. This advantages makes deep feature descriptors suitable for MAD. The descriptors that fall into this category are: VGG, AlexNet, OpenFace and FaceNet,
5. **Distance based Descriptors**: This deals with detecting the landmarks on both the bona fide and morphed image. And the distance of the relative position of the landmark between the bona-fide and morphed images is computed, resulting in a feature vector. The calculated feature vectors are referred to as the distance features. Hence this Distance based technique are used for differential image-based scenario.
6. **Gradient Descriptors**: Image gradient is a change of direction in the color or intensity of the image. These descriptors are used because the morphing process reduces the changes in high frequency of the image and thus decreases the gradient steepness which enhances MAD. The descriptors that fall into this category are: HOG, Canny and Sobel edge detectors.

7 Open Issues and Future Directions

Just like every other field MAD as a research field is not left without existing issue and challenges. The most significant issues and challenges are described follows:

1. ***Lack of robust publicly available database***: it is was found that in most research work for MAD, researchers had to create/generate morphed images using morphing software as there are no extensive publicly accessible databases of morphed and bona fide database and some of the initially available databases does not exist anymore. Researches have been conducted on different in-house databases. This prevents creation of useful and robust comparative benchmarks

for existing MAD algorithms. Thus this can be a great limitation to researchers in creating a standardized and reliable MAD.

2. ***Lack of publicly available MAD algorithm***: another issue faced in MAD is lack of publicly available MAD algorithm which can be used by researchers for comprehensive experimental evaluation of new and existing MAD algorithms. This situation brings about questions such as how reliable are the current state-of-the-art MAD algorithms.
3. ***Diversity of experimental database***: most research works train and test proposed MAD algorithms on a single database generated by a single morphing software. But in reality image morphing is carried out with various morphing software which can give different effect and characteristics. This has made current MAD algorithms not to be robust or effective in detecting morph images created with various morph software.
4. ***Image post-processing***: it has been identified that post-processing of morphed images can alter it features. With this alteration it is become impossible for the current MAD algorithms to detect morphed images successfully. Image post-processing task such as image sharpening and image compression has been ignored in most works. Hence it is important to consider different or possible image post-processing task that can be performed on a morphed image in order to improve performance of MAD algorithms.

In summary a SLR which is a formal way of synthesizing the information existing from existing primary studies significant to the research questions on MAD [92]. From this SLR review issues and challenges in MAD was identified.

8 Conclusion

This systematic literature review (SLR) provides researchers and industry practitioners with a current synthesis of feature extraction techniques in face morphing attack detection, approaches of MAD and the performance metric to assess the performance of the MAD systems. This research revealed that texture descriptors, key point extractors, Gradient descriptors, image degradation descriptors, deep learning based methods and Distance-based descriptors can be used as feature descriptors in MAD.

This study illustrates that MAD is an active research area especially differential image based approach of MAD. The differential image-based approach has be adopted by only two literatures which got low detection accuracy thus making the system not suited for operational deployment. Hence it is recommended that more research should be done on differential image-based approach in order to enhance performance. Also this SLR is useful to the scholarly community in understanding of researches regarding to face morphing attack detection and to gain insight of the gaps that remain in the literature.

Appendix A

Primary Study in Review

See Table 9.

Table 9 Primary studies in review

#	Authors	Topic	Approaches To MAD	Feature extraction techniques	Performance metric
P1	Ferrara [38]	"Face morphing detection in the presence of printing/scanning and heterogeneous image sources"	Print-scan attack	CNN (VGG, AlexNet)	D-EER, BPCER and APCER
P2	Scherhag [97]	"Detection of morphed faces from single images: a multi-algorithm fusion approach"	Digital attack	LBF, BSIF, SIFT, HOG and CNN	D-EER, BPCER and APCER
P3	Venkatesh [98]	"Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network"	Digital attack	CNN (AlexNet)	D-EER, BPCER and APCER
P4	Scherhag [99]	"Detecting morphed face images using facial landmarks"	Differential image-based	Distance based	D-EER, BPCER and APCER
P5	Spreeuwers [100]	"Towards robust evaluation of face morphing detection"	Digital attack	LBP	D-EER, BPCER and APCER
P6	Damer [8]	"Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts"	Differential image-based	Regressing local binary features (LBF)	D-EER, BPCER and APCER

(continued)

Table 9 (continued)

