GAN-based Minutiae-driven Fingerprint Morphing

Meghana Rao Bangalore Narasimha Prasad
Otto-von-Guericke University
Magdeburg, Germany
meghana.bangalore@ovgu.de

Andrey Makrushin
Otto-von-Guericke University
Magdeburg, Germany
andrey.makrushin@ovgu.de

Matteo Ferrara
University of Bologna
Bologna, Italy
matteo.ferrara@unibo.it

Christian Kraetzer
Otto-von-Guericke University
Magdeburg, Germany
kraetzer@ovgu.de

Jana Dittmann
Otto-von-Guericke University
Magdeburg, Germany
jana.dittmann@ovgu.de

ABSTRACT

Fingerprint morphing is the process of combining two or more distinct fingerprints to create a new, morphed fingerprint that includes identity-related characteristics of all constituent fingerprints. Previously, this was done by either applying a model-based minutiae-oriented approach or a data-driven approach based on a Generative Adversarial Network (GAN). The model-based approach provides the ability to manage the number of minutiae coming from the fingerprints, but the resulting fingerprint often appears unrealistic. On the other hand, the data-driven approach produces realistic fingerprints, but it does not guarantee that the resulting fingerprint matches the original fingerprints. In this work, we introduce an algorithm that combines minutiae-oriented and GAN-based approaches to generate morphed fingerprints that look realistic and match their original fingerprints. The algorithm is initially designed to generate double-identity fingerprints and is further extended to generate triple-identity fingerprints. The results of our experiments indicate that the generated fingerprints appear realistic and the majority of them can be seen as double-identity fingerprints. The fingerprints resulting from morphing three fingerprints are unlikely to be triple-identity fingerprints, but rather anonymous ones matching none of the constituent original fingerprints.

CCS CONCEPTS

• **Security and privacy → Biometrics**.

KEYWORDS

Biometrics; Fingerprint reconstruction; Fingerprint morphing

ACM Reference Format:
Meghana Rao Bangalore Narasimha Prasad, Andrey Makrushin, Matteo Ferrara, Christian Kraetzer, and Jana Dittmann. 2024. GAN-based Minutiae-driven Fingerprint Morphing. In *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '24), June 24–26, 2024, Baiona, Spain.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3658664.3659632

This work is licensed under a Creative Commons Attribution International 4.0 License.

IH&MMSec '24, June 24–26, 2024, Baiona, Spain
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0637-0/24/06
https://doi.org/10.1145/3658664.3659632

1 INTRODUCTION

Biometric systems are security technologies that use unique biological characteristics, such as fingerprints, facial features, iris patterns, and voice traits, to verify an individual's identity [1]. They offer a high level of security due to the uniqueness and permanence of biometric traits. Compared to traditional methods like usernames and passwords, these systems are designed to provide higher security and accuracy. However, despite their increasing security, recent research [2], [3], [4], [5] shows that biometric systems are still vulnerable to attacks. One such attack is morphing, where biometric samples of multiple individuals are merged in the signal or feature domain, enabling successful verification of all contributing individuals against the morphed identity. This can create serious security issues, particularly in applications that rely on biometric data for identity verification, such as border or access control systems.

Recent research has identified several types of morphing attacks. In [2] and [6], researchers have shown the feasibility of face morphing, where the facial images from two individuals are combined to create a single identity that can deceive facial recognition systems. Similarly, other studies [3] and [7] have shown that iris morphing at the image level is also a viable option to deceive iris recognition systems. Furthermore, researchers in [4] and [8] have demonstrated that morphing can also be used to imitate individual voices by blending the voice samples of multiple individuals, which can trick voice-based biometric systems.

In addition to the aforementioned morphing attacks, a more critical attack is associated with fingerprints, known as fingerprint morphing. Fingerprint morphing is a deceptive technique in biometrics involving the creation of a synthetic fingerprint that can match multiple genuine fingerprints, potentially compromising the security of fingerprint-based authentication systems. It is considered more critical than face, iris, or voice morphing due to its widespread use in various sectors, including smartphones, laptops, and security systems. The ease of acquiring fingerprints from various surfaces makes them a prime target for morph attacks. In general, the process of fingerprint morphing involves several steps, including collecting genuine fingerprint images from multiple sources. These images are then processed to enhance their quality for morphing. Important features such as minutiae details, local ridge orientations, and ridge frequencies are extracted from each pre-processed fingerprint. Various image manipulation techniques are used to combine these extracted features from different fingerprint images, resulting in a

new synthetic fingerprint that resembles the source fingerprints. Additional processing is done to enhance the appearance of the synthetic fingerprint, making it more realistic. Finally, the morphed fingerprint is added to the biometric reference database by converting it into a compatible format and adding it as a new user identity or replacing an existing fingerprint. The ultimate goal of this process is to create a morphed fingerprint that can be used to mislead a fingerprint recognition system. Researchers in [9], [5], and [10] have demonstrated that it is possible to create double-identity fingerprints by morphing two fingerprints.

Two main approaches for fingerprint morphing have been presented: Model-based minutiae-oriented approach [5] and data-driven GAN-based approach [10]. The double-identity fingerprints generated by the model-based minutiae-oriented approach require additional post-processing to achieve a realistic appearance. In contrast, the double-identity fingerprints generated by the data-driven GAN-based approach exhibit a high degree of realism. Yet, their successful match with both original fingerprints is not assured unless the identity information is explicitly included in the generation process. The main objective of this work is to address these research gaps by developing an algorithm that generates double-identity fingerprints, which are more realistic and have a higher matching rate against their original fingerprints.

As more fingerprints are involved in the morphing process, it becomes challenging to maintain the realism and authenticity of a morphed fingerprint. Each additional fingerprint adds unique features that must be integrated seamlessly into the morphed fingerprint. This challenge has further motivated us to research and develop an algorithm to generate multi-identity fingerprints.

Our quality measures for the generation of morphed fingerprints are derived from [11]. Here we mainly focus on (a) realistic appearance (R) by using the evaluation metric NFIQ2 (Section 4.2), (b) sufficient high image resolution (I) by using a resolution of 512×512 pixels, (c) reflection of basic characteristics (B) of ground truth (training) data by performing a model-based data-driven fingerprint morphing with quality checks of sufficient minutiae, best alignment, sub-optimal selection of distinct regions and controlled minutiae map creation (Section 3) and (d) also considering data anonymity (A) by studying recognition failures as a measure for anonymity (Section 4.2). Our implementation is available at https://github.com/meghanaraobn/GAN-based-Minutiae-driven-Fingerprint-Morphing. The main contributions of this work are:

- Introduction of a novel approach that combines model-based minutiae-oriented and data-driven GAN-based approaches to morph two fingerprints.
- Extension of initially developed approach to check the feasibility of morphing three fingerprints.
- Evaluation of visual quality and morphing attack potential of generated double-identity and triple-identity fingerprints.

2 RELATED WORK

2.1 Fingerprint Reconstruction

The reconstruction of fingerprints can be accomplished through model-based approaches, which involve the use of pre-defined mathematical models. Historically, it was believed that a minutiae-based template did not contain enough information to reconstruct the original fingerprint. However, Cappelli et al. [12] proposed a model-based approach that uses minutiae information stored as ISO/IEC 19794-2 templates [13] for reconstructing fingerprint images. Ross et al. [14] proposed a new method incorporating orientation field, class information, and friction ridge structure from the minutiae template to reconstruct fingerprint images. In their research, Feng et al. [15] proposed a method to reconstruct fingerprint images from its minutiae template with reduced inclusion of spurious minutiae. They converted minutiae into continuous and spiral phases and the fingerprints were reconstructed by combining these two phases. Li et al. [16] proposed a method for reconstructing a complete fingerprint image from minutiae using the AM-FM model that produces fingerprints with fewer artifacts and spurious minutiae points. Various standard tools like SFinGe [17] and Anguli [18] can generate fingerprints similar to those acquired by biometric scanners.

