RESEARCH ARTICLE OPEN ACCESS

Face Recognition System Under Morphing Attacks

S.Jagadeesan M.Sc(CS)., MCA., M.Phil(CS)., ME(CSE).,*,
Assistant Professor, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: jagadeesan12398@gmail.com
S.Sabitha**
Final MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: sabiselvaraj02@gmail.com

****

ABSTRACT

Recently, researchers found that the intended generalizability of face recognition systems increases their vulnerability against attacks. especially , the attacks supported morphed face images pose a severe security risk to face recognition systems. within the previous couple of years, the subject of (face) image morphing and automatic morphing attack detection has sparked the interest of several research laboratories working within the field of biometrics. during this paper, a conceptual categorization and metrics for an evaluation of such methods are presented, followed by a comprehensive survey of relevant publications. additionally , technical considerations and tradeoffs of the surveyed methods are discussed along side open issues and challenges within the field.

Index Terms — **Biometrics, face morphing attack, face recognition, image morphing, morphing attack detection.**

****

I. INTRODUCTION

Automated face recognition [1], [2] represents a long-standing field of research in which a major break-though has been achieved by the introduction of deep neural networks [3], [4]. Due to the high generalization capabilities of deep neural networks specifically and recognition systems in general, the performance of operational face recognition systems in unconstrained environments, e.g., regarding illumination, poses, image quality or cameras, improved significantly. Resulting performance improvements paved the way for deployments of face recognition technologies in diverse application scenarios, ranging from video-based surveillance and mobile device access control to Automated Border Control (ABC). However, recently researchers found that the generalizability of (deep) face recognition systems increases their vulnerability against attacks, e.g., spoofing attacks (also referred to as presentation attacks) [5]. An additional attack vector enabled by the high generalization capabilities is a specific attack against face recognition systems based on morphed face images, as introduced by Ferrara *et al.* [6].

A. *FACE MORPHING ATTACK*

Image morphing has been an active area of image processing research since the 80s [7], [8] with a wide variety of application scenarios, most notably in the film industry. Morphing techniques are often wont to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and have domain. An example of a morphed face image as the result of two non-morphed, i.e., bona fide [9], face images, is depicted in Fig. 1. The created morphed face image will be successfully verified against probe samples of both contributing subjects by state-of-the- art face recognition systems. This means, if a morphed face image is stored as reference within the

database of a face recognition system, both contributing subjects are often successfully verified against this manipulated reference. Thus, morphed face images pose a severe threat to face recognition systems, as the fundamental principal of biometrics, the unique link between the sample and its corresponding subject is violated.

In many countries, the face image used for the ePassport issuance process is provided by the applicant in either analog or digital form. In a face morphing attack scenario,

(a) Subject 1 (b) Morph (c) Subject 2

FIGURE 1. Example for a morphed face image (b) of subject 1 (a) and subject 2 (c). The Morph was manually created using FantaMorph.

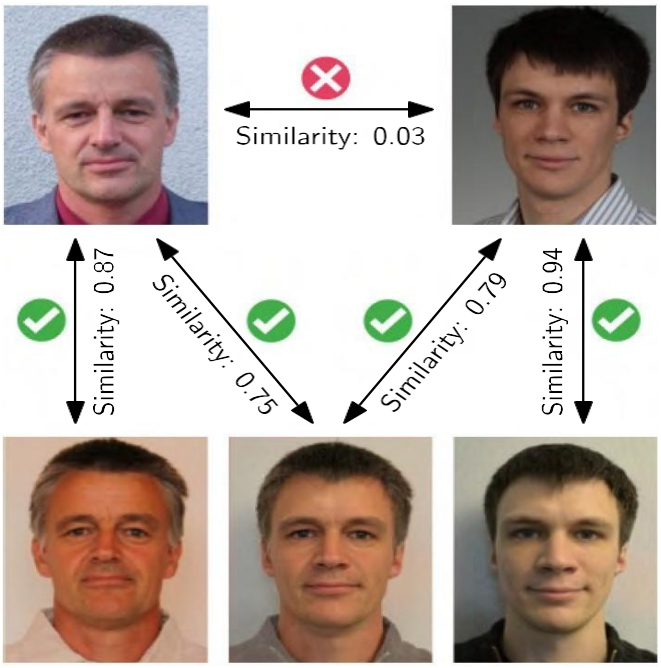

FIGURE 2. Example for the face morphing attack: different instances of face images of both subjects contributing to a face morph are successfully matched against it using a COTS face recognition software with a default decision threshold of 0.5, resulting in an FMR of 0.1%.