#	Authors	Topic	Approaches To MAD	Feature extraction techniques	Performance metric
P7	Damer [101]	"A multi-detector solution towards an accurate and generalized detection of face morphing attacks"	Digital attack	CNN (Openface)	BPCER and APCER
P8	Damer [102]	"On the generalization of detecting face morphing attacks as anomalies: novelty versus outlier detection"	Digital attack	Local Phase Quantization (LPQ) and CNN	D-EER, BPCER and APCER
P9	Debiasi [51]	"PRNU-based detection of morphed face images"	Digital attack	PRNU	D-EER, BPCER and APCER
P10	Scherhag [103]	"Detection of face morphing attacks based on prnu analysis"	Digital attack & print-scan attack	PRNU	D-EER
P11	Wandzik [23]	"Morphing detection using a general-purpose face recognition system"	Digital attack	CNN (AlexNet)	ACC, FAR and FRR
P12	Singh [22]	"Robust morph-detection at automated border control gate using deep decomposed 3D shape & diffuse reflectance"	Print-scan attack	CNN (pre-trained AlexNet)	D-EER, BPCER and APCER
P13	Venkatesh [104]	"Morphed face detection based on deep color residual"	Digital attack	Pyramid local binary pattern (P-LBP)	D-EER, BPCER and APCER
P14	Ramachandra [4]	"Detecting face morphing attacks with collaborative representation of steerable features"	Print-scan attack	Steerable pyramid	BPCER and APCER

(continued)

Table 9 (continued)

#	Authors	Topic	Approaches To MAD	Feature extraction techniques	Performance metric
P15	Jassim [1]	"Automatic detection of image morphing by topology-based analysis"	Print-scan attack	LBP	ACC
P16	Seibold [21]	"Detection of face morphing attacks by deep learning"	Digital attack	CNN (Pre-trained AlexNet)	FAR and FRR
P17	Scherhag [105]	"Deep face representations for differential morphing attack detection"	Print-scan	CNN (FaceNet)	D-EER, BPCER and APCER
P18	Raghavendra [20]	"Detecting Morphed Face Images"	Digital attack	BSIF	FAR and FRR
P19	Makrushin [62]	"Automatic generation and detection of visually faultless facial morphs"	Digital attack	Benford features	FAR and FRR
P20	Damer [106]	"To detect or not to detect: the right faces to morph"	Digital attack & differential image-based	LBP histogram & CNN	BPCER and APCER
P21	Damer [107]	"MorGAN: recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network"	digital attack	LBP histogram & CNN	BPCER and APCER
P22	Scherhag [18]	"Towards detection of morphed face images in electronic travel documents"	Digital attack & differential image-based	LBP, BSIF, SIFT, SURF, HOG, Deep neural network (OpenFace)	D-EER, BPCER and APCER
P23	Scherhag [25]	"Performance variation of morphed face image detection algorithms across different datasets"	Digital attack	LBP, BSIF, SIFT, SURF, HOG	D-EER, BPCER and APCER

(continued)

Table 9 (continued)

#	Authors	Topic	Approaches To MAD	Feature extraction techniques	Performance metric
P24	Kraetzer [108]	"Modeling attacks on photo-ID documents and applying media forensics for the detection of facial morphing"	Digital attack	SIFT, SURF, ORB, FAST, AGAST, sobel & canny edge detector	FAR and FRR
P25	Ortega-Delcampo [48]	"Border control morphing attack detection with a convolutional neural network de-morphing approach"	Digital attack & print-scan attack	CNN (Autoencoder)	D-EER, BPCER and APCER
P26	Neubert [109]	"Face morphing detection: an approach based on image degradation analysis"	Digital attack	FAST, AGAST, shiTomasi	ACC
P27	Scherhag [97]	"Morph detection from single face image: a multi-algorithm fusion approach"	Digital attack	LBP, BSIF, SIFT, SURF, HOG, deep neural network (OpenFace)	D-EER, BPCER and APCER
P28	Ramachandra [89]	"Towards making morphing attack detection robust using hybrid scale-space colour texture features"	Print-scan attack	Laplacian pyramid & LBP	D-EER, BPCER and APCER
P29	Neubert [79]	"A face morphing detection concept with a frequency and a spatial domain feature space for images on eMRTD"	Digital attack	ORB, Discrete fourier transformation (DFT), SURF, SIFT, AGAST, Sobel & Canny, FAST,	FAR and FRR
P30	Debiasi [52]	"PRNU variance analysis for morphed face image detection"	Digital attack	PRNU	D-EER, BPCER and APCER
P31	Zhang [78]	"Face morphing detection using fourier spectrum of sensor pattern noise"	Digital attack	Discrete fourier transformation (DFT)	BPCER and APCER

(continued)