Although all proposed model-based approaches successfully reconstruct fingerprint images that match their original fingerprints, they lack the ability to produce realistic fingerprint images.

As model-based generation approaches struggle to capture the realistic appearance of fingerprints, data-driven generation methods are gaining popularity. Kim et al. [19] and Makrushin et al. [20] proposed algorithms to reconstruct fingerprint images from sets of minutiae using conditional GANs. Both studies introduced new methods to encode minutiae and used the pix2pix network to generate realistic fingerprint images from minutiae maps. The authors showed that the proposed networks can closely resemble real fingerprints and mislead fingerprint recognition systems. In a recent study, Makrushin et al. [21] also presented a method capable of reconstructing realistic fingerprint images with high accuracy, even when trained with a low number of samples, and proposed an approach to reconstruct high-quality fingerprint images using the extended pix2pix network. Researchers have proposed methods using various generative models such as WGAN and CAE [22] [23], lightweight GAN [24], and CycleGAN [25] for synthesizing fingerprint images that resemble real ones. The proposed methods can be used to evaluate large-scale fingerprint search algorithms without privacy concerns and at a lower cost.

While GAN-based reconstructed fingerprint images may appear realistic, their accuracy relies on a large amount of high-quality data, and they exhibit poor performance when trained on low-quality or synthetic fingerprint images, limiting their generalization to real-world fingerprints.

2.2 Fingerprint Morphing

In their research on fingerprint morphing, Othman et al. [9] focused on improving the privacy of fingerprint images and enhancing the security of biometric templates. They proposed a model-based method of blending information from two different fingerprints to generate a new fingerprint using an image-level fusion technique. The process includes decomposing each fingerprint into continuous and spiral components, pre-aligning the components based on a reference point, and combining them to create a new fingerprint image incorporating characteristics from both original fingerprints. Additionally, their method is capable of preventing morphed fingerprints from matching their original fingerprints resulting in anonymous fingerprints and cancelable fingerprint

templates. However, the variation in ridge pattern orientations and fingerprint frequencies can create morphed fingerprint images that appear visually unrealistic. Therefore, selecting fingerprints for morphing requires careful consideration.

Another model-based minutiae-oriented approach by Ferrara et al. [5] focused on a different objective of creating morphed fingerprints that matched their original fingerprints. The authors studied the feasibility of generating double-identity fingerprints, which involves initially aligning the two fingerprints to ensure similarity in ridge orientations within intersecting areas. Subsequently, the optimal cutline is determined to maximize the similarity of ridge patterns around the cutline while preserving a sufficient number of minutiae from both fingerprints. The generation of double-identity fingerprints involves two methods: feature-level and image-level. In the feature-level approach, a new double-identity fingerprint is created by combining local orientations, frequencies, and minutiae from selected regions of both original fingerprints according to the estimated optimal cutline. In the image-level approach, a double-identity fingerprint is generated by fusing the selected regions of the two original fingerprints based on the estimated optimal cutline. Their experiments showed that the image-level approach generated realistic fingerprint images and proved to be more effective than the feature-level approach in terms of the success rate of attacks. However, it was acknowledged that some of the generated fingerprint images using the image-level approach may appear unrealistic due to noticeable cutlines at blending regions. In [26], the same authors investigated the detectability of double-identity fingerprints introduced in [5]. They conclude that the current algorithms are highly susceptible to creating double-identity fingerprints that may fool human examiners and suggest the use of a dedicated detection approach.

The drawback of using a model-based minutiae-oriented approach to create morphed fingerprints is that the resulting image may look unrealistic. To overcome this, Makrushin et al. [10] have suggested a GAN-based approach that utilizes StyleGAN2-ada to generate more realistic morphed fingerprints. The proposed approach consists of two neural networks, a generator, and a discriminator, trained on a large number of fingerprint images. Assuming corresponding vectors in the generator's latent space for any two images, the approach blends these vectors iteratively, producing morphed fingerprints that match the original images. Successful morphs are achieved by blending latent vectors at a 50% blending level. While visually realistic results are obtained, the authors highlight challenges in finding correct latent vectors, particularly when original fingerprints are absent in the training data. The search process is acknowledged as an unstable optimization problem, recommending extensive training or fine-tuning with original images to mitigate issues of the model getting stuck in a local minimum.

To the best of our knowledge, the current research on fingerprint morphing has only focused on morphing two fingerprint images.

3 OUR METHOD

The process of morphing two and three fingerprints is shown in Figure 1. First, we find the best alignment of the original fingerprints based on their local ridge orientations and singularities. We apply affine transformations to ensure that the singularities of all fingerprints align with each other. Once the fingerprints are aligned, we select only the overlapped regions of all fingerprints by cropping out the regions outside the overlapping area. Next, we sub-optimally select distinct regions from each fingerprint, with the criteria that the selected regions should have sufficient minutiae. We then extract minutiae from the selected regions and combine them into a single minutiae list. This list is then encoded into a gray-scale image called a minutiae map. Finally, we input this minutiae map into the trained GAN model, pix2pix, to generate the morphed fingerprints. The performed steps support the quality criteria, reflection of basic characteristics (B) of ground truth (training) data.

As the OpenCV [27] library provides a comprehensive toolkit for advanced image manipulation, all image manipulation operations on the fingerprint images are executed using OpenCV methods. The steps involved in the morphing process are described below.

3.1 Finding the Best Alignment

The process of aligning fingerprints is crucial in ensuring that the resulting morphed fingerprint appears realistic and contains identifiable patterns. The following sections explain in detail the steps involved in finding the best alignment of two and three fingerprints.

3.1.1 Best Alignment of Two Fingerprints. Aligning the two fingerprints, F_1 and F_2, involves retaining the original state of F_1 while applying affine transformations to F_2 to accurately align it with F_1. The alignment process in this study follows the approach presented by Ferrara et al. [5]. However, instead of applying all possible transformations to F_2 to find the best alignment with respect to F_1, we first identify the singularities of both F_1 and F_2 and then perform subsequent transformations to F_2. This approach significantly reduces the time required for the alignment process. It is important to note that in this study, it is essential that both F_1 and F_2 have the same basic patterns.

In the first step, for loop, whorl, and tented arch basic pattern fingerprints, local ridge orientations [28], O^1 and O^2 and segmentation masks [28], M_1 and M_2 are extracted from F_1 and F_2 respectively. We estimate O^1 and O^2 using a gradient-based technique [28] blockwize with a window size of $W \times W$ pixels (where $W = 16$) and then use these features to determine the loop, whorl, and delta singularities of both fingerprints using the Poincaré index algorithm [28]. Loop and tented arch basic pattern fingerprints have one loop singularity, while whorl basic pattern fingerprints have two loop singularities. Each loop singularity is defined by two to four points, where each point is represented by their respective x and y coordinates. We find the position of the first point of the first loop singularity (denoted as l_1^1 and indicated by a white point in Figure 2) of F_2 and align it with that of F_1 by applying the necessary translations. As plain arch basic pattern fingerprints do not have singularities, we find the center of the minimum enclosing circle of a fingerprint within the image for both F_1 and F_2, which is represented by their respective x and y coordinates (Figure 2). We then apply the necessary translations to align this center point of F_2 with that of F_1.

