IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Face Morphing Attack Detection using similarity score patterns between demorphed and live images

HOANG THI THUY, HEEJUNE AHN
[1]Department of Electrical and Information Engineering, Seoul National University of Science and Technology, South Korea
Corresponding author: Heejune Ahn (e-mail: heejune@seoultech.ac.kr).

This study was supported by the Research Program funded by SeoulTech (Seoul National University of Science and Technology).

ABSTRACT Face morphing attacks have become a serious threat to Face Recognition Systems (FRS). Demorphing-based morphing attack detection has been proposed and studied, which uses suspect and live capture, but the unknown morphing parameters in the used morphing algorithm make applying demorphing methods challenging. This paper proposes a robust Face Morphing Attack Detection (FMAD) method leveraging deep learning de-morphing networks. Inspired by differences in similarity score variations between morphed and non-morphed images, the detection pipeline was proposed to learn the variation patterns of similarity scores between live capture and de-morphed face/bona fide images with different demorphing factors. An effective deep de-morphing network based on StyleGAN and the pSp (pixel2style2pixel) encoder was developed. The network generates de-morphed images from suspect and live images with multiple de-morphing factors and calculates similarity scores between feature vectors from the ArcFace network, which are then classified by the detection network. Experiments on morphing datasets from the Color FERET, FRGCv2, and SYS-MAD databases, including landmark-based and deep learning attacks demonstrate that the proposed method performs high accuracy in detecting unseen morphing attacks across different databases. It attains an Equal Error Rate (EER) of less than 3% and a Bona Fide Presentation Classification Error Rate of approximately 11% at an Attack Presentation Classification Error Rate of 0.1%, outperforming previous methods.

INDEX TERMS FMAD (face morphing attack detection), demorphing, neural network, face similarity score, ABC (automatic border control)

I. INTRODUCTION

Biometric methods are widely used to identify individuals based on unique biological and behavioral characteristics. One particular area where biometrics, especially Facial Recognition Systems (FRS), has gained considerable traction is in international airport security protocols. By leveraging biometric data stored in electronic Machine-Readable Travel Documents eMRTDs [1], FRS enables authorities to compare the facial features captured in passports with real-time images of travelers. Despite the high accuracy of state-of-the-art FRS in controlled scenarios, several studies showed that FRS is sensitive or vulnerable to many image modification attacks. One of the most dangerous threats to FRS is a face morphing attack (FMA), which seamlessly mixes multiple face images to a new facial image containing the facial features of the subjects. In the context of biometrics, face morphing poses a serious risk, as it enables the creation of synthetic identities that can bypass security measures. It is important to highlight that the production of high-quality and reliable morphed images requires the ability to remove artifacts and abnormal pixels to achieve high visual similarity, in order to convince the officer.

FMA should maximize both the probability of acceptance of the morphed image by the human officer in the enrollment stage and the possibility of being identified as the same person during the verification stage. In the enrollment stage, an attacker has to find an accomplice and morph his/her facial features with him/herself to apply for a passport or another form of electronic travel document containing the manipulated image. Once the electronic travel document containing

the morphed image is issued to the accomplice, the criminal can utilize it to bypass border controls, whether they are automated or manually operated. Such an attack exploiting the vulnerability of the FRS system was first described in [2]. Numerous face morphing attack methods [3]–[7] have been proposed, which have further highlighted the vulnerability of FRSs.

To counter the risk of such FMA attack, many face morphing attack detection (FMAD) strategies were proposed to identify instances where facial images have been morphed. Two prominent approaches in this domain are single image-based FMAD (S-FMAD) [8], [9] and differential image-based FMAD (D-FMAD) [10]–[14]. While S-FMAD evaluates individual images to determine whether they have undergone morphing, D-FMAD contrasts the suspect image with a trusted probe image to indicate cases of morphing. Among D-FMAD methods, de-morphing has emerged as a promising one. De-morphing was first introduced by Ferrara et al. [15]. In this differential FMAD approach, the trust live capture (TLC) is utilized to revert (de-morph) a potentially morphed image. Essentially, the TLC is subtracted from the suspect image with a predefined weight (de-morphing factor). The resulting de-morphed face image is then compared to TLC using an FRS. Thus, the face recognition score between the TLC and the de-morphed image serves as the final FMAD score. If this comparison yields a non-match, it indicates a morphing attack has been detected; otherwise, the authentication attempt is considered bona fide. Later, Ortega-Delcampo et al. [16] introduced autoencoders to restore accomplices' facial images for detecting morphing. Banerjee et al. [17] restored the facial images of two contributors from a single morphed image. Shiqerukaj et al. [18] combined de-morphing with Deep Face Representation. Peng et al. [19] utilized a symmetric dual network and restoration losses for accomplice image restoration. Min Long et al. [20] proposed a diffusion-based method, focusing on accomplice image reconstruction.

Though some previous methods give reasonable performance, their practical utility in real-world scenarios remains limited. Environmental factors such as varying lighting conditions, facial expressions, and image resolutions can significantly impact the detection accuracy of these methods. Specifically in de-morphing methods, the morphing factor, which represents the weight of the attacker's contribution, is an unknown variable that significantly influences performance. Due to this limitation, Ferrara et al. [15] proposed a practical range of morphing $0.1 \leq \alpha_m \leq 0.45$ for successful enrollment in landmark-based morphing method and also tested with the same range of de-morphing blending weights α_d in landmark-based one. The experiment results showed the effectiveness of de-morphing method itself but its performance varies with the combinations of two (morphing and de-morphing) blending parameters. It is a mathematically ill-posed problem to estimate the morphing factor for the suspect (morphed or bona fide) and TLC. Furthermore, the recent deep learning-based methods diverse the blending parameters so that the estimation of morphing contribution parameters has become difficult and impractical.

With the primary goal of classifying whether the suspect image is morphed or bona fide, rather than reconstructing the accomplice's face from the morphed image, we aim to reduce reliance on prior knowledge of face morphing generation in existing de-morphing methods and improve the efficiency of detecting morphing attacks. To achieve this, we train a neural network to recognize the similarity score patterns of de-morphed images, considering different contribution factors associated with enrollment. As we will show in Fig 8 in section V, similarity score variation of the de-morphed image with the live capture varying the de-morphing factor shows different patterns. Inspired by differences in similarity score variations between morphed and non-morphed images, the detection pipeline was proposed to learn the variation patterns of similarity scores between live capture and de-morphed face images with different de-morphing factors. An effective deep de-morphing network based on StyleGAN and the pSp (pixel2style2pixel) encoder was developed. The network generates de-morphed images from suspect and live images with multiple de-morphing factors and calculates similarity scores between feature vectors from the ArcFace network, which are then classified by the detection network.

The main contributions are in the following:

- We propose a D-FMAD neural network that learns the similarity score patterns of de-morphed images with different contribution factors with TLC image.
- We propose a simple but effective and efficient deep-learning face morphing and de-morphing network utilizing pixel2style2pixel [21], which does not need further fine-tuning. We used this de-morphing network for our pipeline of similarity pattern-based D-FMAD
- We conduct experiments and analysis for created FMAD databases and SYN-MAD datasets. The results demonstrate the proposed similarity pattern-based detection method outperforms the existing FMAD method in detecting unseen morphing attacks across different databases

The rest of this paper is organized as follows. Related works are reviewed in section II. Section III provides a detailed description of the proposed FMAD. The FMAD dataset is described in section IV. The experiment and analysis are presented in section V. Finally, some conclusions are drawn in section VI.

II. RELATED WORKS

A. FACE MORPHING ATTACK METHODS

The face morphing process is defined as a special effect that lends multiple facial images to generate a single image that contains identity features from multiple contributors. In recent years, obtaining a morphed image has become relatively simple and cost-effective for the general public due to advances and public availability of computer vision and image processing tools. There are various open-source solutions, alongside both free and commercial tools in the form

of downloadable applications and online services. These methods are divided into two main approaches: landmark-based and deep learning-based.

1) Landmark-based morph generation

The first and still most common creation method for generating morphs is the landmark-based approach [15], where morphing is accomplished by blending images according to corresponding landmark points within the facial region, such as the nose, eyes, and mouth areas. These reference points can be obtained through either manual annotation or automatic identification based on facial landmark detection algorithms such as Dlib [22]. Once the landmarks are identified on both faces involved in the morphing, they are used to deform or warp the facial features. During the morphing process, pixel replacement may result in misaligned pixels, causing noise and artifacts, and yielding unrealistic and easily detectable images. To address this, post-processing steps like image smoothing, sharpening, edge correction, histogram equalization, and manual retouching are typically performed to minimize artifacts [23]–[25]. Common open-source tools reliant on landmarks include GIMP/GAP [26] and OpenCV [27]. Additionally, there are various commercial options such as Face Fusion, FantaMorph, and FaceMorpher that facilitate the creation of extensive morphed image sets.