a wanted *criminal* could morph his face image with one of a lookalike *accomplice*. If the accomplice applies for an ePassport with the morphed face image, he will receive a valid ePassport equipped with the morphed face image. It is impor tant to note, that morphed face images can be realistic enough to fool human examiners [10], [11]. Both, the criminal and the accomplice could then be successfully verified against the morphed image stored on the ePassport, as visualized in Fig. 2. This means, the criminal can use the ePassport issued to the accomplice to pass ABC gates (or even human inspections at border crossings). The risk posed by this attack, referred to as face morphing attack, is amplified by the fact that realistic morphed face images can be generated by non- experts employing easy-to-use face morphing software which is either freely available or can be purchased at a reasonable price, e.g., FaceMorpher,1 WinMorph2 or FantaMorph.3

B. CONTRIBUTION AND ORGANIZATION

Ferrara et al. [6] were the first to thoroughly investigate the vulnerability of commercial face recognition systems to attacks based on morphed face images. Up to now, a significant amount of literature related to face morphing attacks and their detection has already been published, while only a rather brief overview has been given in [12]. This survey provides a comprehensive overview and critical discussion of published literature related to said topics. This survey primarily addresses biometrics researchers and practitioners. The remainder of this article is organized as follows: the fundamentals of (face) image morphing and quality assessment of face morphs are described in Sect. II and Sect. III, respectively, along with an overview of available software tools in Sect. IV. Subsequently, relevant metrics to assess the vulnerability of face recognition systems against said attack and the performance of morphing attack detection methods are summarized in Sect. V. Proposed approaches for automated morphing attack detection are surveyed and discussed in Sect. VI. Open issues and challenges are outlined in Sect. VII. Finally, a conclusion is given in Sect. VIII.

II. MORPHING OF FACE IMAGES

Image morphing in general represents a well-

investigated field of research, for comprehensive surveys the reader is referred to [7] and [8]. In this section, surveyed approaches are limited to morphing techniques, which have been explicitly applied to (frontal) face images. Face images used to create a morph should meet certain requirements. The best results can be achieved with frontal images exhibiting a neutral facial expression. In the context of the face morphing attack it should be expected that not only for the input face images (provided by the photographer) but also for the resulting morph the prerequisites of the International Civil Aviation Organization (ICAO) [13] for the production of passport portrait photos have to be met. These specifications ensure that all faces are represented equally with respect to resolution, exposure, etc. Semi-profile recordings can indeed be partially corrected, but then there is usually information missing of the far side of the face. Furthermore, the quality of the source images has a direct influence on the result. The quality of the morph cannot be expected to be higher than that of the source images. Distortions and scaling usually negatively affect quality during the process chain. The quality of morphed face images is further discussed in Sect. III.

In general, the morphing process of face images can be divided into three steps. First, a correspondence between the contributing samples is determined. In a second step, called warping, both images are distorted, such that the corresponding elements of both samples are geometrically aligned. Finally, the color values of the warped images are merged, referred to as blending, in order to create the morphed face image. Said processing steps are described in detail in the following subsections, along with post-processing, studies on human perception of morphed face images and a summary of available research resources.

A. CORRESPONDENCE

The most common way of determining correspondences between face images is by determining salient points in both images, so-called landmarks. The simplest way is to manually define the coordinates of prominent characteristics, e.g., eyes, eyebrows, tip of the nose, etc., as for instance done in the morphing process of [6] and [14]. The manual annotation of images is very accurate (if done properly), but time consuming. More convenient is the automated detection of landmarks. The established approach for landmark detection is to detect each point separately, e.g., utilizing geometric features [15]. A more sophisticated solution is to fit a predefined model, e.g., active shape models [16] or elastic bunch graph models [17], [18] to the face image, whereas the fitting of the model is the key issue. Zanella and Fuentes [19] propose an untrained generic model, which is fit to the contours of a binary image using evolutionary strategies. Saragih et al. [20] propose a principled optimization strategy where a non-parametric representation of the landmark distributions is maximized within a hierarchy of smoothed estimates. Further algorithms train multiple regression trees for landmark detection of which the method of Kazemi and Sullivan was further implemented in the widely used dlib landmark detector. For detailed information and benchmarks of different automated landmark detection approaches the reader is referred.