In the second step, we rotate F_{2t} (translated F_2) at one-degree increments, starting from -50° and progressing to 50° for loop and tented

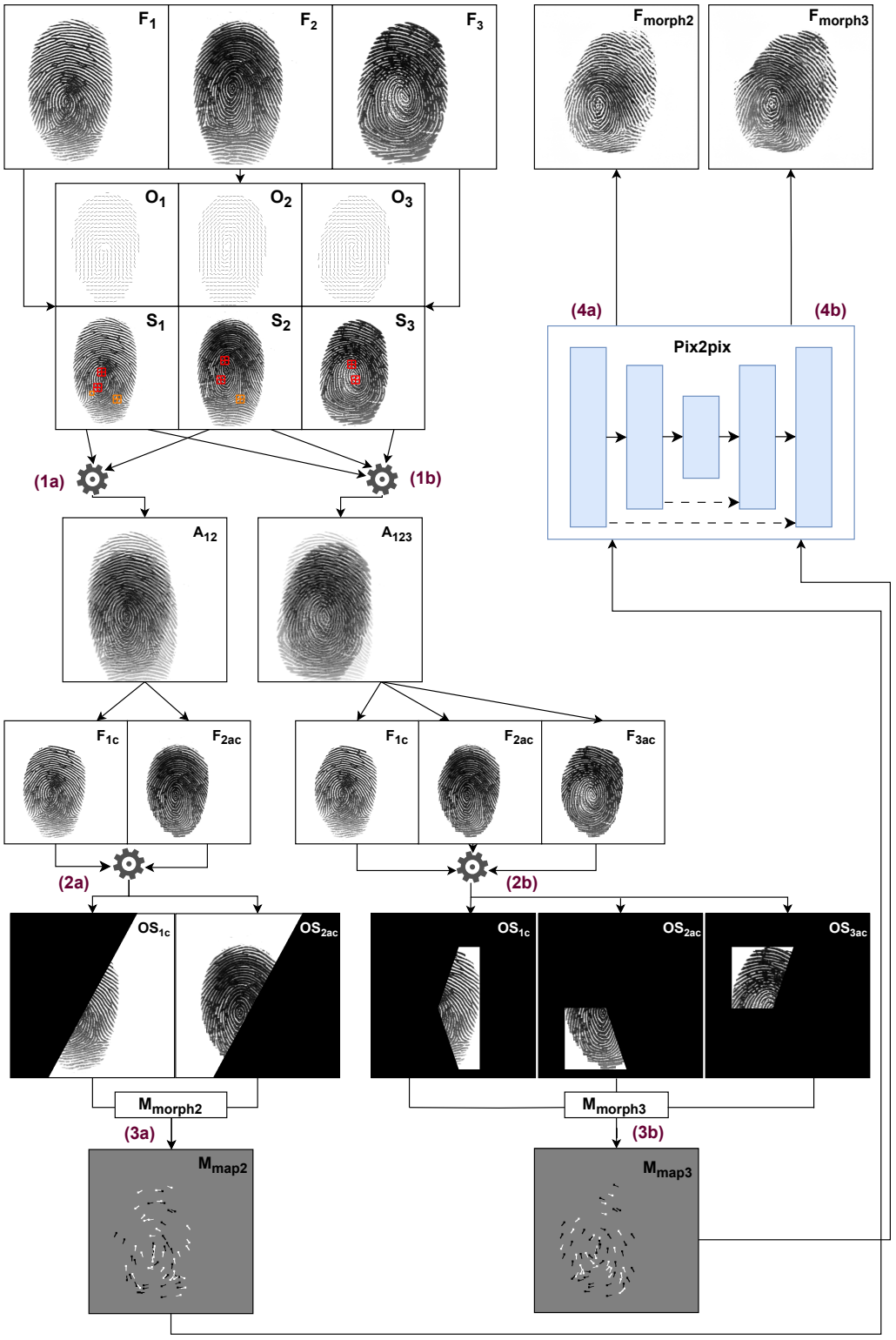

Figure 1: Schema of GAN-based Minutiae-driven fingerprint morphing. Best Alignment: (1a) - $A((O_1, S_1), (O_2, S_2))$**, (1b) -** $A((O_1, S_1), (O_2, S_2), (O_3, S_3))$**. Sub-optimal selection: (2a) -** $OS(F_{1c}, F_{2ac})$**, (2b) -** $OS(F_{1c}, F_{2ac}, F_{3ac})$**. Minutiae map creation: (3a) -** $M(M_{morph2})$**, (3b) -** $M(M_{morph3})$**. Morphed fingerprint generation: (4a) -** $G(M_{map2})$**, (4b) -** $G(M_{map3})$**.**

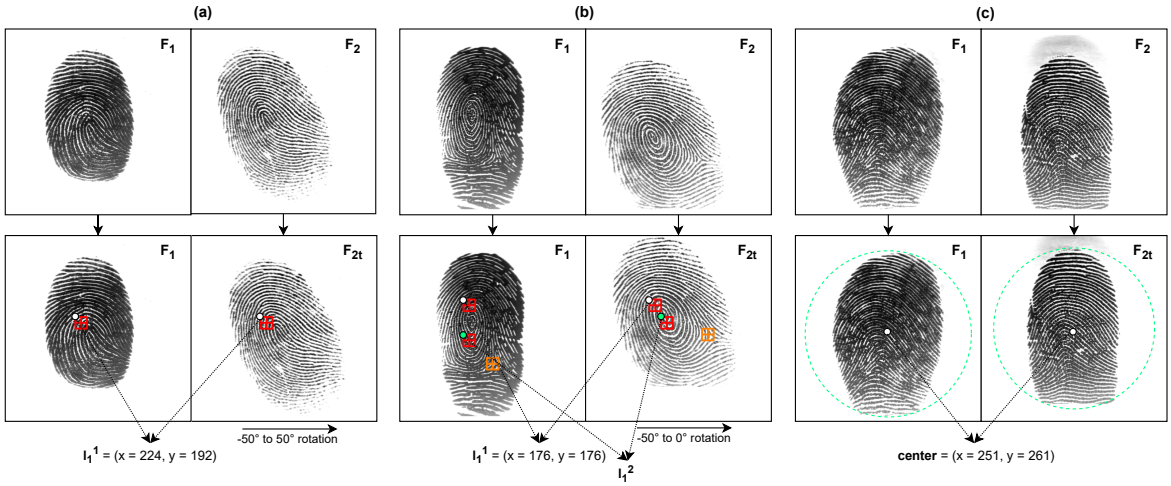

Figure 2: Initial translation process on (a) Loop, (b) Whorl, (c) Plain arch basic pattern fingerprints. F_{2t} - translated F_2.

arch basic pattern fingerprints. However, for whorl basic pattern fingerprints, the process is slightly different. We first locate the position of the first point of the second loop singularity (denoted as l_1^2 and indicated by a green point in Figure 2) of both F_1 and F_{2t}. If this point of F_{2t} is to the left of that of F_1, we rotate F_{2t} from 0° to 50°. Conversely, if it is to the right, we rotate F_{2t} from -50° to 0°. This distinction is made to optimize efficiency by reducing unnecessary rotation steps. It can only be applied to whorl patterns, as they inherently consist of two loops close to each other. At each rotation, we perform the following steps:

- When F_{2t} is rotated, its l_1^1 no longer aligns with that of F_1. Therefore, we need to re-calculate the position of l_1^1 of F_{2t} and apply the required translations to ensure that it aligns with that of F_1. This process is required to position the loop singularities of F_1 and F_{2t} as closely as possible.
- We extract the local ridge orientations O^2 from the translated F_{2t}. We calculate a similarity score following the methodology described in [5] of F_1 and F_{2t} using O^2 and initially extracted O^1 from F_1.