2) Deep learning-based morph generation

Recent advancements in deep learning have opened new avenues for the creation of morph generation by interpolating two facial images in the latent space based on Generative Adversarial Networks (GANs). Generally, GAN-based approaches, such as the MorGAN architecture [4] for morph generation, synthesize morphed images by sampling two facial images within the latent space of the deep learning network, employing a generator comprising encoders, decoders, and a discriminator. Venkatesh et al. [6] employ StyleGAN architecture [28] to enhance the morph generation process by embedding images in the intermediate latent space and increasing the generated image resolution that meets the ICAO standard that minimum inter-eye distance of 90 pixels. Additionally, Zhang et al. [5] propose the use of identity priors to facilitate high-quality morphed face generation (MIPGAN-I and MIPGAN-II), scaling up to threaten FRS posed by GAN-based morphs. Recently, Damer et al. [7] presented a diffusion-based method for face morphing, which shows high quality in morphing facial images compared to MIPGAN I and II.

B. FACE MORPHING ATTACK DETECTION

Face morphing attack detection has been extensively studied in the literature and can be categorized into two types: single-image FMAD and differential FMAD.

1) Single image-based MAD (S-FMAD)

The objective of S-FMAD is to accurately identify face morphing attacks using a single subject's image as input to the algorithm. The FMAD system receives the image to be analyzed, extracting features to determine whether it is a morph or a genuine image. S-FMAD can be applied during both enrollment and verification processes. In the literature on S-FMAD detection, various approaches have been proposed for detecting morph attacks. These include texture-based methods utilizing LBP, LPQ, BSIF, SIFT, and SURF features [29], [30] as well as techniques aimed at extracting noise from images [31], [32]. Some approaches detected morphing by assessing the quality differences between the original (bona fide) image and the resulting morphed image [33], [34]. Deep learning methods [35], [36] are increasingly utilized, showing superior performance compared to texture-based approaches. In order to detect morphing reliably, several approaches are put together in a hybrid form [37], [38]. Additionally, a competition was organized based on Privacy-aware Synthetic Training Data (SYN-MAD) [8] and other works highlight efforts to build a robust and generalized S-MAD with the baseline solution [9].

S-FMAD could be used for both photo enrollment and on-site control, but very challenging because it must adapt to variations in image quality, diverse sensor types (cameras), various morph generation tools, and different print-scan processes.

2) Differential image-based FMAD (D-FMAD)

D-FMAD, on the other hand, leverages a TLC in addition to the suspected morph image. While the advantages gained from the supplementary information offered by the TLC, it's worth noting that TLCs are commonly acquired in semi-supervised environments and are influenced by various external factors. D-FMAD can be classified into two primary approaches: one involves comparing the biometric characteristics of the two facial images, while the other efforts to reverse the morphing process.

The idea of Feature based D-FMAD is to extract feature vectors from a suspect image and a TLC and then compare the extracted vectors to determine whether a suspicious facial image has been morphed. A typical technique is deep face representations proposed by Scherhag et al. [13]. Muhammad Hamza et al. proposed a method to detect morph attacks on datasets containing Morph-2 and Morph-3 images [14]. Baaria Chaudhary et al. [12] employed a wavelet-based Siamese network to identify morph artifacts in the wavelet domain. Le Qin et al. [11] presented methods for detecting and locating face morphing attacks by utilizing feature-wise supervision for both single image-based and differential-based approaches. Additionally, Raghavendra Ramachandra et al. [10] introduced a multispectral image captured as a trusted capture to detect morphing attacks.

Face de-morphing techniques reverse the morphing process, reconstructing the original component images employed in creating the morphed image. Effort in this domain was pioneered by Ferrara et al. in the landmark-based method [15], which, however, relies on prior knowledge of the face morphing generation. In contrast, Ortega-Delcampo et al.

[16] introduced a convolutional neural network (CNN)-based method for detecting face morphing attacks. This approach reconstructs facial images of accomplices without requiring prior knowledge of morphed facial images. Nevertheless, the simplicity of the network architecture results in generated images of insufficient quality. Banerjee et al. [17] managed to restore the facial images of the two contributors from a single morphed facial image using a generator, three discriminators, and a series of adversarial losses. However, the performance significantly declines compared to de-morphing methods with a live image. Peng et al. [19] utilize a symmetric dual network and two layers of restoration losses to restore the facial image of the accomplice. More recently, Min Long et al. [20] proposed a diffusion-based method to encode facial images into semantic and stochastic latent spaces for face de-morphing. Both of these methods focus on reconstructing the facial image of the accomplice rather than detecting morphing attacks. Shiqerukaj et al. [18] combine two differential morphing attack detection methods, i.e. De-morphing [15] and Deep Face Representation [13]. This approach adopts demorphing with a fixed demorphing factor, potentially reducing its effectiveness when the attacker employs different priors.

Face recognition system (FRS) performance is crucial in D-FMAD performance. Different varieties of FRS are available, including commercial-off-the-shelf (COTS) [39]–[41] and deep-learning-based open-source FRS [42]–[44]. The accuracy and reliability of FRS enhance the effectiveness of methods, ensuring robust detection of morphing attacks in biometric security systems. The effectiveness of the deep face recognition network ArcFace in D-FMAD has been shown in many previous works [13], [18]. Therefore, we have integrated ArcFace into our decision network.

C. STYLEGAN

Since Generative Adversarial Networks (GAN) were introduced in 2014, there have been a lot of improvements proposed which made it a state-of-the-art method to generate synthetic images including synthetic human faces. However, there was not much focus on control over the generator part of GAN. Face morphing and de-morphing processes require the controllability of features of human faces, such as pose, hair color, eye color, etc. StyleGAN provides great controllability in a hierarchical way so that lots of reconstruction methods [21], [45], [46] and deep learning face morphing [5], [6] are developed based on it.

In the StyleGAN model, latent code $\boldsymbol{z}$ in the input latent space Z obtained from the input image is first transformed into $\boldsymbol{w}$ in the intermediate latent space W using a non-linear mapping network $f : Z \rightarrow W$, implemented as an 8-layer CNN. The dimensionality of both spaces is set to 512. Learned affine transformations then converted $\boldsymbol{w}$ into styles $\boldsymbol{y}$, controlling adaptive instance normalization (AdaIN) operations after each convolution layer of the synthesis network G. Additionally, the generator introduces explicit *noise inputs* to generate stochastic detail. These noise inputs are single-channel images of uncorrelated Gaussian noise, fed to each layer of the synthesis network and added to the output of the corresponding convolution through learned per-feature scaling factors.

Since the morphing and de-morphing process uses the existing (real) face images, not simply generating artificial face images, we need to get the feature vectors of the face images. GAN inversion aims to invert a given image back into the latent space of a pre-trained GAN model so that the image can be faithfully reconstructed from the inverted code by the generator. [47]. We compared the previous StyleGAN inversion method focusing on reconstruction performance after latent space operations for morphing and de-morphing applications and found pSp Encoder [21] performs best for morphing and de-morphing purposes. The pSp (pixel to Style to pixel) framework is based on the power of a pre-trained StyleGAN and the W^+ latent space. Rather than using explicit noise input, this model learns the latent code relative to the average style vector $\bar{W}$. Adapting to different levels of detail in StyleGAN, the pSp encoder E extends the backbone with a feature pyramid and map2style network, generating 18 style vectors. This encoder is able to match each input image to a coding in the latent domain and shows a strong representation.

III. PROPOSED FMAD METHOD

Fig. 1 illustrates the pipeline of the proposed face morphing attack detection method. The pipeline consists of 4 main stages: a (face feature) encoder network, a latent space blending block, a face decoder (StyleGAN) generator, and an ML-based decision with similarity scores evaluator. Latent vectors extracted from suspect (morphed or bona fide) images and TLC through an encoder network are blended together in the StyleGAN W+ latent space at multiple de-morphing factors. The obtained latent codes are fed into a StyleGAN generator to produce corresponding de-morphed images. These de-morphed images are compared with TLC images using ArcFace features in a machine learning-based classifier to distinguish between bona fide attempts and morph attacks

It is noteworthy that we do not propose a new encoder nor do we retrain StyleGAN. Instead, we leverage the strengths of existing models to carry out multiple de-morphing processes, thereby enabling the detection of morphed images. In this study, we employ the pSp encoder [21] with styleGAN-based decoder and ArcFace face similarity to benchmark the performance of the proposed method. However, the proposed similarity pattern-based method can be applied to other similar implementations.