B. WARPING

If the landmarks are determined, the image should be distorted in a manner, that corresponding landmarks are aligned. A straight forward method for morphing is scattered data interpolation. The landmarks, also called control points, are moved to a new position, the new position of all intervening pixels is interpolated based on the nearby control points. More advanced morphing techniques take the correlation between the landmarks into account. For example, Sederberg and Parry propose a grid or mesh-based warping technique called Free-Form Deformation (FFD), which was extended by Lee et al. [to multi-level FFD. The whole image is considered as a grid, which is deformed by the flow of the landmarks. Another approach is field morphing introduced by Beier and Neely, where grid lines are controlling the metamorphosis of the image in the transformation. In particular, for manual morphing this approach has advantages, as the user can position lines instead of points. For

automatic morphing the lines can be derived from detected landmarks. In the work of Schaefer et al. the moving least squares are minimized in order to estimate the optimal affine transformation. This approach can be employed to optimize different warping methods based on landmarks or lines. Choi and Hwang propose a morphing process by simulating the image as a mass spring system. Thus, each translated landmark influences nearby pixels and landmarks.

Most state-of-the-art morphing algorithms, e.g., as used for the morph-creation, do not consider the image as a grid, but apply a Delaunay triangulation on the landmarks in

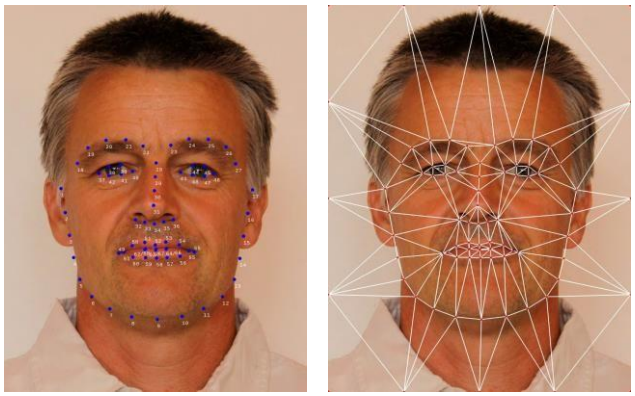

FIGURE 3. Examples of detected landmarks (using dlib landmark detector) and corresponding Delaunay triangles.

order to determine non overlapping triangles, as depicted in Fig. 3. Delaunay triangulations maximize the minimum angle of each triangle in the triangulation and can be calculated efficiently. Subsequently, the triangles of both contributing images are distorted, rotated and shifted until an alignment is achieved.

The first step in traditional approaches for creating a morph between a pair of face images I0 and I1 is to define a map φ from I0 to I1. The contribution of every subject to the warping process is defined by an αw-value, whereas an αw = 0 would be the landmark-position of the primary subject, αw = 1 the landmark-position of the second subject and an αw between 0 and 1 any combination of both. The impact of various αw-values on the resulting face morph are often seen by analyzing the primary versus the last row of Fig. 4. One issue which may occur are disocclusions which refers to regions within the object space that are visible in I0, but disappear in I1 as described by Liao et al. For disocclusions in I0, the map φ is typically undefined, for disocclusions in I1 it is discontinuous. To obtain a more complete representation, one can introduce a second map from I1 back to I0. Maintaining consistency between the two maps during an optimization process becomes quite expensive One approach solving this issue is proposed by Wu and Liu. The images are warped forward and backward in order to obtain a com- plete mapping φ. In addition, to obtain a more natural warping, the face images are projected into a 3D space and an energy function is minimized to avoid ghost and blur artifacts. Seitz and Dyer also propose a projection into 3D-space, so as to think about perspective effects during the morphing process. Another technique for morphing in 3D-space is given by Yang et al. In order to recover the face geometry, the 2D face image is projected on a pre-learned 3D face mask. In particular, for variances in pose and expression this approach promises a higher quality.

Further, some warping algorithms don't need previously detected landmarks. Bichsel proposes to employ the Bayesian framework in order to determine the optimal mapping function.

C. BLENDING

After the alignment of the 2 contributing images, the 2 arranged textures are combined using blending, usually over the whole image region. The most frequent way of blending for face morph creation is linear blending, i.e. all color values at same pixel positions are combined in the same manner. Similar to the warping process the contribution to the blending of each image can be weighted by an αb-value, e.g. αb = 0.5 for averaging. The impact of a changing αb-value to the morphed image are often seen in Fig. 4 on the vertical axis.

D. FURTHER APPROACHES

There are, however, some morphing algorithms, where a sub- division into the steps described above isn't feasible. In a morphing approach is proposed using generative morphing to combine warping and blending. The resulting morphed image is regenerated from small pieces of the source images. Korshunova et al. propose to train a Convolutional Neural Network (CNN) to swap the face image of one subject with the face of a second one. A huge disadvantage of this method is, that a new network has to be trained for each subject.