After each rotation, we store the similarity score, translation values (t_x and t_y), and the rotation angle of F_{2t} in a list. We then choose the configuration with the highest similarity score from the list and apply the corresponding translations and rotations to F_{2t}. This results in F_{2rt}, which has loop singularities closer to those of F_1. The process of determining the initial optimal rotation angle step is skipped for plain arch basic pattern fingerprints.
In the third step, for all basic pattern fingerprints, both translations and rotations are applied to F_{2rt} (or F_{2t} in the case of plain arch patterns) to achieve the best alignment with F_1. To apply translation, we shift the image along both x and y axes, ranging from -5 to 5 units. During each translation step, we rotate F_{2rt} from -5° to 5° for loop, whorl, and tented arch basic pattern fingerprints. However, for arch basic pattern fingerprints, F_{2t} is rotated from -30° to 30°. In each rotation-translation iteration, we extract the local ridge orientations O^2, from F_{2rt} (or F_{2t} for arch patterns). Subsequently, we calculate a similarity score of F_1 and F_{2rt} (or F_{2t} for plain arch patterns) using O^2 and initially extracted O^1 from F_1. We store the resulting similarity score, translation values, and rotation angle in a list. We then pick the configuration with the highest similarity score from the list and apply the corresponding translations and rotations to F_{2rt} (or F_{2t} for plain arch), thereby obtaining F_{2a}.
In the final step, we crop both F_1 and F_{2a} regions that are not present in the overlapping regions as shown in Figure 3. The resulting fingerprints F_{1c} and F_{2ac} will be used in the subsequent steps following the alignment process.

3.1.2 Best Alignment of Three Fingerprints. Aligning the three fingerprints, F_1, F_2, and F_3 involves retaining the original state of F_1 while applying affine transformations to F_2 and F_3 to align them with F_1 accurately. All the steps used for finding the best alignment of F_2 with F_1 and F_3 with F_1 are consistent with those used in 3.1.1. The resulting fingerprints F_{1c}, F_{2ac} and F_{3ac} will be used in the subsequent steps following the alignment process.
The sample results from the best alignment of two and three fingerprints are shown in Figure 3.

3.2 Sub-optimal Selection of Distinct Regions

Once the fingerprints are aligned, the next important step is to optimally select distinct regions from each fingerprint. These regions should have a sufficient amount of local features, specifically minutiae, which are essential for creating a morphed fingerprint with a higher probability of matching the original fingerprints.

3.2.1 Sub-optimal Selection from Two Fingerprints. The process of the optimal selection of distinct regions from two fingerprints is inspired by the idea presented by Ferrara et al. [5].
We start the process by extracting minutiae from both fingerprints using VeriFinger tool [29] and append them to two separate minutiae lists: M_1 for F_{1c} and M_2 for F_{2ac}. To select different regions from both fingerprints, we divide each image into two halves.
We first create a mask image I_m with the same dimensions as F_{1c} and F_{2ac} and initialize it with 0 (black) pixels. We define a set of continuous points P on I_m, as shown in Figure 4, and fill the curve

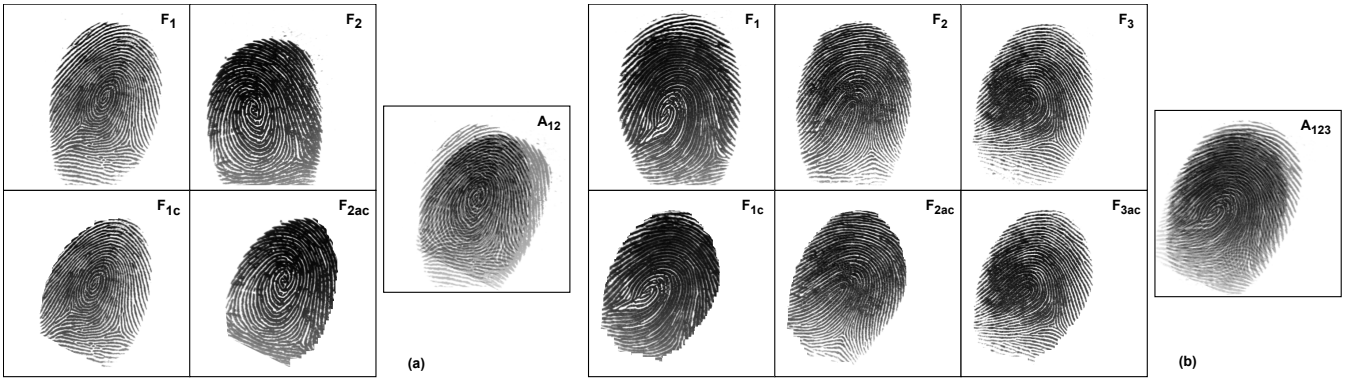

Figure 3: Best alignment results of (a) Two and (b) Three fingerprints. A_{12} **and** A_{123} **are the alignment representations.** F_{1c}**,** F_{2ac} **and** F_{3ac} **are the cropped fingerprints after alignment.**

connecting these points with 255 (white) pixels. We use this mask image as a reference image to select regions from one fingerprint corresponding to areas with white pixels on I_m and regions from the second fingerprint corresponding to areas with black pixels on I_m. We define a set of continuous points, P, iteratively on I_m such that the dividing line progresses horizontally and vertically across I_m, passing through its center. At each iteration, we perform the following steps:

- We draw a curve that connects all continuous points in P with white pixels. The resulting I_m will have one half filled with black pixels and the other half filled with white pixels.
- We select the region of F_{1c} that corresponds to the white pixel area of I_m and region of F_{2ac} that corresponds to the black pixel area of I_m. We then use the initially extracted minutiae lists, M_1 from F_{1c} and M_2 from F_{2ac}, and filter them. Each minutia extracted will contain its positional information, represented by X and Y coordinates. Using this information, we filter out minutiae in M_1 that are positioned at the black pixel area of I_m and filter out the minutiae in M_2 that are positioned at the white pixel area of I_m. Consequently, we create two distinct minutiae lists: M_{1f} with the filtered minutiae of F_{1c} and M_{2f} with the filtered minutiae of F_{2ac}.
- Simultaneously, we also select F_{1c} region that is located at the black pixel area of I_m and select the F_{2ac} region that is located at the white pixel area of I_m. We apply the same filtering procedure and create M_{1f} and M_{2f} minutiae lists.

After every iteration, we store the filtered minutiae lists M_{1f} and M_{2f}. Our next step is to choose the combination with the highest number of minutiae in both M_{1f} and M_{2f}, given that each count is greater than 12. Finally, we merge the selected M_{1f} and M_{2f} into a single minutiae list called M_{morph}.

3.2.2 Sub-optimal Selection from Three Fingerprints. Similar to the process explained in 3.2.1, we create minutiae lists: M_1 for F_{1c}, M_2 for F_{2ac}, and M_3 for F_{3ac}, which will be used in the further steps. When dividing an image into more than two parts, it is ideal to focus only on the area containing the fingerprint. To do this, we find the bounding box of the fingerprint within the image, as shown in Figure 5. Since all three fingerprints are aligned, and only their

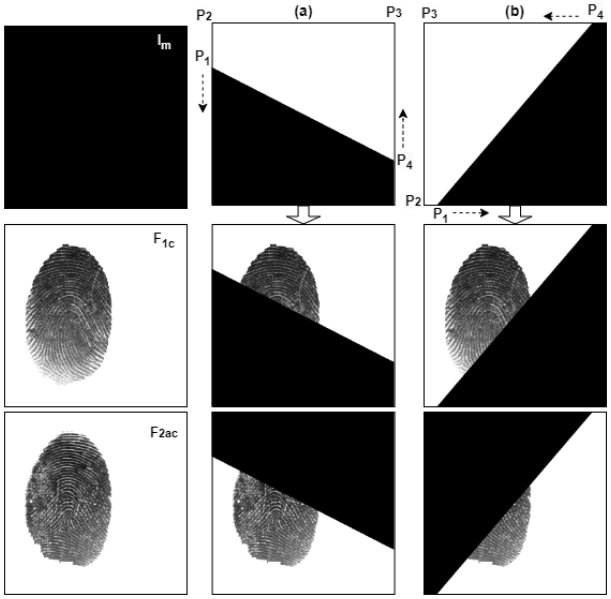

Figure 4: Sub-optimal selection process from two fingerprints. I_m **is the mask image.** p_1**,** p_2**,** p_3 **and** p_4 **are the points defined on** I_m**. (a) Horizontal (b) Vertical diving line progression.**

overlapping regions are considered, the bounding boxes of all three fingerprints would be identical. Therefore, we begin by determining the bounding box of F_{1c}, which will also be the bounding box for F_{2ac} and F_{3ac}, and then select different regions within this bounding box from each fingerprint. In a manner similar to the approach discussed in 3.2.1, we begin by creating three mask images, I_m^1, I_m^2, and I_m^3, that are initialized with 0 (black) pixels. To divide a fingerprint image within the bounding box, we define four methods, as shown in Figure 5. Each method defines three sets of continuous points: P_1, P_2, and P_3 on all three fingerprint images. Each point in P_1, P_2, and P_3 is defined by its x and y coordinates. When these sets of points are connected, they represent three different regions inside the bounding box. Our goal is to select one region from each