Table 9 (continued)

#	Authors	Topic	Approaches To MAD	Feature extraction techniques	Performance metric
P32	Makrushin [63]	"Generalized Benford's Law for blind detection of morphed face images"	Digital attack	Benford features	FPR and TPR
P33	Raghavendra [110]	"Transferable deep-CNN features for detecting digital and print-scanned morphed face images"	Digital & print-scan attack	CNN (AlexNet and VGG19)	D-EER, BPCER and APCER

References

1. Jassim S, Asaad A (2018) Automatic detection of image morphing by topology-based analysis. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1007–1011. https://doi.org/10.23919/EUSIPCO.2018.8553317
2. Wandzik L, Garcia RV, Kaeding G, Chen X (2017) CNNs under attack: on the vulnerability of deep neural networks based face recognition to image morphing. In: Kraetzer C, Shi Y-Q, Dittmann J, Kim HJ (eds) Digital forensics and watermarking, vol 10431. Springer International Publishing, Cham, pp 121–135. https://doi.org/10.1007/978-3-319-64185-0_10
3. Olanrewaju L, Oyebiyi O, Misra S, Maskeliunas R, Damasevicius R (2020) Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose–Chaudhuri–Hocquenghem error-correcting codes. Signal Image Video Process 14(5):847–855. https://doi.org/10.1007/s11760-019-01609-y
4. Ramachandra R, Venkatesh S, Raja K, Busch C (2020) Detecting face morphing attacks with collaborative representation of steerable features. In: Chaudhuri BB, Nakagawa M, Khanna P, Kumar S (eds) Proceedings of 3rd international conference on computer vision and image processing, vol 1022. Springer, Singapore, pp 255–265. https://doi.org/10.1007/978-981-32-9088-4_22
5. Wu J (2011) Face recognition jammer using image morphing. Boston University, Saint Mary's Street, Boston, ECE-2011-03
6. Rathgeb C, Dantcheva A, Busch C (2019) Impact and detection of facial beautification in face recognition: an overview. IEEE Access 7:152667–152678. https://doi.org/10.1109/ACCESS.2019.2948526
7. Kenneth OM, Bashir SA, Abisoye OA, Mohammed AD (2021) Face morphing attack detection in the presence of post-processed image sources using neighborhood component analysis and decision tree classifier. In: Misra S, Muhammad-Bello B (eds) Information and communication technology and applications, vol 1350. Springer International Publishing, Cham, pp 340–354. https://doi.org/10.1007/978-3-030-69143-1_27
8. Damer N et al (2019) Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In: Brox T, Bruhn A, Fritz M (eds) Pattern recognition, vol 11269. Springer International Publishing, Cham, pp 518–534. https://doi.org/10.1007/978-3-030-12939-2_36