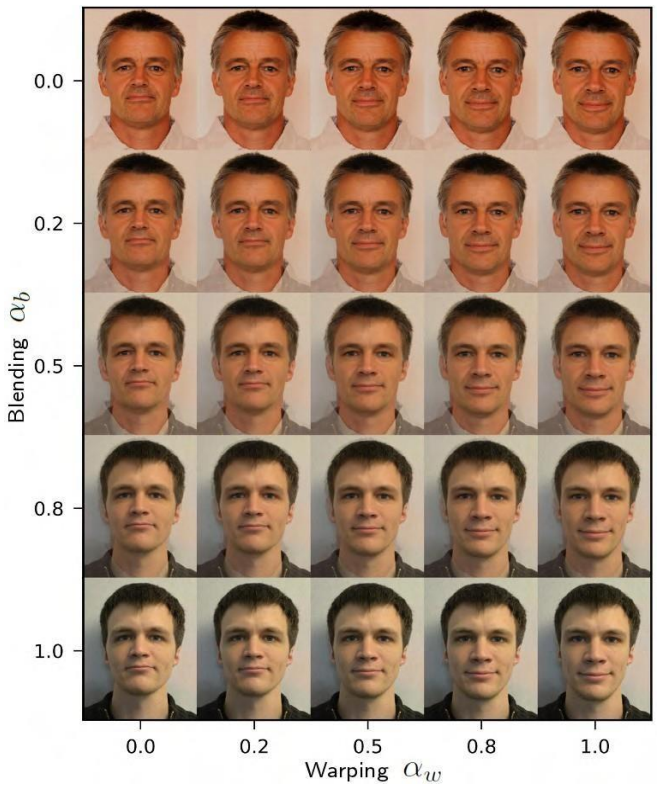

FIGURE 4. Matrix of the two variables in a morphing process (blending and warping). This morph sequence was created using dlib for landmark detection, Delaunay triangulation and linear affine transformation for warping and linear blending.

Beside the morphing of samples in image domain, it is possible to morph in feature domain for minutiae sets for iris-codes. It would be feasible to also morph face representations in feature domain, e.g., by averaging the feature vector of a CNN. In order to use the morphed feature vector during a face recognition system, a face image are often reconstructed from the feature domain. However, it's presumably , that the recon- structed morphed face image only works for an equivalent feature space, meaning an attack against an equivalent face recognition system, as used for creation of the morphed feature vector.

E. POST-PROCESSING

After the creation of the morphed face image, the image could be further processed and altered. In order to obscure the image manipulation, the image quality might be enhanced or reduced on purpose. In particular, the automated creation of morphed face images can cause morphing artifacts. Missing or misplaced landmarks might cause shadow or ghost artifacts, as they will be seen in Fig. 5 (a). This issue can be tackled by swapping the facial area of the morphed face image with an adapted outer area of one of the subjects Artifacts in the hair region are often concealed by an interpolation of the hair region as proposed by Weng et al. Further, unnatural color gradients and edges might occur, thanks to inappropriate interpolation methods, which may be removed by blurring or sharpening. Due to the averaging during the blending process, the histograms of the color values might get narrow. This artifact can be avoided by an adaptation of the color histogram, e.g. by using histogram equalization or an adaption of lumination, in order to achieve realistic histogram shapes. Examples for sharpening and histogram equalization are depicted in Fig. 5 (b) and (c).

In addition to the removal or reduction of morphing artifacts, further post-processing steps might be carried out, which can sometimes be unavoidable, i.e., printing and scanning of the image, in order to use it as a passport photo. Even with high-end photo printer within the processing pipeline, some information contained within the face image signal will always be lost within the process, masking or reducing morphing artifacts, as described. Once the image has been submitted to a passport application office, it has to be scanned again. Again, information are often lost, helping to cover or reduce erroneous artifacts.

Further, information from or trace of the morphing process are often lost when the image

format is modified . By storing the image in a lossy format, high-frequency information is eliminated from the signal permanently. If the image is loaded and stored multiple times as part of the process chain, the accumulated compression error can significantly degrade the image quality.

VI. QUALITY ASSEMENT OF FACE MORPHS

Generally speaking, automatically generated databases of morphed face images are expected to differ in quality from real world attack scenarios.. Automatically generated morphs might reveal artifacts, which can be avoided when the attacker

FIGURE 5. Examples of different post-processing methods likely to beapplied by an attacker to conceal the morphing process. (a) Original morph. (b) Sharpness. (c) Hist. equlization.

is producing only one single high quality morph between himself and his accomplice and manually optimizing the resulting image. When aiming to develop a robust detection algorithm on such an automatically generated database, it is crucial to assure high quality of morphed face images. Otherwise, it is likely that a trained classifier might strongly rely on these specific artifacts.