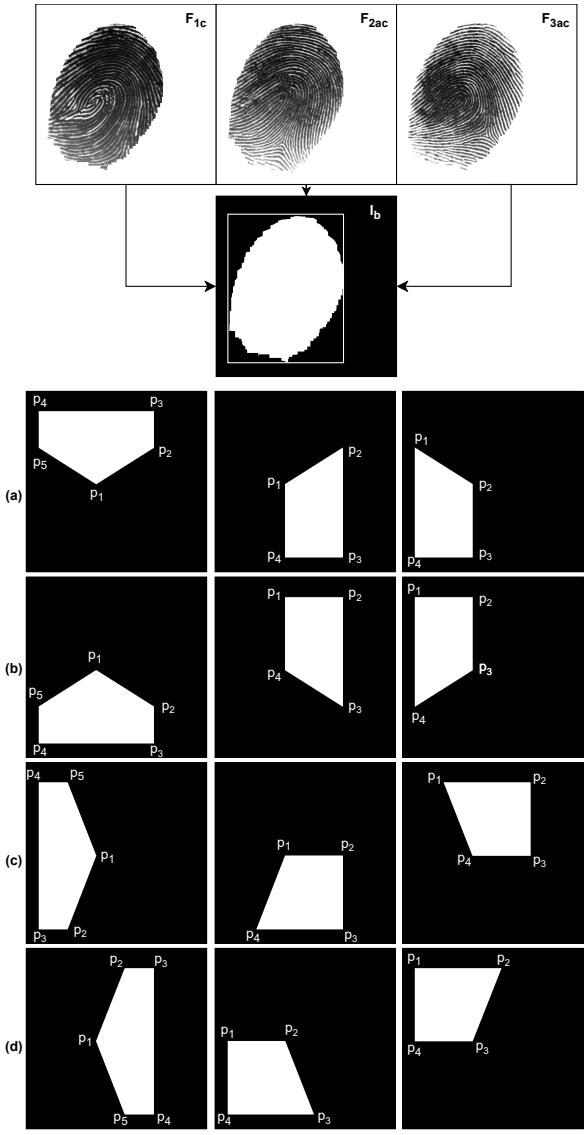

Figure 5: Bounding box and sub-optimal selection process from three fingerprints. (a), (b), (c), and (d) are defined methods. p_1, p_2, p_3, p_4 and p_5 are points defined on mask images.

fingerprint. To select distinct regions from each fingerprint, we follow the below steps for each of the defined methods:

- We connect all the continuous points in P_1 with white pixels on the mask image I_m^1. The resulting I_m^1 will have only the P_1 region filled with white pixels, as shown in Figure 5. We then select the region from F_{1c} that corresponds to the white pixel area of I_m^1. Likewise, we connect the points in P_2 and P_3 with white pixels on I_m^2 and I_m^3 and select the corresponding white pixel area from F_{2ac} and F_{3ac} respectively.
- We filter out minutiae in M_1, M_2, and M_3 that are positioned at the black pixel area of I_m^1, I_m^2, and I_m^3, respectively. We then create three distinct minutiae lists: M_{1f}, M_{2f} and M_{3f}, which include the filtered minutiae of F_{1c}, F_{2ac} and F_{3ac}, respectively.
- We repeat the same process by changing the P_1, P_2 and P_3 regions selected from each fingerprint.

After each iteration, we store M_{1f}, M_{2f} and M_{3f}. Then, we select a combination of three that has the highest number of minutiae in each of them. Finally, we merge the selected M_{1f}, M_{2f} and M_{3f} into a single list of minutiae called M_{morph}.
The sample results of the sub-optimal selection of distinct regions from two and three fingerprints are shown in Figure 6.

3.3 Creation of Minutiae Map

Using the combined minutiae list, M_{morph}, we encode all the minutiae information onto an image called a minutiae map, which is of the same size as the fingerprint images. There are several methods for encoding minutiae, which include gray squares [19], directed lines [20], and pointing minutiae [21].
According to the authors in [21], encoding methods for directed lines and pointing minutiae effectively capture the complementary characteristics of bifurcations and endings. However, their experiments show that pointing minutiae encoding outperforms directed lines. Therefore, we have opted to use the pointing minutiae encoding method from [21] to create a minutiae map M_{map} from M_{morph}.
The sample results of the minutiae map creation using pointing minutiae encoding from M_{morph} are shown in Figure 6.

3.4 Generation of Morphed Fingerprint

The final step involves utilizing M_{map} as input for a GAN model to generate morphed fingerprints F_{morph}. In this study, the publicly available modified pix2pix network [21], cloned from gensynth-pix2pix is used to generate morphed fingerprints.
We have chosen to use the pix2pix network [30], a conditional GAN, well-suited for image-to-image translation tasks. The pix2pix network consists of two networks, the generator G and discriminator D, trained in an adversarial manner.
In this study, transforming the minutiae map M_{map} into a morphed fingerprint F_{morph} that matches the original fingerprints is crucial. The generator G plays a vital role in achieving this, using a U-Net architecture [31]. In contrast to other approaches that use an encoder-decoder network to solve image-to-image translation problems, the U-Net architecture addresses the challenge of missing information from the input image by using skip connections to share information between parallel layers.
Unlike a traditional GAN discriminator that processes the entire input and classifies it as real or fake, the PatchGAN discriminator used in this study processes the input in patches. The image is divided into patches of $N \times N$ size, and the discriminator checks if each patch is real or fake by running it convolutionally across the entire image. The output is obtained by averaging the responses obtained from the discriminator for all the patches.
During the training process, the generator translates a minutiae map into a fingerprint image. The discriminator, on the other hand, evaluates a tensor composed of both the fingerprint image and the minutiae map, which serves as a conditional input. After the training process, the discriminator is no longer utilized. Only the generator is used for generating morphed fingerprints from M_{map}.