A. THE VIRTUAL MORPHING METHOD

To facilitate explanation, a virtual morphing model based on StyleGAN is defined. The actual morphing method may be similar to or different from this model. Assuming that a suspect image I_{susp} is identified as a morphed image resulting from the morphing process involving criminal image I_{crim}

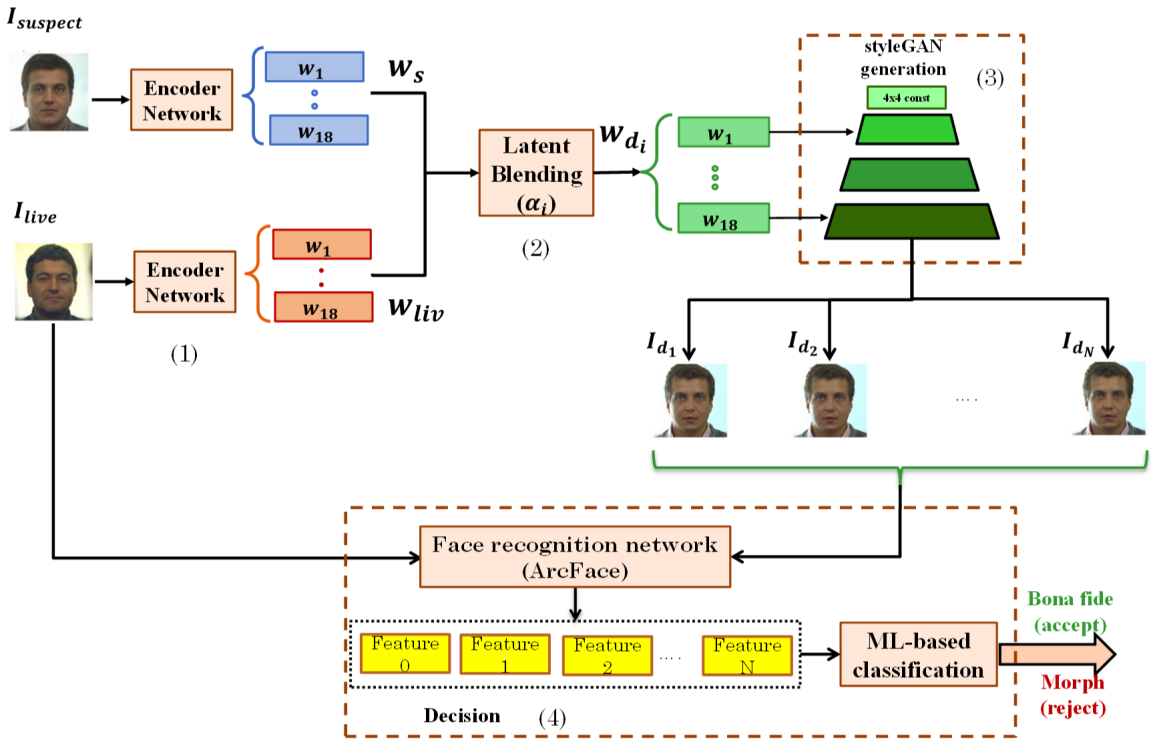

FIGURE 1. Proposed Morphing Attack Detection Pipeline. There are 4 main stages: (1) encoder network, (2) latent space blending block, (3) face decoder (StyleGAN) generator, and (4) ML-based decision with similarity scores evaluator

and accomplice image I_{acc}:

$$I_m = F^m(I_{crim}, I_{acc}, \alpha_m), \tag{1}$$

where F^m presents the morph generation and the morphing factor α_m controls the contribution of the criminal.

The criminal face image I_{crim} and accomplice face image I_{acc} are first transformed into W_{crim} (latent code for the criminal) and W_{acc} (latent code for the accomplice) through an encoder network, respectively. The morphed latent vectors are then generated via the following blending procedure:

$$W_m = \alpha_m \cdot W_{crim} + (1 - \alpha_m) \cdot W_{acc} \tag{2}$$

Morphed latent code W_m is fed into the StyleGAN generator along with $\bar{W}$ the average style vector of the pre-trained generator to produce the corresponding morphed images I_m.

$$\begin{aligned} I_m &= G(W_m + \bar{W}) && (3)\\ &= G[\alpha_m \cdot W_{crim} + (1 - \alpha_m) \cdot W_{acc} + \bar{W}] && (4)\\ &= G[\alpha_m \cdot E(I_{crim}) + (1 - \alpha_m) \cdot E(I_{acc}) + \bar{W}] && (5) \end{aligned}$$

where $G(.)$ and $E(.)$ denote the StyleGAN generator and encoder, respectively.

B. THE PROPOSED DE-MORPHING METHOD

The proposed de-morphing network is also based on pSp network, which is again specific for StyleGAN. Given a trust live capture (TLC) I_{live}, an inverse morphing process can be applied to recover the accomplice's facial image I_{acc}. From (2), the de-morphed latent codes can be obtained with de-morphing factor α_d as follows:

$$W_d = (W_{susp} - \alpha_d \cdot W_{live})/(1 - \alpha_d) \tag{6}$$

Even though we could use a more sophisticated formula for latent space de-morphing and possibly the morphing method can use different contribution factors for each latent element, we found this simple and basic formula performs very well in general for detecting the morphing attacks.

Finally, a de-morphed image is generated from the de-morphed latent vectors through the StyleGAN generator:

$$\begin{aligned} I_d &= F^d(I_{susp}, I_{live}, \alpha_d) = G(W_d + \bar{W}) && (7)\\ &= G[(W_{susp} - \alpha_d \cdot W_{live})/(1 - \alpha_d) + \bar{W}] && (8)\\ &= G[(E(I_{susp}) - \alpha_d \cdot E(I_{live}))/(1 - \alpha_d) + \bar{W}] && (9) \end{aligned}$$

where $F^d(\cdot)$ presents the de-morphing process.

In practical scenarios, the information regarding morphing factor α_m (or contribution weight of criminal in morphed image) is not available. Experiments in session IV demonstrate that even if an associated de-morphing factor could be approximated through practical assumptions, the task of reconstructing the facial features of the accomplice remains notably challenging because of post-processing. Ferrara et al. [15] also showed similar phenomena in the landmark-based demophing method. However, it may be possible to detect morphed images by performing de-morphing across various values of de-morphing factor α_d.

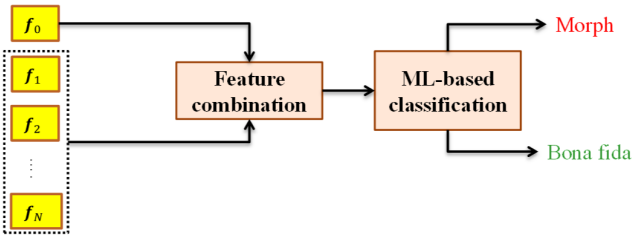

FIGURE 2. The machine learning-based decision stage involves using face features from both TLC and de-morphed images in a feature combination to obtain an N-dimension feature, which is then aggregated in a classifier to make the final decision

C. MORPHING DETECTION NETWORK WITH SIMILARITY SCORES

We apply the above de-morphing process with the same TLC I_{live} and suspect image I_{susp} at N de-morphing factor in range $[0.1, 0.5]$ and obtain multiple de-morphed images $\{I_{d_i}\}, i = 1, 2, ..., N]$. A face recognition network (ArcFace [42] in this work) is employed to extract the face-related features f_i with the size of 512 from the TLC image and set of N de-morphed images for $i = 0, 1, 2, ..., N$, f_0 is TLC's feature. These features are the input for the detection neural network at the decision stage. A simple but effective combination of the deep features is subtraction, which provides different features while keeping the training effort low. The network subsequently employs four consecutive fully connected layers comprising 256, 128, 64, and N nodes, respectively. These layers are used to extract an N-dimensional feature vector. This feature is aggregated in the final layer to estimate the FMAD score and reach the decision as illustrated in Fig. 2

IV. DATASET

A MAD database has been created from the FRGCv2 and Color FERET databases. The selected images are verified to meet ISO/ICAO specifications [48], ensuring there are no strong expressions, closed eyes, hats, or glasses. The final dataset includes 1239 subjects: 806 from Color FERET (466 male and 340 female) and 433 from FRGC (241 male and 192 female). Each dataset is divided into two groups: set A for morphing and set B contains probe images. For the images selected from the Color FERET database, one image is chosen as the criminal image and one as the probe image per subject. For the images from the FRGCv2 database, one image is chosen as the criminal image and five as probe images per subject.

Furthermore, the SYN-MAD [8] dataset including MIPGAN-I, MIPGAN-II, FaceMorpher, Webmorph, and OpenCV is additionally conducted for FMA detection evaluation. That dataset contains 4483 (984 OpenCV, 1000 FaceMorpher, 500 Webmorph, 1000 MIPGAN-I, 999 MIPGAN-II) morphed face images and 204 bona fide images from the FRLL dataset. During the morphing and de-morphing processes, all images are normalized to a resolution of 256×256

A. FMAD DATASET CREATION

Generally put, the strength of a morphing attack depends upon the criminal face. When the criminal and accomplice's faces are similar the morphed face is hard to detect. Previous works are not aligned on how to choose the dataset and only generate morphed images with equal weights of criminal and accomplice. Therefore, in this paper, we generated morphed images according to 2 protocols.

1) Protocol 1: for de-morphing network's performance evaluation

Protocol 1 is designed to evaluate the morphing generation success rate with different morphing factors in the range [0.1, 0.45]

For each subject indicated as a criminal, candidate accomplices were selected to execute morphing as follows:

1) The image of each subject (criminal) in set A is compared with the other of the same gender of the same source database (FRGC or Color FERET). The K subjects (K = 4 for experiments) with the highest ArcFace cosine similarity scores with the criminal are chosen as the accomplices for morphing.
2) The morphing processes following our StyleGan-based in (5) and FaceMorpher [3] (landmark-based) are performed between each pair of criminal and accomplice with a specific value of alpha in the range of $[0.1, 0.45]$. This results in a total of $1,239 \times 4$ (number accomplices per Criminal) $\times 8$ (number morphing factor) $= 39,648$ morphed attempts for each morphing method.
3) For the generated morphed images, ArcFace similarity scores are calculated against the probe image of the criminal to determine the morphing attack success probability (Criminal Morph Acceptance Rate) at a specific morphing factor.