9. Tolosana R, Gomez-Barrero M, Busch C, Ortega-Garcia J (2020) Biometric presentation attack detection: beyond the visible spectrum. IEEE Trans Inf Forensics Secur 15:1261–1275. https://doi.org/10.1109/TIFS.2019.2934867
10. Ferrara M, Franco A, Maltoni D (2016) On the effects of image alterations on face recognition accuracy. In: Bourlai T (ed) Face recognition across the imaging spectrum. Springer International Publishing, Cham, pp 195–222. https://doi.org/10.1007/978-3-319-28501-6_9
11. Mohammadi A, Bhattacharjee S, Marcel S (2018) Deeply vulnerable: a study of the robustness of face recognition to presentation attacks. IET Biom 7(1):15–26. https://doi.org/10.1049/iet-bmt.2017.0079
12. Jayashalini R, Priyadharshini S (2017) Face anti-spoofing using robust features and fisher vector encoding based innovative real time security system for automobile applications. Inf Commun Technol 11
13. Seibold C, Hilsmann A, Eisert P (2018) Reflection analysis for face morphing attack detection. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1022–1026. https://doi.org/10.23919/EUSIPCO.2018.8553116
14. Zanella V, Fuentes O (2004) An approach to automatic morphing of face images in frontal view. In: Monroy R, Arroyo-Figueroa G, Sucar LE, Sossa H (eds) MICAI 2004: advances in artificial intelligence, vol 2972. Springer, Berlin, Heidelberg, pp 679–687. https://doi.org/10.1007/978-3-540-24694-7_70
15. Robertson DJ, Kramer RSS, Burton AM (2017) Fraudulent ID using face morphs: experiments on human and automatic recognition. PLOS ONE 12(3):e0173319. https://doi.org/10.1371/journal.pone.0173319
16. Seibold C, Samek W, Hilsmann A, Eisert P (2021) Accurate and robust neural networks for security related applications exampled by face morphing attacks
17. Robertson DJ, Mungall A, Watson DG, Wade KA, Nightingale SJ, Butler S (2018) Detecting morphed passport photos: a training and individual differences approach. Cogn Res Princ Implic 3(1):27. https://doi.org/10.1186/s41235-018-0113-8
18. Scherhag U, Rathgeb C, Busch C (2018) Towards detection of morphed face images in electronic travel documents. In: 2018 13th IAPR international workshop on document analysis systems (DAS), Vienna, pp 187–192. https://doi.org/10.1109/DAS.2018.11
19. Ferrara M, Franco A, Maltoni D (2014) The magic passport. In: IEEE international joint conference on biometrics, Clearwater, FL, USA, pp 1–7. https://doi.org/10.1109/BTAS.2014.6996240
20. Raghavendra R, Raja KB, Busch C (2016) Detecting morphed face images. In: 2016 IEEE 8th international conference on biometrics theory, applications and systems (BTAS), Niagara Falls, NY, USA, pp 1–7. https://doi.org/10.1109/BTAS.2016.7791169
21. Seibold C, Samek W, Hilsmann A, Eisert P (2017) Detection of face morphing attacks by deep learning. In: Kraetzer C, Shi Y-Q, Dittmann J, Kim HJ (eds) Digital forensics and watermarking, vol 10431. Springer International Publishing, Cham, pp 107–120. https://doi.org/10.1007/978-3-319-64185-0_9
22. Singh JM, Ramachandra R, Raja KB, Busch C (2021) Robust morph-detection at automated border control gate using deep decomposed 3D shape and diffuse reflectance. http://arxiv.org/abs/1912.01372
23. Wandzik L, Kaeding G, Garcia RV (2018) Morphing detection using a general- purpose face recognition system. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1012–1016. https://doi.org/10.23919/EUSIPCO.2018.8553375
24. Korshunov P, Marcel S (2018) Vulnerability of face recognition to deep morphing. In: International conference on biomedical, p 5
25. Scherhag U, Rathgeb C, Busch C (2018) Performance variation of morphed face image detection algorithms across different datasets. In: 2018 international workshop on biometrics and forensics (IWBF), Sassari, pp 1–6. https://doi.org/10.1109/IWBF.2018.8401562
26. Kramer RSS, Mireku MO, Flack TR, Ritchie KL (2019) Face morphing attacks: investigating detection with humans and computers. Cogn Res Princ Implic 4(1):28. https://doi.org/10.1186/s41235-019-0181-4