As described by Scherhag et al. it is difficult to define objective metrics for quality assessment of face morphs thanks to the massive number of contributing factors. Basically, the output image of the algorithms can be evaluated according to the criteria summarized in the following subsections.

A. IMAGE QUALITY

Each processing step affects the standard of a picture . In particular, factors such as image size, sharpness, color saturation, aspect ratio and the overall natural appearance of the face image should be influenced as little as possible by the morphing algorithm. The minimum requirements for these factors can be found in the specifications for passport images of the ICAO [13]. Thus, for example, the minimum resolution of the facial image is set to an inter eye distance of 90 pixels. If a picture deviates from these minimum requirements, it is no longer accepted in countries that comply with ICAO recommendations to produce a passport or other machine readable travel documents (e.g., citizen cards). Furthermore, the image quality may be affected by compression of the image. In the case of lossy compression, the storage of high-frequency information is deliberately omitted in order to increase the compression rate. At high compression rates, however, this can lead to elimination of details and compression artifacts in the image. Since poor image quality usually results from lack of information, for example, too few pixels or too little high-frequency information, it is often difficult to improve the quality later.

Quality metrics for images can be used to objectively evaluate the output images based on quality measures derived from the signal. Since no reference image is available in the evaluation of the output image, the classical image quality determination methods, such as signal-to-noise ratio or mean square deviation, are not feasible. For the choice of the standard metric, the standard properties to be considered need to be determined. The metric proposed by Farias and Mitra

FIGURE 6. Examples of BRISQUE scores for quality estimation (low values indicate high image quality). The BRISQUE score of bona fide (a) and uncompressed morphed images (b) are close to each other, the score of aJPEG compressed morphed image (c) is noticeably higher.

evaluates the occurrence of image artifacts, such as block artifacts, blur or noise. If the authentic appearance of a submitted passport image is to be

evaluated for the human observer, then metrics are recommended that take under consideration the human perception, i.e., factors like sharpness or perceptual of the image. Another option is the automated assess- ment of the naturalness of the image using some no-reference image quality metrics, e.g., Blind / Referenceless Image Spatial Quality Evaluator (BRISQUE). Fig. 6 shows examples of BRISQUE values where low values indicated high quality and vice versa. On the left a non-morphed face image is shown, the associated BRISQUE value of 21 cor- responds to a high quality. The middle image may be a top quality morph without compression, the BRISQUE value is slightly worse. The image on the right shows the same morph with JPEG compression. Even if no artifacts are visible, the BRISQUE value is strongly influenced by the compression.

A. MORPHING ARTIFACTS

Morphing artifacts as illustrated in Fig. 7 (right) can appear in the image during the multi-step morph process. Within landmark-based methods artifacts are usually caused by the absence or misplacement of landmarks. As a result, the corresponding image areas are not transformed correctly so that they do not completely overlap. This creates shadow-like, semi-transparent areas, so-called ghost artifacts. Fig. 7 depicts a manual morphed face image and an automatically generated morph comprising said artifacts. On the right, one can see a morphed facial image with poorly placed landmarks. Especially, in the region of the neck, but also on the hair and ears, strong ghost artifacts can be observed. The iris proved to be particularly susceptible to artifacts because algorithms for automatic landmark determination are usually not able to provide the iris with correct landmarks. As a workaround, the located left and right eye corner could approximate the iris center half way between the two corners. Furthermore, shadow effects may occur in facial hair (e.g., beards and eyelashes), in differently pigmented areas (e.g., liver spots, tattoos), or by glasses and jewelry. Morph artifacts, which are caused by landmark-based morphing, can usually be remedied by manual post-processing in image processing programs as shown by Ferrara et al. [6]. An additional cause of artifacts may be the differences in the source images or inappropriate interpolation methods, which can lead to unnatural color gradients and overly hard edges in the target images. Further artifacts induced by morphing could also be low contrast and blur of the pictures , which can result from the averaging and interpolation of pixel positions and color values. Another type of morph artifact may be generated using machine learning to create the morphed facial images. Due to the opacity of the process of the training algorithms, the errors might be difficult to narrow down or classify. Some of the potential mistakes are missing or deformed countenance , blurred areas and ghost artifacts. The emergence of such artifacts can be reduced by appropriate learning methods and a large number of training data. Due to the high agility of the relevant research area, a rapid improvement in the quality of morph images that can be achieved by the application of machine learning can also be expected.