2) Protocol 2: for morphing image detection performance evaluation

Protocol 2 presents the quantitative evaluation of vulnerability analysis of proposed morphed images to the Face Recognition System (FRS) at a morphing factor equal to 0.5, following [49] where morphing images with equal weights pose the highest vulnerability to FRS.

Candidates of accomplice for each criminal are selected as in protocol 1. If a pair of subjects is chosen where the first is the criminal and the second is the accomplice, the reverse order (the first as accomplice and the second as criminal) will not be selected. Instead, the next candidate with the highest score will be chosen. This results in a total of 1239×4 (number of accomplices per criminal) $= 4,956$ morphed attempts for each morphing method. Due to the limited number of probes per subject in the FERET dataset and following previous works [5], [50], Mated Morphed Presentation Match Rate (MMPMR) and Fully Mated Morphed Presentation Match Rate (FMMPMR) in table 3 are only reported on the FRGC database.

TABLE 1. Overview of the created morphed database

		Number of samples
FERET	Proposed morph	17,848
	LM-based morph	20,915
	Bona fide	1,612
FRGC	Proposed morph	10,272
	LM-based morph	12,068
	Bona fide	866

TABLE 2. Comparison of the Criminal Morph Acceptance Rate (CMAR) of the (Proposed) Morphing Attack Method with the Landmark-based Method at Different Morphing alpha

Morph alpha	Proposed (FRGC)	Proposed (FERET)	FaceMorpher [3] (FRGC)	FaceMorpher [3] (FERET)
0.10	31.8	22.1	47.6	32.7
0.15	43.1	33.2	65.1	49.9
0.20	57.7	47.1	78.0	67.0
0.25	71.5	61.8	86.6	78.4
0.30	81.0	73.7	91.5	86.0
0.35	88.8	82.8	94.3	90.8
0.40	92.6	89.2	95.5	94.0
0.45	95.2	93.0	96.7	95.2

For FMAD, morphed images that successfully match against criminal images are collected from protocols 1 and 2. Table 1 summarizes the created database for face morphing attack detection. For each dataset created using a different method from the original dataset, we split it into training and testing sets in a $7:3$ ratio. Then, we trained a model on one dataset and tested it on all the other datasets, as shown in Table 7, Section V. The SYN-MAD dataset is used solely for evaluation. Face de-morphing is executed on the suspect image (bona fide or morphed image) and corresponding TLC from Set B. For the FRGC dataset, the first image in the probe set is selected as the Live image. Meanwhile, since each subject in the SYN-MAD dataset has only 2 genuine images (1 neutral and 1 smiling) when one image is utilized as Criminal for morphing, the remaining image of the subject will be used as the TLC.

B. PROPERTIES AND STATISTICS OF MORPHING ATTACK DATASETS

During the morphing and de-morphing experimentation, a threshold score corresponding to a FAR (false acceptance rate) of 0.1% has been used for both datasets according to Frontex guidelines, where the target FAR is 0.1% and FRR is 5%. Table 2 summarizes the criminal morph acceptance rate (C-MAR) of morphed images in protocol 1. The results indicate that as the criminal's contribution to the image becomes more noticeable, the acceptance rate of morphed images increases significantly, eventually reaching a level comparable to that of the landmark-based method [3] (95.2% and 93% compared to 96.7% and 95.2%).

Fig. 3 and 4 present some examples of morphed images generated by the proposed StyleGAN-based morphing method and FaceMorpher [3]. The first and second columns show involving criminals and accomplices, respectively, with the cosine similarity score calculated between them. The third to fifth columns display morphed images with morphing alphas ranging from 0.3 to 0.5. The scores of these morphed images are compared with the live images in the last column. It is obvious that as the morphing alpha increases, the morphed images exhibit higher similarity scores when compared to the Criminal, indicating a greater correlation to the Criminal.

TABLE 3. Quantitative evaluation of vulnerability of ArcFace [42] FRS at morphing alpha 0.5

	MMPMR (%)	**FMMPMR (%)**
Landmark-I [23]	99.68	98
Landmark-II [47]	91.79	84.96
FaceMorpher [16]	96.42	92.43
StyleGan [7]	72.80	56.95
MIPGAN-I [9]	94.45	85.94
MIPGAN-II [9]	94.21	86.94
Proposed	94.46	82.40

The Mated Morphed Presentation Match Rate (MMPMR) and Fully Mated Morphed Presentation Match Rate (FMMPMR) of the created morph, indicating the vulnerability of the Face Recognition System (FRS) on protocol 2, are shown in Table 3. It should be noted that the created databases differ from other databases used in scientific publications on MA and MAD. In particular, the intra-class variation is much higher in our database due to the number of selected subjects. This approach ensures that our database is more eligible to simulate real-world scenarios. Even though the comparisons are relative, the results show that the proposed morph method indicates high vulnerability, outperforming both StyleGAN and Landmark-II, and approaching the performance of the MIPGAN method. This emphasizes the high quality of morphs produced by the proposed method, making them reliable for the evaluation proposed detection method.

V. EXPERIMENTS AND RESULTS

In this section, we will first evaluate the proposed de-morphing algorithm and then the similarity score pattern detection method with this de-morphing approach.

A. PERFORMANCE OF THE PROPOSED DE-MORPHING METHOD

Table 4 reports the genuine acceptance rate (GAR) without de-morphing compared to those obtained with different values of the de-morphing factor α_d in the range of $[0.1, 0.45]$. Tables 5 and 6 present the criminal morph acceptance rate (C-MAR) as a function of both the morphing factor used to create the morphed images and the de-morphing factor from FRGC and FERET database, respectively. The results indicate a trade-off between the false acceptance rate (FAR), also referred to as the CMAR, and the false rejection rate (FRR), equivalent to 1 - GAR, as the de-morphing factor α_d increases. Moreover, the proposed de-morphing method demonstrates greater efficiency when applied to morphs from

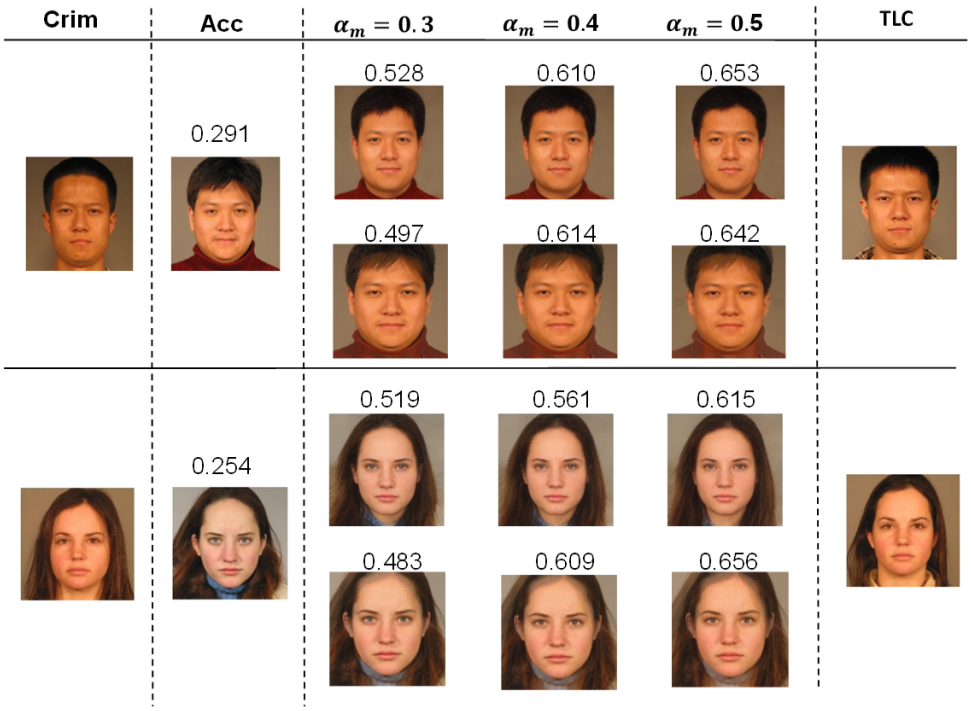

FIGURE 3. Examples of morphed images from FRGCv2. For each attack, the first and second columns show the criminals and accomplices with their similarity scores. The third to fifth columns display morphed images with alpha from 0.3 to 0.5, and their scores are compared with live images in the last column. The upper row is proposed morphed images, and the lower row is morphed images by FaceMorpher [3]