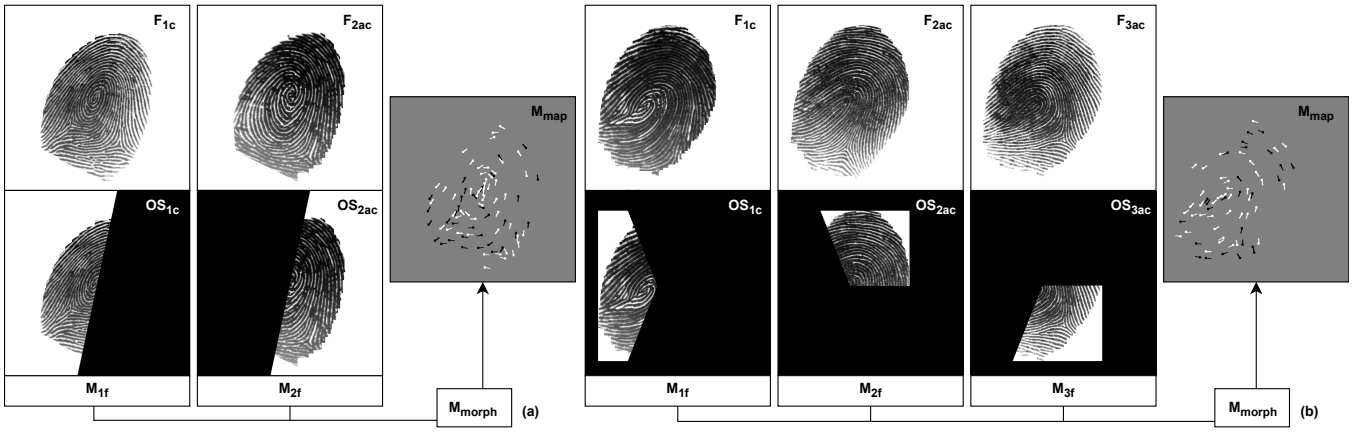

Figure 6: Sub-optimal selection and minutiae map creation results of (a) Two and (b) Three fingerprints. OS_{1c}, OS_{2ac} **and** OS_{3ac} **are sub-optimal selected regions.** M_{morph} **is the combined minutiae list.** M_{map} **is the minutiae map.**

The original version of the pix2pix architecture was designed to handle images with a size of 256×256 pixels. To ensure sufficient high image resolution (I), we worked with fingerprint images having a resolution of 512×512 pixels. For this, we used a modified pix2pix network by [21], where the authors extended the original network by adding an additional convolutional layer to both the generator and the discriminator. This modification eliminated the need to down-scale high-resolution images, preserving the important details of fingerprints.

In our experiments, we use pix2pix model snapshots after 15, 30, and 55 training epochs. Note that the pix2pix models have been trained with fingerprint images acquired with a CrossMatch sensor. Hence all the generated images have a similar appearance to those captured by a CrossMatch sensor.

4 EVALUATION

4.1 Experimental Datasets

We use the CrossMatch DB1 A+B dataset from the Third International Fingerprint Verification Competition (FVC2004) [32] for both fingerprint morphing and evaluation of morphed fingerprints. Each fingerprint image is of dimension 640×480. The dataset has 880 images of fingerprints, featuring eight impressions each from 110 different fingers. Necessary cropping and padding operations are performed to reduce the fingerprint images to 512×512 dimensions. An impression of each finger is used to generate morphed fingerprints while the remaining seven impressions are used for testing. Such a testing scenario better simulates real-life attacks because a fingerprint impression acquired during the verification will be different from the one used during the morphing process. Two datasets $D2$ and $D3$ are created for morphing two and three fingerprints respectively and total sample combinations used in our experiments are shown in Table 1.

4.2 Evaluation Metrics

We consider two metrics in our experiments, one is used to evaluate the realistic appearance of morphs, and the other to evaluate the threat posed by morphs to fingerprint matching systems.

To assess the threat posed by morphs, we calculate the morphing success defined as the ratio of multi-identity (double- or triple-identity) fingerprints in all morphed fingerprints. For instance, double-identity fingerprints should match as many impressions as possible of the two real fingerprints that took part in the morphing procedure. Note that, if the morphed fingerprint matches only one constituent fingerprint, this morph cannot be seen as successful. We use two fingerprint matchers: VeriFinger and MCC. The VeriFinger scores range from 0 to infinity. The commonly used VeriFinger decision thresholds are 36, and 48 which correspond to the False Accept Rate (FAR) of 0.1% and 0.01% respectively. We further refer to FAR values at these thresholds as FAR1000 and FAR10000. The MCC scores range from 0 to 1. The decision thresholds for FAR1000 and FAR10000 are 0.1205 and 0.1329 respectively.

We apply the metric called the Morphing Attack Potential (MAP) introduced in [33]. The morphing success is measured here for the increasing number of fingerprint matchers, while the number of original fingerprint impressions to be matched also increases. MAP is drawn as a table for a particular FAR level.

The realistic appearance (R) of morphed fingerprints is measured indirectly by calculating the NFIQ2 scores. NFIQ2 is a fingerprint quality metric that adheres to the international standard of biometric sample quality ISO/IEC 29794-1:2016 [34] and is designed to predict the usability of a fingerprint for user authentication purposes. It has been observed that NFIQ2 can also serve as an indicator of the realistic appearance since it correlates well with the visual quality. The NFIQ2 scores range from 0 to 100. Higher values indicate higher utility. Scores below six indicate useless fingerprints, while scores above 35 correspond to perfectly useful fingerprints. Scores above 45 indicate perfect fingerprint patterns.

Table 1: Total sample combinations in dataset $D2$ **and** $D3$**.**

Datasets	Loop	Whorl	Arch	Total
D2	2411	2333	1316	6060
D3	440	560	206	1206

4.3 Results

Figure 7 displays sample morphed fingerprints: (a) and (b) show double-identity and triple-identity fingerprints respectively that match their corresponding original fingerprints.

4.3.1 Morphing Attack Potential. Table 2 demonstrates the MAP values for morphed fingerprints. Since, we have morphed fingerprints with the same basic pattern, we first report the MAP values for loops, whorls and archs separately. Then, the "overall" section reports aggregated values for all patterns. The "M1" columns show the ratio of successfully matched morphs with at least one fingerprint matching algorithm, while the "M1+M2" columns show the ratio of successfully matched morphs with both algorithms. The rows 1, 2, .., 7 denote the lowest number of probe fingerprint images, that have been matched successfully.

For example, looking at the section "overall", row "1", columns "30 epochs" and "M1", the value of 46.32% means that this percentage of all generated morphs fool at least one fingerprint matching algorithm with at least one out of seven probe images for the two constituent fingers. The remaining 54.68% morphs are not able to fool any of the addressed fingerprint matching algorithms. In our considerations, these morphs are seen as anonymous fingerprints addressing data anonymity (A). The value of 4.42% in the section "overall", row "3", columns "30 epochs" and "M1+M2" means that only 4.42% of all generated morphs fool both fingerprint matching algorithms with at least three out of seven probe images.

For loops and whorls, the pix2pix snapshots at the 30th epoch are the best, followed by the snapshots at the 15th and 55th epochs. For archs, the pix2pix snapshot at the 15th epoch is the best, followed by the snapshots at the 30th and 55th epochs. The "overall" dynamic is similar to loops and whorls with the 30th epoch as the best one followed by the 15th and 55th epochs. Note that the difference between snapshots at the 15th and 30th epochs is very low while the snapshots at the 55th epochs perform significantly worse.

As it can be seen in Table 2, the resulting morphs are not perfect: not all generated morphs have the potential to fool a fingerprint-matching system. However, it is important that no compatibility check between original fingerprints has been done before morphing except that the fingerprints have the same basic pattern.

The reason for a quick degradation of the morphing success if matching with one, two, three and so on impressions is that the fingerprint is not always completely presented on an image and the morphing procedure takes into account only a part of the original fingerprint with a "sufficient" number of minutiae. Hence, the minutiae presented in the morphed fingerprint may not be presented on a different impression of the original fingerprint at all, making successful fingerprint matching impossible.

The reason for the degradation of the morphing success if matching with one and two fingerprint matchers is not obvious. The possible explanation might be that the fingerprint matchers rely on completely different clues.

The overall low MAP values are caused not only by imperfections in the fingerprint morphing procedure but also by imperfections in fingerprint reconstruction from minutiae and imperfections in the fingerprint matching algorithms addressed.

Table 3 presents the result of morphing three fingerprints. The MAP values in the table suggest that it is very improbable to create a successful morph from three fingerprints unless the constituent original fingerprints are carefully selected. If we invert the values in the row "1", and column "M1", we get the number of anonymous fingerprints resulting from the morphing procedure. Even though creating anonymous fingerprints is not our goal, we can state that our algorithm for morphing three fingerprints creates anonymous fingerprints in approximately 90% cases, surely only in case the resulting morphed fingerprints appear realistic.