27. Makrushin A, Wolf A (2018) An overview of recent advances in assessing and mitigating the face morphing attack. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1017–1021. https://doi.org/10.23919/EUSIPCO.2018.8553599
28. Scherhag U, Rathgeb C, Merkle J, Breithaupt R, Busch C (2019) Face recognition systems under morphing attacks: a survey. IEEE Access 7:23012–23026. https://doi.org/10.1109/ACCESS.2019.2899367
29. Swartz MK (2011) The PRISMA statement: a guideline for systematic reviews and meta-analyses. J Pediatr Health Care 25(1):1–2. https://doi.org/10.1016/j.pedhc.2010.09.006
30. Torres-Carrion PV, Gonzalez-Gonzalez CS, Aciar S, Rodriguez-Morales G (2018) Methodology for systematic literature review applied to engineering and education. In: 2018 IEEE global engineering education conference (EDUCON), Tenerife, pp 1364–1373. https://doi.org/10.1109/EDUCON.2018.8363388
31. Misra S (2021) A step by step guide for choosing project topics and writing research papers in ICT related disciplines. In: Misra S, Muhammad-Bello B (eds) Information and communication technology and applications, vol 1350. Springer International Publishing, Cham, pp 727–744. https://doi.org/10.1007/978-3-030-69143-1_55
32. Hordri NF, Yuhaniz SS, Shamsuddin SM (2017) A systematic literature review on features of deep learning in big data analytics. Int J Adv Soft Comput Appl 9(1):33–49
33. Dang DD, Pekkola S (2017) Systematic literature review on enterprise architecture in the public sector, vol 15, no 2, p 25
34. Yannascoli SM, Schenker ML, Carey JL, Ahn J, Baldwin KD (2013) How to write a systematic review: a step-by-step guide, vol 23, p 6
35. Okoli C (2015) A guide to conducting a standalone systematic literature review. Commun Assoc Inf Syst 37. https://doi.org/10.17705/1CAIS.03743
36. Lin EOW, Pan F, Moscheni F (2003) A no-reference quality metric for measuring image Blur. In: Seventh international symposium on signal processing and its applications, vol 1. IEEE, p 4
37. Wang Z, Sheikh HR, Bovik AC (2002) No-reference perceptual quality assessment of JPEG compressed images. In: Proceedings. International conference on image processing, rochester, vol 1, NY, USA, pp I-477–I-480. https://doi.org/10.1109/ICIP.2002.1038064
38. Ferrara M, Franco A, Maltoni D (2019) Face morphing detection in the presence of printing/scanning and heterogeneous image sources. IET Biom 10(3):290–303. https://doi.org/10.1049/bme2.12021
39. Witlox K (2019) Face unmorphing. In: 31th Twenty student conference on IT, Netherlands, pp 1–7
40. Simoncelli EP, Freeman WT (1995) The steerable pyramid: a flexible architecture for multi-scale derivative computation. In: Proceedings, international conference on image processing, vol 3, Washington, DC, USA, pp 444–447. https://doi.org/10.1109/ICIP.1995.537667
41. Ehsaeyan E (2016) An improvement of steerable pyramid denoising method. Electron Eng 12(1):7
42. Kannala J, Rahtu E (2012) BSIF: binarized statistical image features. In: 21st international conference on pattern recognition, vol 1, Tsukuba, Japan, pp 1363–1366
43. Huang D, Shan C, Ardabilian M, Wang Y, Chen L (2011) Local binary patterns and its application to facial image analysis: a survey. IEEE Trans Syst Man Cybern Part C Appl Rev 41(6):765–781. https://doi.org/10.1109/TSMCC.2011.2118750
44. Song K-C, Yan Y-H, Chen W-H, Zhang X (2013) Research and perspective on local binary pattern. Acta Autom Sin 39(6):730–744. https://doi.org/10.1016/S1874-1029(13)60051-8
45. Liu Z, Luo P, Wang X, Tang X (2015) Deep learning face attributes in the wild. In: 2015 IEEE international conference on computer vision (ICCV), Santiago, Chile, pp 3730–3738. https://doi.org/10.1109/ICCV.2015.425
46. Winiarti S, Prahara AM, Pramudi D (2018) Pre-trained convolutional neural network for classification of tanning leather image. Int J Adv Comput Sci Appl 9(1). https://doi.org/10.14569/IJACSA.2018.090129