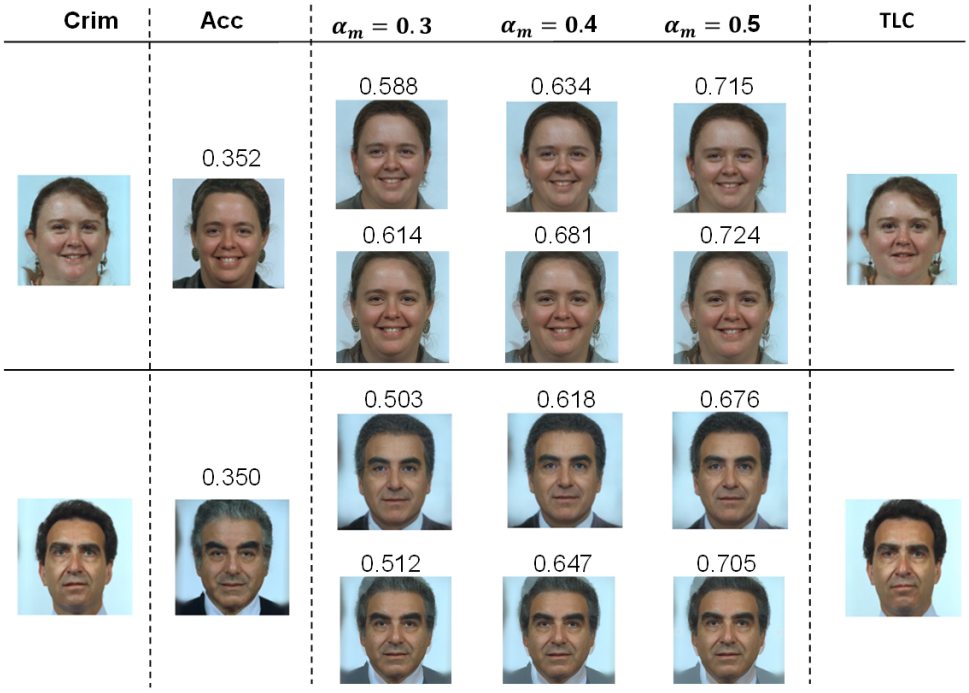

FIGURE 4. Examples of morphed images from FERET. For each attack, the first and second columns show the criminals and accomplices with their similarity scores. The third to fifth columns display morphed images with alpha from 0.3 to 0.5, and their scores are compared with live images in the last column. The upper row is proposed morphed images, and the lower row is morphed images by FaceMorpher [3]

TABLE 4. Genuine acceptance rate (%) on FERET and FRGC datasets with different values of de-morphing alpha using proposed method

	No demorph	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
FERET	100.0	100.0	100.0	99.9	99.9	99.8	99.8	98.8	97.5
FRGC	100.0	100.0	100.0	100.0	99.5	98.6	97.9	96.5	94.2

TABLE 5. Criminal Morph Acceptance Rate (%) on FRGC dataset at different values of the morphing alpha when performing de-morphing with different values of de-morphing alpha

Morph alpha	No de-morph	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
0.10	31.8	**8.2**	5.1	2.8	1.4	0.9	0.5	0.1	0.0
0.15	43.1	12.1	**7.7**	4.8	2.5	1.3	0.8	0.3	0.1
0.20	57.7	17.7	12.1	**7.3**	4.5	2.5	1.2	0.6	0.1
0.25	71.5	26.1	18.9	11.7	**7.2**	4.0	2.3	1.0	0.5
0.30	81.0	36.9	27.7	18.0	11.5	**7.0**	4.0	1.7	0.8
0.35	88.8	47.3	37.7	27.7	18.3	11.4	**6.9**	3.3	1.1
0.40	92.6	58.5	48.3	37.8	27.7	18.4	11.4	**6.5**	2.9
0.45	95.2	69.7	60.8	50.3	39.4	27.7	18.9	10.9	**5.8**

the FERET database compared to those from FRGCv2. Examples of de-morphing on bona fide and morphed images are presented in Fig. 5 and 6. The first and second columns show the suspect (bona fide or morph) and TLC. The third to seventh columns display de-morphed images with alpha from 0.1 to 0.5, and their scores are compared with TLC. It is obvious that as the de-morphing alpha increases from 0.1 to 0.5, the reduction in similarity score for bona fide images is around 0.1, whereas the reduction in similarity score for morphed images is more substantial, varying from 0.2 to 0.35

The performance of proposed de-morph is compared to the landmark-based de-morphing method [15] in Fig. 7. The solid line indicates the results of the proposed de-morphing and the dashed line indicates the landmark-based de-morphing method [15]. It is evident that when the morphing alpha is 0.25 or higher the proposed method significantly outperforms the landmark-based method in CMAR. Importantly, there is no notable decline in the GAR as observed in the landmark-based method.

B. MORPHING ATTACK DETECTION PERFORMANCE

For FMAD purposes, N de-morphing factors in a range of $[0.1, 0.5]$ are used to produce de-morphed images from the suspect and TLC. As the validating experiments will be presented later, we found that $N = 5$ is a good hyper-parameter value for computation efficiency and detection performance.

TABLE 6. Criminal Morph Acceptance Rate (%) on FERET dataset at different values of the morphing alpha when performing de-morphing with different values of de-morphing alpha

Morph alpha	No de-morph	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
0.10	22.1	**4.8**	2.8	1.4	0.7	0.5	0.3	0.1	0.1
0.15	33.2	8.4	**4.9**	2.6	1.4	0.8	0.4	0.2	0.1
0.20	47.1	12.7	8.5	**4.6**	2.5	1.4	0.6	0.3	0.1
0.25	61.8	19.4	13.3	8.4	**4.6**	2.4	1.1	0.6	0.3
0.30	73.7	29.3	20.9	13.5	8.0	**4.6**	2.5	1.1	0.4
0.35	82.8	40.8	30.7	21.8	14.1	8.8	**4.6**	2.3	1.0
0.40	89.2	53.3	42.9	32.2	22.8	14.7	8.7	**4.2**	1.9
0.45	93.0	64.7	55.8	44.4	33.9	24.1	15.1	8.7	**4.5**

TABLE 7. The Detection performance of proposed MAD algorithms on created MAD dataset using different morphing methods with cross-database

Train dataset	Test dataset	EER (%)	BPCER10 (%)
FERET (proposed)	FERET (proposed)	0.78	0.12
	FRGC (proposed)	1.56	0.69
	FERET (LM-based [3])	2.83	0.99
	FRGC (LM-based [3])	3.76	1.15
FRGC (proposed)	FERET (proposed)	0.99	0.37
	FRGC (proposed)	2.12	1.15
	FERET (LM-based [3])	2.44	1.12
	FRGC (LM-based [3])	3.82	2.08
FERET (LM-based [3])	FERET (proposed)	1.19	0.37
	FRGC (proposed)	2.86	1.15
	FERET (LM-based [3])	2.50	1.12
	FRGC (LM-based [3])	4.12	2.31
FRGC (LM-based [3])	FERET (proposed)	1.19	0.50
	FRGC (proposed)	3.11	1.15
	FERET (LM-based [3])	3.09	0.99
	FRGC (LM-based [3])	4.36	2.54
Average		**2.66 ± 1.06**	**1.18±0.63**

The ability to detect FMA through multiple de-morphing was evaluated using the Equal Error Rate (EER) and the Bona Fide Presentation Classification Error Rate at Attack Presentation Classification Error Rate $= 10\%$(BPCER10). The results on created morphed dataset are presented in Table 7. The D-FMAD method is generally more likely to detect FMAs with lower weights compared to FMAs where morphs have been created using equal weights of the contributing face images. Therefore, while the training set includes morphed images with morphing factors ranging from 0.1 to 0.5, table 7 reports only the testing results for morphed images with a morphing factor of 0.5, which poses the highest risk to facial recognition systems (FRS). The proposed detection method achieves EER approximately 1% on the FERET dataset and roughly 3% on the FRGC dataset when morphed images are generated by the proposed morphing attack. Although the EER is higher for morphed images created using the landmark-based method [3], it is still around 3% on the FERET dataset and not far off 4% on the FRGC dataset. It is evident from the results that the proposed method exhibits stability across different datasets and effectively detects unseen FMA, including both deep learning-based and landmark-based methods. Furthermore, results for testing with fully morphed images using morphing factors ranging from 0.1 to 0.5, as detailed in Appendix A. The findings demonstrate that our method achieves strong performance even when the morphing factor is unknown.

Table 8 presents the detection performances of proposed method compared to six S-MAD methods (top four solutions in competition SYN-MAD 2022 [8] and two solutions using depth information [9]) on the SYN-MAD dataset. The proposed detection method excels in detecting morphed images from StyleGAN-based attacks. Even though EER is slightly higher on some specific landmark-based morphs, it overall maintains stable detection performance when applied to unseen morphing attacks.