B. PLAUSIBILITY OF FACE MORPHS

The quality of a morph can also be assessed by how plausible the image appears as a facial image. Here, on the one hand, the natural appearance of the produced image plays a role, and on the other hand, the similarity of the morph with the contributing data subject. The natural appearance can be adversely affected by strong artifacts. In addition, the similarity of the contributing subjects, e.g., with respect to gender, ethnicity or age group, influences the plausibility of the resulting morph. e.g., the morph depicted in Fig.1 appears less plausible since the age gap between the two contributing subjects is more than 20 years. Thus, it's recommended to pick similar subjects as a basis. An approach for an automatic selection of suitable subjects is given.

FIGURE 7. Comparison between a manually created high quality (left) and an automatically created low quality face morph (right).

evaluates the occurrence of image artifacts, such as block artifacts, blur or noise. If the authentic

appearance of a submitted passport image is to be evaluated for the human observer, then metrics are recommended that take under consideration the human perception, i.e., factors like sharpness or perceptual of the image. Another option is the automated assess- ment of the naturalness of the image using some no-reference image quality metrics, e.g., Blind / Referenceless Image Spatial Quality Evaluator (BRISQUE). Fig. 6 shows examples of BRISQUE values where low values indicated high quality and vice versa. On the left a non-morphed face image is shown, the associated BRISQUE value of 21 cor- responds to a high quality. The middle image may be a top quality morph without compression, the BRISQUE value is slightly worse. The image on the right shows the same morph with JPEG compression. Even if no artifacts are visible, the BRISQUE value is strongly influenced by the compression.

C. MORPHING ARTIFACTS

Morphing artifacts as illustrated in Fig. 7 (right) can appear in the image during the multi-step morph process. Within landmark-based methods artifacts are usually caused by the absence or misplacement of landmarks. As a result, the corresponding image areas are not transformed correctly so that they do not completely overlap. This creates shadow-like, semi-transparent areas, so-called ghost artifacts. Fig. 7 depicts a manual morphed face image and an automatically generated morph comprising said artifacts. On the right, one can see a morphed facial image with poorly placed landmarks. Especially, in the region of the neck, but also on the hair and ears, strong ghost artifacts can be observed. The iris proved to be particularly susceptible to artifacts because algorithms for automatic landmark determination are usually not able to provide the iris with correct landmarks. As a workaround, the located left and right eye corner could approximate the iris center half way between the two corners. Furthermore, shadow effects may occur in facial hair (e.g., beards and eyelashes), in differently pigmented areas (e.g., liver spots, tattoos), or by glasses and jewelry. Morph artifacts, which are caused by landmark-based morphing, can usually be remedied by manual post-processing in image processing programs as shown by Ferrara et al. [6]. An additional cause of artifacts may be the differences in the source images or inappropriate interpolation methods, which can lead to unnatural color gradients and overly hard edges in the target images. Further artifacts induced by morphing could also be low contrast and blur of the pictures , which can result from the averaging and interpolation of pixel positions and color values. Another type of morph artifact may be generated using machine learning to create the morphed facial images. Due to the opacity of the process of the training algorithms, the errors might be difficult to narrow down or classify. Some of the potential mistakes are missing or deformed countenance , blurred areas and ghost artifacts. The emergence of such artifacts can be reduced by appropriate learning methods and a large number of training data. Due to the high agility of the relevant research area, a rapid improvement in the quality of morph images that can be achieved by the application of machine learning can also be expected.

D. PLAUSIBILITY OF FACE MORPHS

The quality of a morph can also be assessed by how plausible the image appears as a facial image. Here, on the one hand, the natural appearance of the produced image plays a role, and on the other hand, the similarity of the morph with the contributing data subject. The natural appearance can be adversely affected by strong artifacts. In addition, the similarity of the contributing subjects, e.g., with respect to gender, ethnicity or age group, influences the plausibility of the resulting morph. e.g., the morph depicted in Fig.1 appears less plausible since the age gap between the two contributing subjects is more than 20 years. Thus, it's recommended to pick similar subjects as a basis. An approach for an automatic selection of suitable subjects is given.

III. MORPHING SOFTWARE

Applications were considered for the common desktop operating systems (Windows, Linux, Mac) and mobile operating systems (Android, iOS). Excluded from the list are web services available on the internet. These web services provide an easy way to manually create morphed images. However, firstly, an automated generation of face morphs is difficult and secondly, it is

unclear how the uploaded images are processed and stored, which would make it impossible for researchers to upload face images of their models/volunteers and to comply with privacy regulations at the same point in time.