47. Korshunova I, Shi W, Dambre J, Theis L (2017) Fast face-swap using convolutional neural networks. http://arxiv.org/abs/1611.09577
48. Ortega-Delcampo D, Conde C, Palacios-Alonso D, Cabello, E (2020) Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access 1–1. https://doi.org/10.1109/ACCESS.2020.2994112
49. Schroff F, Kalenichenko D, Philbin J (2015) FaceNet: a unified embedding for face recognition and clustering. In: 2015 IEEE conference on computer vision and pattern recognition (CVPR), pp 815–823. https://doi.org/10.1109/CVPR.2015.7298682
50. Surasak T, Takahiro I, Cheng C, Wang C, Sheng P (2018) Histogram of oriented gradients for human detection in video. In: 2018 5th international conference on business and industrial research (ICBIR), Bangkok, pp 172–176. https://doi.org/10.1109/ICBIR.2018.8391187
51. Debiasi L, Scherhag U, Rathgeb C, Uhl A, Busch C (2018) PRNU-based detection of morphed face images. In: 2018 international workshop on biometrics and forensics (IWBF), Sassari, pp 1–7. https://doi.org/10.1109/IWBF.2018.8401555
52. Debiasi L, Rathgeb C, Scherhag U, Uhl A, Busch C (2018) PRNU variance analysis for morphed face image detection. In: 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS), Redondo Beach, CA, USA, pp 1–9. https://doi.org/10.1109/BTAS.2018.8698576
53. Bonettini N et al (2018) Fooling PRNU-based detectors through convolutional neural networks. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 957–961. https://doi.org/10.23919/EUSIPCO.2018.8553596
54. Chierchia G, Parrilli S, Poggi G, Verdoliva L, Sansone C (2011) PRNU-based detection of small-size image forgeries. In: 2011 17th international conference on digital signal processing (DSP), Corfu, Greece, pp 1–6. https://doi.org/10.1109/ICDSP.2011.6004957
55. Chierchia G, Cozzolino D, Poggi G, Sansone C, Verdoliva L (2014) Guided filtering for PRNU-based localization of small-size image forgeries. In: 2014 IEEE international conference on acoustics, speech and signal processing (ICASSP), Florence, Italy, pp 6231–6235. https://doi.org/10.1109/ICASSP.2014.6854802
56. Verma SB, Sravanan C (2016) Analysis of SIFT and SURF feature extraction in palmprint verification system. In: IEEE international conference on computing, communication and control technology
57. Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110. https://doi.org/10.1023/B:VISI.0000029664.99615.94
58. Lowe DG (1999) Object recognition from local scale-invariant features. In: Proceedings of the seventh IEEE international conference on computer vision, vol 2, Kerkyra, Greece, pp 1150–1157. https://doi.org/10.1109/ICCV.1999.790410
59. Ren S, Cao X, Wei Y, Sun J (2014) Face alignment at 3000 FPS via regressing local binary features. In: 2014 IEEE conference on computer vision and pattern recognition, Columbus, OH, USA, pp 1685–1692. https://doi.org/10.1109/CVPR.2014.218
60. King DE (2009) Dlib-ml: a machine learning toolkit. J Mach Learn Res 10:1755–1758
61. Ojansivu V, Heikkilä J (2008) Blur insensitive texture classification using local phase quantization. In: Elmoataz A, Lezoray O, Nouboud F, Mammass D (eds) Image and signal processing, vol 5099. Springer, Berlin, Heidelberg, pp 236–243. https://doi.org/10.1007/978-3-540-69905-7_27
62. Makrushin A, Neubert T, Dittmann J (2017) Automatic generation and detection of visually faultless facial morphs. In: Proceedings of the 12th international joint conference on computer vision, imaging and computer graphics theory and applications, Porto, Portugal, pp 39–50. https://doi.org/10.5220/0006131100390050
63. Makrushin A, Kraetzer C, Neubert T, Dittmann J (2018) Generalized Benford's Law for blind detection of morphed face images. In: Proceedings of the 6th ACM workshop on information hiding and multimedia security, Innsbruck Austria, pp 49–54. https://doi.org/10.1145/3206004.3206018
64. Fu D, Shi YQ, Su W (2007) A generalized Benford's law for JPEG coefficients and its applications in image forensics. San Jose, CA, United States, p 65051L. https://doi.org/10.1117/12.704723

65. Zhang H, Wohlfeil J, Grießbach D (2016) Extension and evaluation of the AGAST feature detector. In: ISPRS annals of the photogrammetry, remote sensing and spatial information sciences, vol III–4, pp 133–137. https://doi.org/10.5194/isprsannals-III-4-133-2016
66. Kulkarni AV, Jagtap JS, Harpale VK (2013) Object recognition with ORB and its implementation on FPGA. Int J Adv Comput Res 3(3):6
67. Karami E., Prasad S, Shehata M (2015) Image matching using SIFT, SURF, BRIEF and ORB: performance comparison for distorted images. In: 2015 newfoundland electrical and computer engineering, Canada, p 5
68. Hutchison D et al (2010) Adaptive and generic corner detection based on the accelerated segment test. In: Daniilidis K, Maragos P, Paragios N (eds) Computer vision—ECCV 2010, vol 6312. Springer, Berlin, Heidelberg, pp 183–196. https://doi.org/10.1007/978-3-642-15552-9_14
69. Biadgie Y, Sohn K-A (2014) Feature detector using adaptive accelerated segment test. In: 2014 international conference on information science & applications (ICISA), Seoul, South Korea, pp 1–4. https://doi.org/10.1109/ICISA.2014.6847403
70. Cooke T, Whatmough R (2005) Detection and tracking of corner points for structure from motion. In: Defence science and technology organisation, Australia, Technical DSTO-TR-1759
71. Juranek L, Stastny J, Skorpil V (2018) Effect of low-pass filters as a shi-tomasi corner detector's window functions. In: 2018 41st international conference on telecommunications and signal processing (TSP), Athens, pp 1–5. https://doi.org/10.1109/TSP.2018.8441178
72. Urban S, Weinmann M (2015) Finding a good feature detector-descriptor combination for the 2d keypoint-based registration of TlS point clouds. In: ISPRS annals of the photogrammetry, remote sensing and spatial information sciences, vol. II-3/W5, pp 121–128. https://doi.org/10.5194/isprsannals-II-3-W5-121-2015
73. Rublee E, Rabaud V, Konolige K, Bradski G (2011) ORB: an efficient alternative to SIFT or SURF. In: 2011 international conference on computer vision, Barcelona, Spain, pp 2564–2571. https://doi.org/10.1109/ICCV.2011.6126544
74. Tchagang AB, Valdes JJ (2019) Discrete fourier transform improves the prediction of the electronic properties of molecules in quantum machine learning. In: 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), Edmonton, AB, Canada, pp 1–4. https://doi.org/10.1109/CCECE.2019.8861895
75. Mironovova M, Bíla J (2015) Fast fourier transform for feature extraction and neural network for classification of electrocardiogram signals. In: 2015 fourth international conference on future generation communication technology (FGCT), Luton, United Kingdom, pp 1–6. https://doi.org/10.1109/FGCT.2015.7300244
76. Luka J, Fridrich J, Goljan M (2006) Digital camera identification from sensor pattern noise. IEEE Trans Inf Forensics Secur 1(2):205–214. https://doi.org/10.1109/TIFS.2006.873602
77. Liu B, Wei X, Yan J (2015) Enhancing sensor pattern noise for source camera identification: an empirical evaluation. In: Proceedings of the 3rd ACM workshop on information hiding and multimedia security, Portland Oregon USA, pp 85–90. https://doi.org/10.1145/2756601.2756614
78. Zhang L-B, Peng F, Long M (2018) Face morphing detection using fourier spectrum of sensor pattern noise. In: 2018 IEEE international conference on multimedia and expo (ICME), San Diego, CA, pp 1–6. https://doi.org/10.1109/ICME.2018.8486607
79. Neubert T, Kraetzer C, Dittmann J (2019) A face morphing detection concept with a frequency and a spatial domain feature space for images on eMRTD. In: Proceedings of the ACM workshop on information hiding and multimedia security, Paris, France, pp 95–100. https://doi.org/10.1145/3335203.3335721
80. Zhu Z, Zhang G, Li H (2018) SURF feature extraction algorithm based on visual saliency improvement, vol 5, no 3, p 5
81. Anjana MV, Sandhya L (2017) Implementation and comparison of feature detection methods in image mosaicing. IOSR J Electron Commun Eng 2(3):7–11