To evaluate the impact of varying the number of de-morphing, additional tests have been carried out for different numbers of de-morphing factors ($N = 2, 3, 5, 9$). Fig. 9 shows EER and BPCER10 for these values of N on all

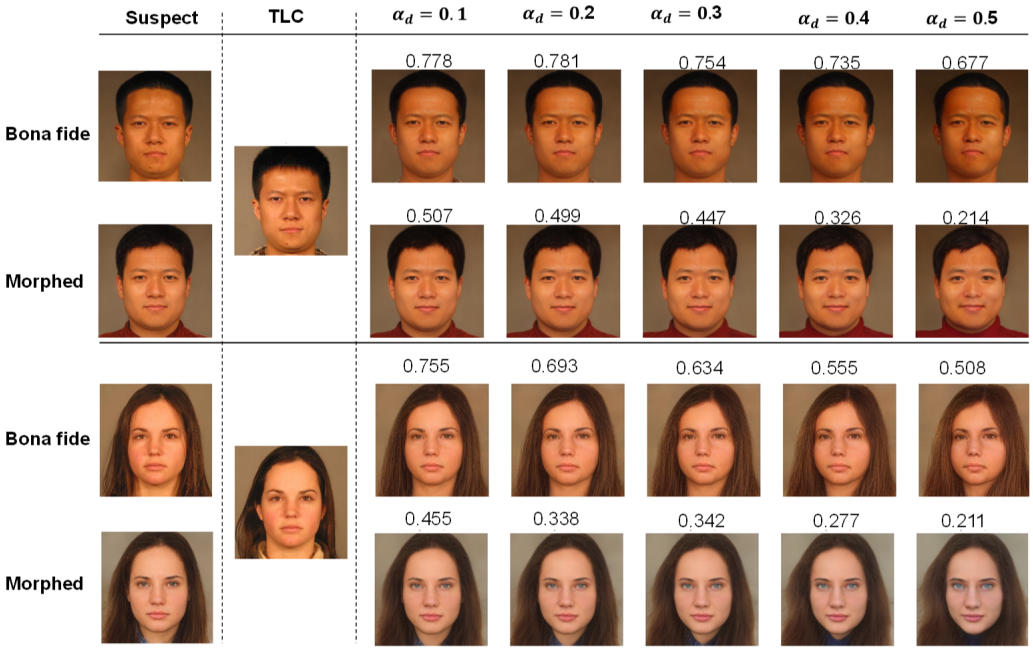

FIGURE 5. Examples of de-morphing on bona fide and morphed images from FRGCv2. The first and second columns show the suspect (bona fide or morph) and TLC. The third to seventh columns display de-morphed images with alpha from 0.1 to 0.5, and their scores are compared with TLC.

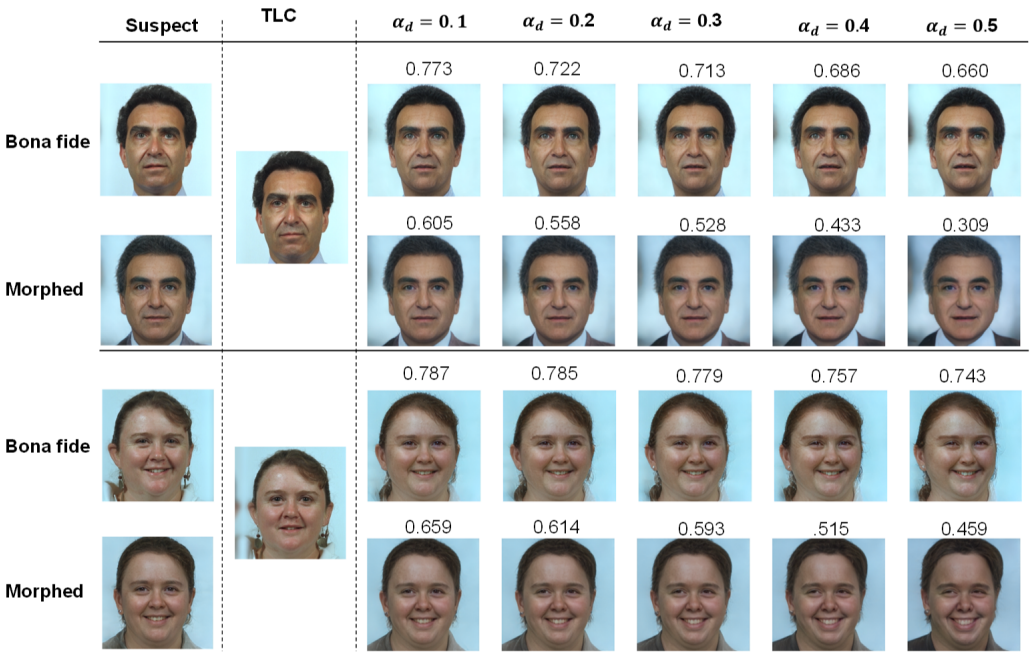

FIGURE 6. Examples of de-morphing on bona fide and morphed images from FERET. The first and second columns show the suspect (bona fide or morph) and TLC. The third to seventh columns display de-morphed images with alpha from 0.1 to 0.5, and their scores are compared with TLC.

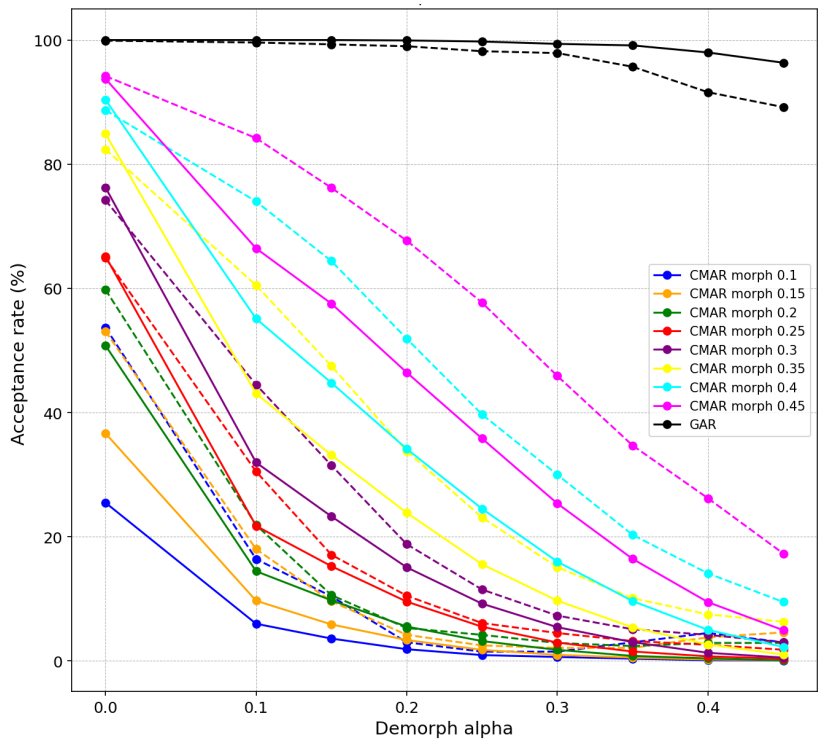

FIGURE 7. Comparison between proposed landmark-based methods. The solid line indicates the results of the proposed de-morphing and the dashed line indicates the landmark-based de-morphing method [15]. The proposed method significantly outperforms the landmark-based method in CMAR on the same morphing and de-morphing factor values. Notably, there is no significant decrease in GAR, unlike the decline seen with the landmark-based method.

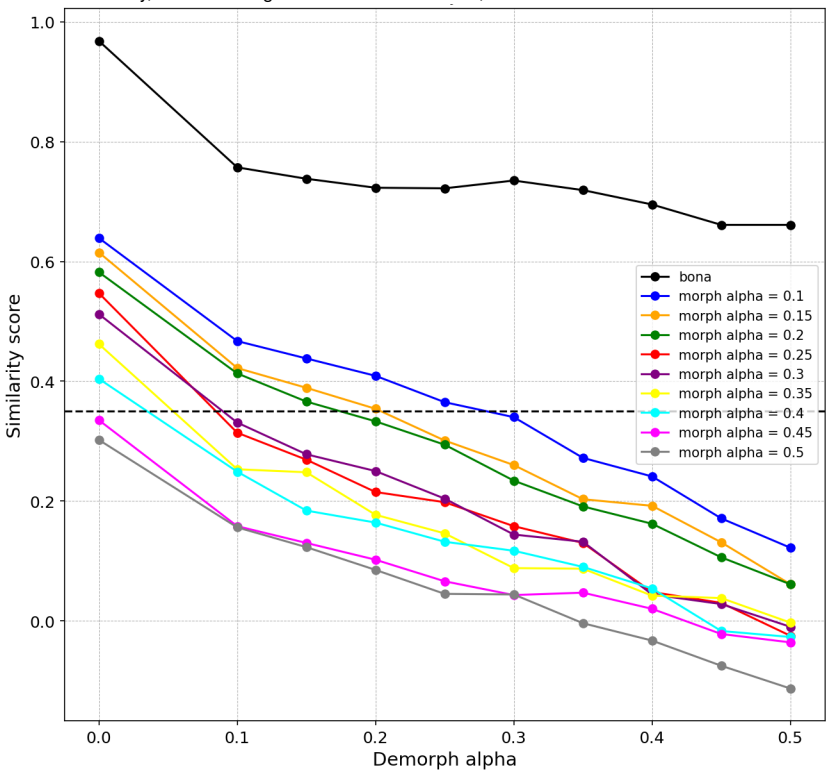

FIGURE 8. An example of the change of similarity scores between TLC and de-morphed face images at several morphing alphas. As the de-morphing factor rises from 0.1 to 0.5, the similarity scores between TLC and de-morphed images of a morphed image drop significantly below the threshold. In contrast, for bona fide images, these scores remain well above the threshold

TABLE 8. The detection performance of proposed MAD algorithms on the SYN-MAD database