Table 2: MAP for Two Fingerprints Morphing. The MAP values are given at the FAR1000 decision thresholds (Verifinger: 36, MCC: 0.1205).

	15 epochs		30 epochs		55 epochs	
	M1	**M1+M2**	**M1**	**M1+M2**	**M1**	**M1+M2**
average of left and right loops						
1	53.61%	21.87%	55.17%	23.79%	47.18%	16.43%
2	40.17%	11.19%	42.27%	12.90%	33.71%	8.08%
3	29.97%	5.50%	33.24%	6.90%	25.06%	4.25%
4	21.94%	2.38%	23.89%	2.87%	18.22%	1.63%
5	13.11%	0.80%	15.18%	0.94%	10.94%	0.51%
6	6.01%	0.13%	6.54%	0.25%	4.98%	0.04%
7	1.06%	0.00%	1.36%	0.00%	0.93%	0.00%
whorls						
1	40.08%	13.12%	45.61%	16.50%	41.58%	11.53%
2	27.52%	4.59%	32.83%	7.46%	30.69%	4.37%
3	19.59%	1.89%	25.80%	3.69%	22.93%	1.93%
4	14.06%	0.94%	19.16%	1.71%	16.59%	0.60%
5	8.66%	0.30%	12.73%	0.47%	10.46%	0.13%
6	4.41%	0.00%	6.43%	0.04%	4.71%	0.04%
7	0.26%	0.00%	0.64%	0.00%	0.43%	0.00%
average of archs and tented archs						
1	39.86%	10.70%	35.52%	8.23%	27.10%	5.69%
2	28.93%	4.84%	23.91%	3.52%	17.01%	2.92%
3	22.01%	2.80%	18.26%	1.36%	12.64%	1.19%
4	14.78%	1.19%	11.95%	1.06%	8.62%	0.42%
5	8.90%	0.38%	8.48%	0.71%	6.08%	0.00%
6	3.55%	0.00%	3.00%	0.00%	2.61%	0.00%
7	0.00%	0.00%	0.13%	0.00%	0.38%	0.00%
overall						
1	44.24%	16.22%	46.32%	17.66%	40.05%	12.31%
2	31.75%	7.36%	33.81%	8.71%	28.28%	5.41%
3	22.97%	3.51%	26.14%	4.42%	20.86%	2.64%
4	16.35%	1.53%	18.70%	1.96%	14.95%	0.92%
5	9.79%	0.46%	12.00%	0.59%	9.21%	0.25%
6	4.64%	0.05%	5.54%	0.12%	4.11%	0.03%
7	0.51%	0.00%	0.83%	0.00%	0.56%	0.00%

4.3.2 Ablation study. In order to better understand the sources of imperfection and improve our morphing approach in the future, we conduct two ablation studies. In the first one, we assess the fingerprint-matching performance of VeriFinger and MCC by building all possible genuine pairs and checking the ratio of matching scores that exceed the decision threshold.

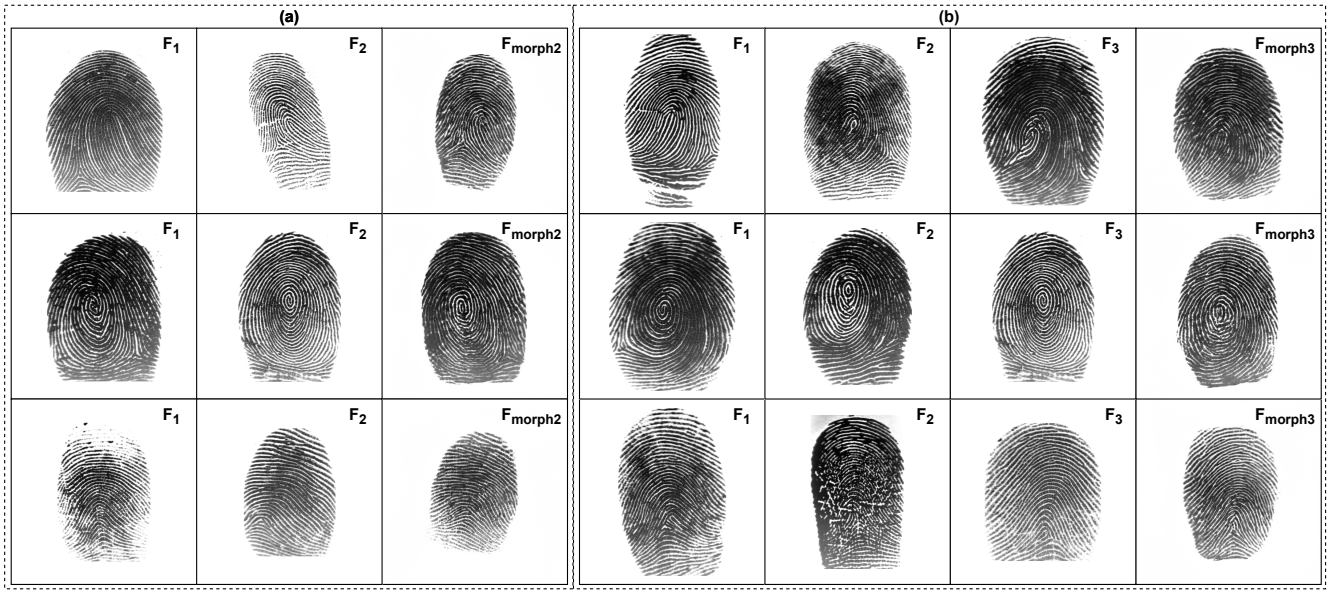

Figure 7: Sample morphed results of (a) Two and (b) Three fingerprints. F_1, F_2 and F_3 are original fingerprints. F_{morph2} are double-identity fingerprints and F_{morph3} are triple-identity fingerprints.

Table 3: MAP for Three Fingerprints Morphing. The MAP values are given at the FAR1000 decision thresholds (VeriFinger: 36, MCC: 0.1205) for overall fingerprint patterns.

	15 epochs		30 epochs		55 epochs	
	M1	M1+M2	M1	M1+M2	M1	M1+M2
1	9.45%	0.10%	11.69%	2.24%	9.78%	0.75%
2	3.81%	0.17%	5.64%	0.50%	4.98%	0.25%
3	1.91%	0.08%	2.65%	0.08%	2.24%	0.08%
4	0.91%	0.00%	1.33%	0.00%	1.16%	0.00%
5	0.33%	0.00%	0.41%	0.00%	0.50%	0.00%
6	0.08%	0.00%	0.00%	0.00%	0.25%	0.00%
7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