82. Bhosale SB, Kayastha VS, Harpale (2014) Feature extraction using surf algorithm for object recognition. Int J Tech Res Appl 2(4):3
83. Oyallon E, Rabin J (2015) An analysis of the SURF method. Image Process Line 5:176–218. https://doi.org/10.5201/ipol.2015.69
84. Asmaidi A, Putra DS, Risky MM, FUR (2019) Implementation of sobel method based edge detection for flower image segmentation. SinkrOn 3(2):161. https://doi.org/10.33395/sinkron.v3i2.10050
85. Gao W, Zhang X, Yang L, Liu H (2010) An improved Sobel edge detection. In: 2010 3rd international conference on computer science and information technology, Chengdu, China, pp 67–71. https://doi.org/10.1109/ICCSIT.2010.5563693
86. Sumeyya I, Fatma SH, Merve T, Suhap S (2017) The enhancement of canny edge detection algorithm using Prewitt, Robert, Sobel Kernels. In: Conference: international conference on engineering technologies, Turkey
87. Vincent O, Folorunso O (2009) A descriptive algorithm for Sobel image edge detection. In: SITE 2009: informing science + IT education conference. https://doi.org/10.28945/3351
88. Canny J (1986) A computational approach to edge detection. IEEE Trans Pattern Anal Mach Intell 8(6):679–698. https://doi.org/10.1109/TPAMI.1986.4767851
89. Ramachandra R, Venkatesh S, Raja K, Busch C (2019) Towards making morphing attack detection robust using hybrid scale-space colour texture features. In: 2019 IEEE 5th international conference on identity, security, and behavior analysis (ISBA), Hyderabad, India, pp 1–8. https://doi.org/10.1109/ISBA.2019.8778488
90. El-Abed M, Charrier C, Rosenberger C (2012) Evaluation of biometric systems. In: Yang J (ed) New trends and developments in biometrics, InTech. https://doi.org/10.5772/52084
91. Mansfield AJ (200) Best practices in testing and reporting performance of biometric devices. National Physical Laboratory, USA, Technical NPL Report CMSC
92. Vaidya AG, Dhawale AC, Misra A (2016) Comparative analysis of multimodal biometrics. Int J Pharm Technol 8(4):22969–22981
93. Sokolova M, Lapalme G (2009) A systematic analysis of performance measures for classification tasks. Inf Process Manag 45(4):427–437. https://doi.org/10.1016/j.ipm.2009.03.002
94. Flach P (2019) Performance evaluation in machine learning: the good, the bad, the ugly, and the way forward. In: Proceedings of the AAAI conference on artificial intelligence, vol 33, pp 9808–9814. https://doi.org/10.1609/aaai.v33i01.33019808
95. Olaleye T, Arogundade O, Adenusi C, Misra S, Bello A (2021) Evaluation of image filtering parameters for plant biometrics improvement using machine learning. In: Patel KK, Garg D, Patel A, Lingras P (eds) Soft computing and its engineering applications, vol 1374. Springer, Singapore, pp 301–315. https://doi.org/10.1007/978-981-16-0708-0_25
96. Sharma D, Yadav UB, Sharma P (2009) The concept of sensitivity and specificity in relation to two types of errors and its application in medical research, vol 2, p 7
97. Scherhag U, Rathgeb C, Busch C (2018) Detection of morphed faces from single images: a multi-algorithm fusion approach, p 7
98. Venkatesh S, Ramachandra R, Raja K, Spreeuwers L, Veldhuis R, Busch C (2020) Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network. In: 2020 IEEE winter conference on applications of computer vision, pp 269–278. https://doi.org/10.1109/WACV45572.2020.9093488
99. Scherhag U, Budhrani D, Gomez-Barrero M, Busch C (2018) Detecting morphed face images using facial landmarks. In: Mansouri A, El Moataz A, Nouboud F, Mammass D (eds) Image and signal processing, vol 10884. Springer International Publishing, Cham, pp 444–452. https://doi.org/10.1007/978-3-319-94211-7_48
100. Spreeuwers L, Schils M, Veldhuis R (2018) Towards robust evaluation of face morphing detection. In: 2018 26th European signal processing conference (EUSIPCO), Rome, pp 1027–1031. https://doi.org/10.23919/EUSIPCO.2018.8553018
101. Damer N, Zienert S, Wainakh Y, Saladie AM, Kirchbuchner F, Kuijper A (2019) A multi-detector solution towards an accurate and generalized detection of face morphing attacks. In: 2019 22th International conference on Information Fusion, pp 1–8