In order to enable well-founded and efficient experiments, it is generally advisable to use applications that can produce morphs in an automated manner in good quality without manual post-processing. Open source algorithms have the advantage that they can be much better automated and adapted to the needs than commercial applications.

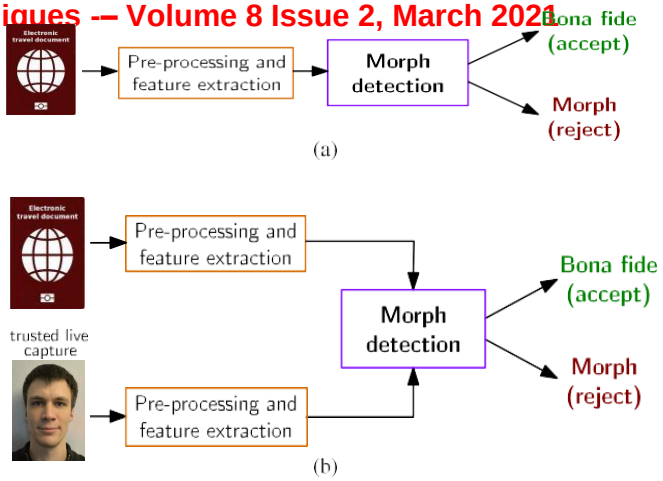

FIGURE 8. Morphing attack detection scenarios. (a) No-reference morphing attack detection. (b) Differential morphing attack detection.

VI. FACE MORPHING ATTACK DETECTION

Proposed approaches can be coarsely categorized with respect to the considered morphing attack detection scenario. The two classes of detection methods, i.e., *no-reference* and *differential*, are described in the following subsection. Subse- quently, the state-of-the-art with respect to morph detection algorithms is surveyed.

DETECTION SCENARIOS

Two automated morph detection scenarios depicted in Fig. 8 can be distinguished:

- *No-reference morphing attack detection*: the detector processes a single image, e.g., an off-line authenticity check of an electronic travel document (this scenario is also referred to as single image morphing attack detection or forensic morphing attack detection);
- *Differential morphing attack detection*: a trusted live capture from an authentication attempt serves as additional source of information for the morph detector, e.g., during authentication at an ABC gate (this scenario is also referred to as image pair-based morphing attack detection). Note that all information extracted by no-reference morph detectors might as well be leveraged within this scenario.

VII. ISSUES AND CHALLENGES

Several open issues and challenges exist in research related to face morphing and face morphing attack detection. The most relevant issues and challenges, which have already been pointed out throughout this survey, can be briefly summarized as follows:

- *Quality*: the automated generation of high-quality face morphs remains a challenging issue and of utmost importance in order to enable statistically significant testing of developed morphing attack detection methods under realistic conditions, see Sect. III.
- *Comparability/benchmarks*: the lack of publicly available large-scale databases comprising bona fide as well as morphed face images and open-source face morphing attack detection software prevents from a meaningful comparative benchmark of the current state-of-the-art inthis field.
- *Result reporting*: while first efforts have been made to apply standardized metrics for reporting the performance of morphing attack detection mechanisms equivalent measures for the vulnerability of face recognition systems w.r.t morphing attacks are non-existent; however, these would be vital in order to enable an unambiguous comparisons of proposed approaches.
- *Over-fitting/robustness analysis*: like any other image-based classification task,

approaches to morphing attack detection are prone to overfitting, i.e., rigorous evaluations including face morphs from unseen databases created by unseen morphing techniques are necessary.

- *Print-scan databases*: to simulate real-world scenarios where potentially morphed portrait images are printed and scanned, publicly available large-scale databases of printed and scanned bona fide and morphed face images are required.

VIII. CONCLUSION

This survey provides a comprehensive overview of published literature within the field of (face) image morphing and face morphing attack detection also as an in depth discussion of open issues and challenges. The research during this important field is merely in its infancy while not being limited to face recognition systems. The feasibility of morphing biometric samples has also been shown for other biometric characteristics, e.g. fingerprint or iris, which could also be morphed in feature domain. the likelihood of morphing biometric features and subsequently reconstructing a biometric sample from morphed feature vectors underlines the importance of knowledge protection mechanisms, i.e. biometric template protection or conventional cryptographic techniques. almost like face, for other characteristics certain aspects require more in-depth analysis, e.g., biometric quality estimation of (morphed) fingerprint or iris samples respectively. The reported face image morphing attack detection accuracy is yet not reflecting generalization to datasets incorporating the important world sort of capture conditions. this may change, once benchmark portals like the NIST Face Recognition Vendor Test (FRVT) MORPH competition are established. Nevertheless, robust algorithms must also anticipate the massive sort of image post-processing also as printing and scanning technology that would be utilized in the govern- mental procedures for the appliance of electronic travel documents. Morphing attack detection mechanisms that are robust against all those factors, would require a big amount of future research.