	OpenCV		FacaMorpher		Webmorph		MIPGAN I		MIPGAN II	
	EER (%)	BPCER10 (%)	EER (%)	BPCER10 (%)	EER (%)	BPCER10 (%)	EER (%)	BPCER10 (%)	EER (%)	BPCER10 (%)
MorphHRNet [8]	5.69	1.96	5.90	1.96	9.80	10.78	15.30	24.02	10.41	11.27
Xception [8]	7.32	4.90	0.60	1.47	14.60	21.57	36.90	57.35	44.54	67.65
Con-Text Net A [8]	17.48	32.84	**0.00**	0.00	26.20	48.53	12.30	16.18	12.91	19.61
Con-Text Net B [8]	22.66	43.14	**0.00**	0.00	31.40	55.39	30.30	60.29	29.43	61.76
D-FW-MixFaceNet [9]	13.72	-	0.10	-	10.80	-	6.70	-	6.61	-
D-FW-CDCN [9]	**0.30**	-	**0.00**	-	**0.00**	-	11.9	-	14.11	-
Proposed	1.29	0.98	1.26	1.00	1.11	0.96	**0.10**	0.73	**0.18**	0.74

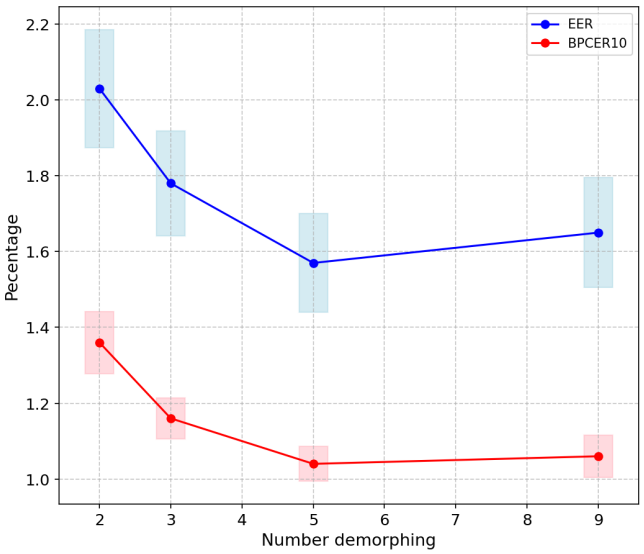

FIGURE 9. ERR and BPCER10 for different numbers de-morphing. The line plot illustrates the average values, while the rectangles surrounding each data point indicate the range of potential error, with the heights representing the standard deviation at a rate of $1/5$

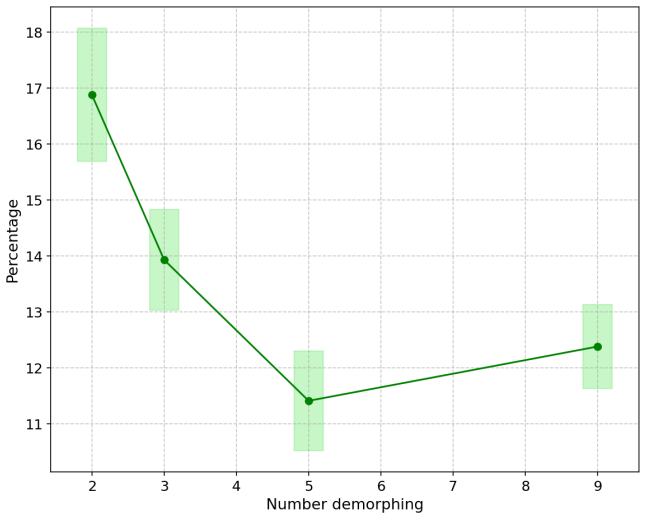

FIGURE 10. BPCER when APCER $= 0.1\%$ for different numbers de-morphing. The line plot illustrates the average values, while the rectangles surrounding each data point indicate the range of potential error, with the heights representing the standard deviation at a rate of $1/5$

testing datasets. The line plot illustrates the average EER and BPCER10, while the rectangles surrounding each data point indicate the range of potential error, with the heights representing the standard deviation at a rate of $1/5$. Increasing the number of de-morphing factors slightly reduces the EER but also increases detection time. In contrast, using a large number of de-morphing processes can lead to overfitting. For real-time applications, $N = 5$ is a good trade-off.

Additionally, to be applicable in real-world scenarios, the False Acceptance Rate (FAR) should be smaller than 0.1%. The Bona Fide Presentation Classification Error Rate at an Attack Presentation Classification Error Rate of 0.1% (BPCER0.1) for different numbers of de-morphing is also shown in Fig. 10. The BPCER0.1 value at $N = 5$ is 11.41%, which is still higher than the Frontex requirements [51] of being smaller than 5%. This remains a motivation for improving the FMAD method in the future.

VI. CONCLUSION

In this paper, we proposed a full D-FMAD pipeline based on DL de-morphing technology that addresses challenges in face morphing attacks at FRS. Inspired by differences in similarity score variations between morphed and non-morphed images, the proposed approach learns the change patterns of similarity scores between live capture and de-morphed face images with different demorphing factors. An effective deep de-morphing network based on StyleGAN and the pSp (pixel2style2pixel) encoder was developed. The method generates de-morphed images from suspect and live images with multiple de-morphing factors and calculates similarity scores between feature vectors from the ArcFace network, which are then classified by the detection network. Experiments on morphing datasets from the Color FERET, FRGCv2, and SYS-MAD databases, including landmark-based and deep learning attacks demonstrate that the proposed method performs high accuracy in detecting unseen morphing attacks across different databases.

It is important to emphasize that the approach using the similarity score variation in the proposed pipeline is not restricted to specific de-morphing techniques. This underscores the potential for improving FMAD tasks by employing advanced de-morphing techniques, particularly since current researches still fall short of meeting the needs of real-world systems.

APPENDIX. A

This appendix contains additional results on testing datasets with unknown morphing factors in the range $[0.1, 0.5]$. This result is superior to those obtained from morphed images with equal weight contributions ($\alpha_m = 0.5$), indicating that the D-FMAD methods are generally more effective when dealing with FMAs created from face images with lower weights.

TABLE 9. The detection performance of proposed MAD algorithms on the created MAD dataset with unknown morphing factors in range $[0.1, 0.5]$.

Train dataset	Test dataset	EER (%)	BPCER10 (%)
FERET (proposed)	FERET (proposed)	0.56	0.12
	FRGC (proposed)	1.10	0.46
	FERET (LM-based [3])	1.53	0.25
	FRGC (LM-based [3])	1.80	0.69
FRGC (proposed)	FERET (proposed)	0.90	0.00
	FRGC (proposed)	1.97	0.46
	FERET (LM-based [3])	1.40	0.25
	FRGC (LM-based [3])	2.30	0.69
FERET (LM-based [3])	FERET (proposed)	1.10	0.12
	FRGC (proposed)	1.88	0.46
	FERET (LM-based [3])	1.52	0.24
	FRGC (LM-based [3])	2.81	0.92
FRGC (LM-based [3])	FERET (proposed)	1.08	0.13
	FRGC (proposed)	2.46	0.69
	FERET (LM-based [3])	1.86	0.37
	FRGC (LM-based [3])	2.96	1.15
Average		**1.70±0.67**	**0.44±0.31**

REFERENCES

[1] LOGICAL DATA STRUCTURE-LDS. Machine readable travel documents.

[2] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. The magic passport. In IEEE International Joint Conference on Biometrics, pages 1–7, 2014.

[3] FaceMorpher. Online. https://github.com/alyssaq/face_morpher.

[4] Naser Damer, Alexandra Mosegui Saladie, Andreas Braun, and Arjan Kuijper. 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), pages 1–10. IEEE, 2018.

[5] Haoyu Zhang, Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Naser Damer, and Christoph Busch. Mipgan—generating strong and high quality morphing attacks using identity prior driven gan. IEEE Transactions on Biometrics, Behavior, and Identity Science, 3(3):365–383, 2021.

[6] Sushma Venkatesh, Haoyu Zhang, Raghavendra Ramachandra, Kiran Raja, Naser Damer, and Christoph Busch. Can gan generated morphs threaten face recognition systems equally as landmark based morphs?-vulnerability and detection. In 2020 8th International Workshop on Biometrics and Forensics (IWBF), pages 1–6. IEEE, 2020.

[7] Naser Damer, Meiling Fang, Patrick Siebke, Jan Niklas Kolf, Marco Huber, and Fadi Boutros. Mordiff: Recognition vulnerability and attack detectability of face morphing attacks created by diffusion autoencoders. In 2023 11th International Workshop on Biometrics and Forensics (IWBF), pages 1–6. IEEE, 2023.

[8] Marco Huber, Fadi Boutros, Anh Thi Luu, Kiran Raja, Raghavendra Ramachandra, Naser Damer, Pedro C Neto, Tiago Gonçalves, Ana F Sequeira, Jaime S Cardoso, et al. Syn-mad 2022: Competition on face morphing attack detection based on privacy-aware synthetic training data. In 2022 IEEE International Joint Conference on Biometrics (IJCB), pages 1–10. IEEE, 2022.

[9] Harsh Rachalwar, Meiling Fang, Naser Damer, and Abhijit Das. Depth-guided robust face morphing attack detection. In 2023 IEEE International Joint Conference on Biometrics (IJCB), pages 1–9. IEEE, 2023.