102. Damer N, Grebe JH, Zienert S, Kirchbuchner F, Kuijper A (2019) On the generalization of detecting face morphing attacks as anomalies: novelty versus outlier detection. In: 2019 IEEE 10th international conference on biometrics theory, applications and systems (BTAS), Tampa, FL, USA, pp 1–5. https://doi.org/10.1109/BTAS46853.2019.9185995
103. Scherhag U, Debiasi L, Rathgeb C, Busch C, Uhl A (2019) Detection of face morphing attacks based on PRNU analysis. IEEE Trans Biom Behav Identity Sci 1(4):302–317. https://doi.org/10.1109/TBIOM.2019.2942395
104. Venkatesh S, Ramachandra R, Raja K, Spreeuwers L, Veldhuis R, Busch C (2019) Morphed face detection based on deep color residual noise. In: 2019 ninth international conference on image processing theory, tools and applications (IPTA), Istanbul, Turkey, pp 1–6. https://doi.org/10.1109/IPTA.2019.8936088
105. Scherhag U, Rathgeb C, Merkle J, Busch C (2020) Deep face representations for differential morphing attack detection. http://arxiv.org/abs/2001.01202
106. Damer N et al (2019) To detect or not to detect: the right faces to morph. In: 2019 international conference on biometrics (ICB), Crete, Greece, pp 1–8. https://doi.org/10.1109/ICB45273.2019.8987316
107. Damer N, Saladie AM, Braun A, Kuijper A (2018) MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In: 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS), Redondo Beach, CA, USA, pp 1–10. https://doi.org/10.1109/BTAS.2018.8698563
108. Kraetzer C, Makrushin A, Neubert T, Hildebrandt M, Dittmann J (2017) Modeling attacks on photo-ID documents and applying media forensics for the detection of facial morphing. In: Proceedings of the 5th ACM workshop on information hiding and multimedia security, Philadelphia Pennsylvania USA, pp 21–32. https://doi.org/10.1145/3082031.3083244
109. Neubert T (2017) Face morphing detection: an approach based on image degradation analysis. In: Kraetzer C, Shi Y-Q, Dittmann J, Kim HJ (eds) Digital forensics and watermarking, vol 10431. Springer International Publishing, Cham, pp 93–106. https://doi.org/10.1007/978-3-319-64185-0_8
110. Raghavendra R, Raja KB, Venkatesh S, Busch C (2017) Transferable deep-CNN features for detecting digital and print-scanned morphed face images. In: 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW), Honolulu, HI, USA, pp 1822–1830. https://doi.org/10.1109/CVPRW.2017.228