REFERENCES

[1] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, ‘‘Face recog nition: A literature survey,’’ *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, Dec. 2003.

[2] S. Z. Li and A. K. Jain, Eds., *Handbook of Face Recognition*. London, U.K.: Springer, 2011.

[3] F. Schroff, D. Kalenichenko, and J. Philbin, ‘‘FaceNet: A unified embed- ding for face recognition and clustering,’’ in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2015, pp. 815–823.

[4] O. M. Parkhi, A. Vedaldi, and A. Zisserman, ‘‘Deep face recognition,’’ in *Proc. Brit. Mach. Vis. Conf. (BMVC)*, 2015, p. 6.

[5] A. Mohammadi, S. Bhattacharjee, and S. Marcel, ‘‘Deeply vulnerable: A study of the robustness of face recognition to presentation attacks,’’ *IET Biometrics*, vol. 7, no. 1, pp. 15–26, Jan. 2018.

[6] M. Ferrara, A. Franco, and D. Maltoni, ‘‘The magic passport,’’ in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Sep./Oct. 2014, pp. 1–7.

[7] G. Wolberg, ‘‘Image morphing: A survey,’’ *Vis. Comput.*, vol. 14, nos. 8–9, pp. 360–372, Dec. 1998.

[8] A. Patel and P. Lapsiwala, ‘‘Image morphing algorithm: A survey,’’ *Int. J. Comput. Appl.*, vol. 5, no. 3, pp. 156–160, 2015.

[9] *Information Technology—Biometric Presentation Attack Detection— Part 3: Testing and Reporting*, Standard ISO/IEC 30107-3:2017, ISO/IEC JTC1 SC37 Biometrics, International Organization for Standardization, Geneva, Switzerland, 2017.

[10] M. Ferrara, A. Franco, and D. Maltoni, ‘‘On the effects of image alter- ations on face recognition accuracy,’’ in *Face Recognition Across the Imaging Spectrum*. Cham, Switzerland: Springer, 2016, pp. 195–222.

[11] D. J. Robertson, A. Mungall, D. G. Watson, K. A. Wade,
S. J. Nightingale, and S. Butler, ‘‘Detecting morphed passport photos: A training and individual differences approach,’’ *Cognit. Res., Principles Implications*, vol. 3, no. 1, p. 27, Jun. 2018.

[12] A. Makrushin and A. Wolf, ‘‘An overview of recent advances in assessing and mitigating the face morphing attack,’’ in *Proc. 26th Eur. Signal Process. Conf. (EUSIPCO)*, 2018, pp. 1017–1021.

[13] *ICAO Doc 9303, Machine Readable Travel Documents—Part 9: Deploy- ment of Biometric Identification and Electronic Storage of Data in MRTDs*, 7th ed., Int. Civil Aviation Org., Montreal, QC, Canada, 2015.

[14] R. Raghavendra, K. B. Raja, and C. Busch, ‘‘Detecting morphed face images,’’ in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2016, pp. 1–7.

[15] I. Craw, D. Tock, and A. Bennett, ‘‘Finding face features,’’ in *Computer Vision—ECCV*. Berlin, Germany: Springer, 1992, pp. 92–96.

[16] T. F. Cootes, C. J. Taylor, D. H. Cooper, and J. Graham, ‘‘Active shape models-their training and application,’’ *Comput. Vis. Image Understand.*, vol. 61, no. 1, pp. 38–59, Jan. 1995.

[17] L. Wiskott, J.-M. Fellous, N. Krüger, and C. von der Malsburg, ‘‘Face recognition by elastic bunch graph matching,’’ in *Computer Analysis of Images and Patterns*. Berlin, Germany: Springer, 1997, pp. 456–463.

[18] T. F. Cootes, G. J. Edwards, and C. J. Taylor, ‘‘Active appearance models,’’ *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 681–685, Jun. 2001.

[19] V. Zanella and O. Fuentes, ‘‘An approach to automatic morphing of face images in frontal view,’’ in *MICAI 2004: Advances in Artificial Intelligence*. Berlin, Germany: Springer, 2004, pp. 679–687.

[20] J. M. Saragih, S. Lucey, and J. F. Cohn, ‘‘Face alignment through sub- space constrained mean-shifts,’’ in *Proc. IEEE 12th Int. Conf. Comput. Vis. (ICCV)*, Sep./Oct. 2009, pp. 1034–1041.