[10] Raghavendra Ramachandra, Sushma Venkatesh, Naser Damer, Narayan Vetrekar, and Rajendra S Gad. Multispectral imaging for differential face morphing attack detection: A preliminary study. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pages 6185–6193, 2024.

[11] Le Qin, Fei Peng, and Min Long. Face morphing attack detection and localization based on feature-wise supervision. IEEE Transactions on Information Forensics and Security, 17:3649–3662, 2022.

[12] Baaria Chaudhary, Poorya Aghdaie, Sobhan Soleymani, Jeremy Dawson, and Nasser M Nasrabadi. Differential morph face detection using discriminative wavelet sub-bands. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pages 1425–1434, 2021.

[13] Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, and Christoph Busch. Deep face representations for differential morphing attack detection. IEEE transactions on information forensics and security, 15:3625–3639, 2020.

[14] Muhammad Hamza, Samabia Tehsin, Hanen Karamti, and Norah Saleh Alghamdi. Generation and detection of face morphing attacks. IEEE Access, 10:72557–72576, 2022.

[15] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Face demorphing. IEEE Transactions on Information Forensics and Security, 13(4):1008–1017, 2017.

[16] David Ortega-Delcampo, Cristina Conde, Daniel Palacios-Alonso, and Enrique Cabello. Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access, 8:92301–92313, 2020.

[17] Sudipta Banerjee, Prateek Jaiswal, and Arun Ross. Facial de-morphing: Extracting component faces from a single morph. In 2022 IEEE International Joint Conference on Biometrics (IJCB), pages 1–10. IEEE, 2022.

[18] Elidona Shiqerukaj, Christian Rathgeb, Johannes Merkle, Pawel Drozdowski, and Benjamin Tams. Fusion of face demorphing and deep face representations for differential morphing attack detection. In 2022 International Conference of the Biometrics Special Interest Group (BIOSIG), pages 1–5. IEEE, 2022.

[19] Fei Peng, Le-Bing Zhang, and Min Long. Fd-gan: Face de-morphing generative adversarial network for restoring accomplice's facial image. IEEE Access, 7:75122–75131, 2019.

[20] Min Long, Quantao Yao, Le-Bing Zhang, and Fei Peng. Face de-morphing based on diffusion autoencoders. IEEE Transactions on Information Forensics and Security, 2024.

[21] Elad Richardson, Yuval Alaluf, Or Patashnik, Yotam Nitzan, Yaniv Azar, Stav Shapiro, and Daniel Cohen-Or. Encoding in style: a stylegan encoder for image-to-image translation. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pages 2287–2296, 2021.

[22] Davis E King. Dlib-ml: A machine learning toolkit. The Journal of Machine Learning Research, 10:1755–1758, 2009.

[23] Yanlin Weng, Lvdi Wang, Xiao Li, Menglei Chai, and Kun Zhou. Hair interpolation for portrait morphing. In Computer Graphics Forum, volume 32, pages 79–84. Wiley Online Library, 2013.

[24] Clemens Seibold, Wojciech Samek, Anna Hilsmann, and Peter Eisert. Detection of face morphing attacks by deep learning. In Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16, pages 107–120. Springer, 2017.

[25] Tom Neubert, Andrey Makrushin, Mario Hildebrandt, Christian Kraetzer, and Jana Dittmann. Extended stirtrace benchmarking of biometric and forensic qualities of morphed face images. Iet Biometrics, 7(4):325–332, 2018.

[26] GIMP. Gnu image manipulation program web site. Online. https://www.gimp.org.

[27] OpenCV. Accessed: 2023. Online. https://learnopencv.com/face-morph-using-opencv-cpp-python.

[28] Tero Karras, Samuli Laine, and Timo Aila. A style-based generator architecture for generative adversarial networks. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pages 4401–4410, 2019.

[29] Ulrich Scherhag, Ramachandra Raghavendra, Kiran B Raja, Marta Gomez-Barrero, Christian Rathgeb, and Christoph Busch. On the vulnerability of face recognition systems towards morphed face attacks. In 2017 5th international workshop on biometrics and forensics (IWBF), pages 1–6. IEEE, 2017.

[30] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Morph deterction from single face image: A multi-algorithm fusion approach. In Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications, pages 6–12, 2018.

[31] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Luuk Spreeuwers, Raymond Veldhuis, and Christoph Busch. Detecting morphed face attacks using residual noise from deep multi-scale context aggregation

network. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pages 280–289, 2020.
[32] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Luuk Spreeuwers, Raymond Veldhuis, and Christoph Busch. Morphed face detection based on deep color residual noise. In 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), pages 1–6. IEEE, 2019.
[33] Clemens Seibold, Anna Hilsmann, and Peter Eisert. Reflection analysis for face morphing attack detection. In 2018 26th European Signal Processing Conference (EUSIPCO), pages 1022–1026. IEEE, 2018.
[34] Ulrich Scherhag, Luca Debiasi, Christian Rathgeb, Christoph Busch, and Andreas Uhl. Detection of face morphing attacks based on prnu analysis. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(4):302–317, 2019.
[35] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Face morphing detection in the presence of printing/scanning and heterogeneous image sources. IET Biometrics, 10(3):290–303, 2021.
[36] Naser Damer, Steffen Zienert, Yaza Wainakh, Alexandra Mosegui Saladie, Florian Kirchbuchner, and Arjan Kuijper. A multi-detector solution towards an accurate and generalized detection of face morphing attacks. In 2019 22th International Conference on Information Fusion (FUSION), pages 1–8. IEEE, 2019.
[37] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, and Christoph Busch. Single image face morphing attack detection using ensemble of features. In 2020 IEEE 23rd International Conference on Information Fusion (FUSION), pages 1–6. IEEE, 2020.
[38] Raghavendra Ramachandra, Sushma Venkatesh, Kiran Raja, and Christoph Busch. 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), pages 1–8. IEEE, 2019.
[39] Eyedea. Available: https://www.eyedea.cz/eyeface-sdk.
[40] C. S. GmbH. Facevacs Technology. Online. Available: https://www.cognitec.com/facevacs-technology.html.
[41] F. COTS. Verilook Cots. Online. Available: http://www.neurotechnology.com/verilook.html.
[42] Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pages 4690–4699, 2019.
[43] Qiong Cao, Li Shen, Weidi Xie, Omkar M Parkhi, and Andrew Zisserman. Vggface2: A dataset for recognising faces across pose and age. In 2018 13th IEEE international conference on automatic face & gesture recognition (FG 2018), pages 67–74. IEEE, 2018.
[44] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 815–823, 2015.
[45] Jiapeng Zhu, Yujun Shen, Deli Zhao, and Bolei Zhou. In-domain gan inversion for real image editing. In European conference on computer vision, pages 592–608. Springer, 2020.
[46] Tianyi Wei, Dongdong Chen, Wenbo Zhou, Jing Liao, Weiming Zhang, Lu Yuan, Gang Hua, and Nenghai Yu. E2style: Improve the efficiency and effectiveness of stylegan inversion. IEEE Transactions on Image Processing, 31:3267–3280, 2022.
[47] Weihao Xia, Yulun Zhang, Yujiu Yang, Jing-Hao Xue, Bolei Zhou, and Ming-Hsuan Yang. Gan inversion: A survey. IEEE transactions on pattern analysis and machine intelligence, 45(3):3121–3138, 2022.
[48] Information technology — Biometric data interchange formats — Part 5: Face image data. doccument ISO/IEC 19794-5, 2011.
[49] Ramachandra Raghavendra, KiranB Raja, Sushma Venkatesh, and Christoph Busch. Face morphing versus face averaging: Vulnerability and detection. In 2017 IEEE International Joint Conference on Biometrics (IJCB), pages 555–563. IEEE, 2017.
[50] Rameen Abdal, Yipeng Qin, and Peter Wonka. Image2stylegan: How to embed images into the stylegan latent space? In Proceedings of the IEEE/CVF international conference on computer vision, pages 4432–4441, 2019.
[51] RDU Frontex. Best practice operational guidelines for automated border control (abc) systems. European Agency for the Management of Operational Cooperation, Research and Development Unit,. https://bit.ly/2KYBXhz Accessed, 9(05):2013, 2012.

HOANG THI THUY was born in Vietnam, in 1994. She received her B.S. degree in Control and Automation Engineering from Le Quy Don Technical University, Hanoi, Vietnam, in 2018. Now, she is working toward an M.S. degree in the Department of Electrical and Information Engineering (EIE) at Seoul National University of Science and Technology (SeoulTech), South Korea. Her current research interests include computer vision, machine learning, and face morphing.

HEEJUNE AHN is a professor in the Department of Electrical and Information Engineering (EIE) at Seoul National University of Science and Technology (SeoulTech), South Korea. He conducts research works in computer vision, machine learning, and computer networks. Professor Ahn earned his Ph.D. in 2000 from KAIST, Korea. He finished his postdoc at the University of Erlangen-Nuremberg, Germany. He also served as a senior engineer in LG Electronics, and chief engineer in Tmax Soft Inc, South Korea. He joined SeoulTech in 2004.