In the second ablation study, we assess the reconstruction performance of our pix2pix models. To this end, we repeat the experiment from the first ablation study, replacing one of the original impressions in each genuine pair with its reconstructed counterpart.
Table 4 reports the True Accept Rates (TAR) at three decision thresholds corresponding to FAR of 1%, 0.1%, and 0.01%. The results of "Original vs Original" comparisons give us an idea about the ability of fingerprint matchers to fairly judge the attack potential caused by morphs. If a fingerprint matcher is not able to match samples in all genuine pairs, we should not expect that it matches morphed fingerprints against all constituent fingerprints. We can also see that reconstruction of fingerprints from minutiae changes the minutiae co-allocation sometimes prohibiting the successful matching with original impressions of a fingerprint. The TAR values at FAR=0.1% (the reference decision threshold addressed in Tables 2 and 3) can be seen as the upper bound for the MAP values presented in the row "1", column "M1" for the "overall" case in Tables 2 and 3. If we take the pix2pix model snapshot after the 30th training epoch, we see that only 89.74% genuine pairs can be recognized as such by VeriFinger and only 63.2% by MCC. If we take a fingerprint morph perfectly representing the minutiae structure from all constituent fingerprints, there is more than 10% probability that this morph will be rejected by VeriFinger and more than 36% probability that this morph will be rejected by MCC. The probability that both systems accept this perfect morph is a product of the TAR values. It yields only 56.72% which is the upper bound for the MAP values presented in row "1", column "M1+M2" for the "overall" case in Tables 2 and 3.
The results of comparing the generated morphed fingerprints with their two original fingerprints are graphically represented in Figure 8. The first graph displays a scatter plot of VeriFinger and MCC scores, while the second graph is a line graph that shows the matching success rate of the morphed fingerprints based on the decision threshold of VeriFinger and MCC for 30 training epochs.
The scatter plot graph displays dots in three distinct colors. Green dots correspond to double-identity fingerprints. Orange dots represent partial-identity fingerprints. Red dots indicate virtual-identity (anonymous) fingerprints. The dotted lines of different colors signify the two decision thresholds of VeriFinger and MCC.
The line graph has two lines: green for double-identity and red for virtual-identity fingerprints. The graph demonstrates that as the decision threshold increases, the percentage of double-identity fingerprints decreases. At a specific decision threshold, these two lines intersect, where the percentage of double-identity fingerprints and virtual-identity fingerprints are equal. This happens when the VeriFinger decision threshold is 48.5 and the MCC decision threshold is 0.1006. Before this decision threshold, the percentage of double-identity fingerprints is higher. However, after this decision threshold, the percentage of virtual-identity fingerprints increases. Note that this analysis does not include partial-identity fingerprints.

Table 4: Ablation study. FAR100: VF 24, MCC 0.1083; FAR1000: VF 36, MCC 0.1205; FAR10000: VF 48, MCC 0.1329.

VeriFinger			MCC		
TAR@(FAR=1%)	TAR@(FAR=0.1%)	TAR@(FAR=0.01%)	TAR@(FAR=1%)	TAR@(FAR=0.1%)	TAR@(FAR=0.01%)
Original vs. Original					
99.81%	99.45%	98.67%	95.91%	92.66%	87.73%
Original vs. pix2pix reconstructed (15 epochs snapshot)					
94.64%	**89.89%**	82.86%	73.56%	62.40%	51.33%
Original vs. pix2pix reconstructed (30 epochs snapshot)					
94.82%	89.74%	**83.18%**	**74.06%**	**63.20%**	**52.52%**
Original vs. pix2pix reconstructed (55 epochs snapshot)					
89.48%	82.79%	75.91%	64.09%	53.33%	43.00%

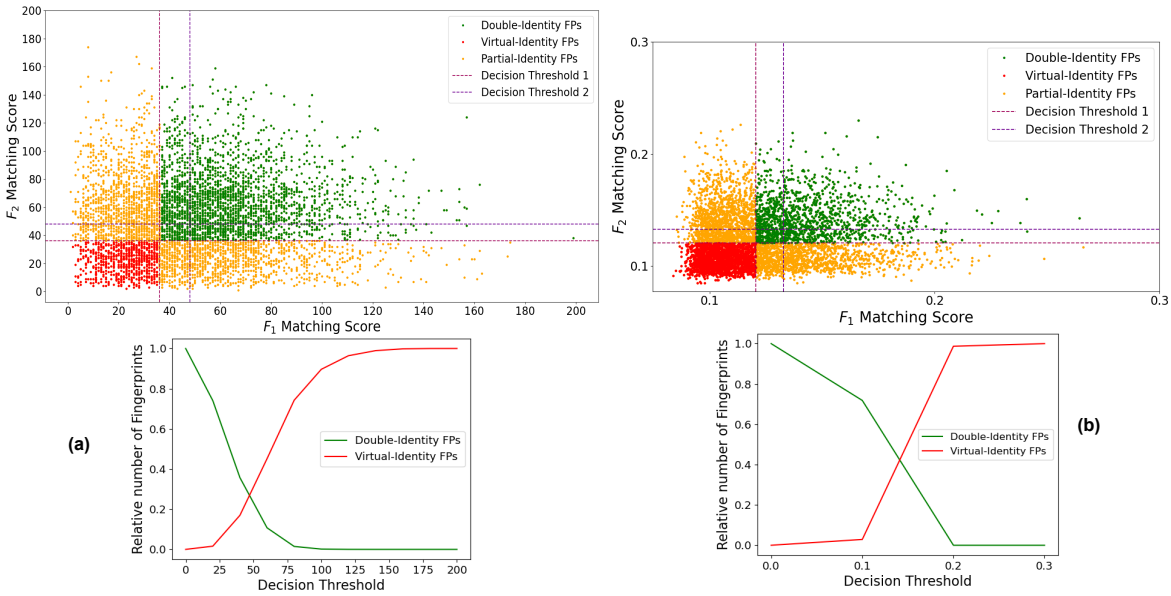

Figure 8: Graphical representations of (a) VeriFinger (b) MCC scores of two morphed fingerprints for the 30 epochs snapshot.

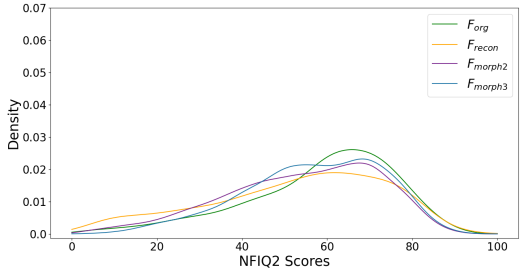

Figure 9: NFIQ2 scores distributions.

Figure 9, the probability density graph shows the distributions of NFIQ2 scores of original, reconstructed, and morphed fingerprints (for 30 training epochs) to measure the realistic appearance (R). The NFIQ2 scores of the morphed fingerprints are on average slightly lower than those of the original fingerprints. However, most morphed fingerprints still have NFIQ2 scores greater than 35, which we interpret as a high visual quality and a realistic appearance (R).

5 COMPARATIVE OVERVIEW

Although the morphing attack potential of our morphed fingerprints is lower than those in [26], our approach offers far more flexibility in combining the fingerprints. For instance, the approach introduced in [9] requires a careful selection of fingerprints for morphing. In contrast, we do not select fingerprints that are suitable for morphing with each other. We morph all possible pairs with the same basic pattern even if the original fingerprint is only partially presented and contains a very low number of minutiae.

Even though we have not demonstrated it in experiments, our approach is not limited to morphing fingerprints captured by the same sensor which is the major limitation of the image-based approach in [5]. Note that the feature-based approach from [5] can easily overcome this limitation but falls short in creating realistic patterns. In comparison with the approach in [10], we take control of minutiae in the morphed fingerprint which makes the tedious iterative search for latent representations of the original fingerprints in the latent space of the GAN generator obsolete.

If we use a better pix2pix reconstruction model and add the quality

check of original fingerprints used for morphing by simply requiring a sufficient number of minutiae, the morphing attack potential will grow significantly.

6 CONCLUSION

Our fingerprint morphing approach introduced combines minutiae-oriented and GAN-based approaches to create double- and triple-identity fingerprints aiming at deceiving fingerprint matching algorithms i.e. forcing them to match the morphed fingerprint (biometric template) with several different fingerprints (probe samples).
We have addressed the limits of the existing algorithms which are either the inability to generate realistic morphs, to combine fingerprint images from different acquisition devices, or to integrate the minutiae co-allocation into the morphing process.
We have demonstrated the ability of our algorithm to create double-identity fingerprints without a careful pre-selection of suitable fingerprint pairs. Our approach for the creation of triple-identity fingerprints has rather turned out to be a generation of anonymous fingerprints with approx. 10% of triple-identity fingerprints and approx. 90% of anonymous fingerprints. In summary, we have addressed four requirements for synthetic biometric data: realistic appearance (R), sufficient high image resolution (I), reflection of basic characteristics of ground truth (training) data (B), and data anonymity (A). In our ablation studies, we figured out that the reasons for the low ratio of multi-identity fingerprints beyond the morphing algorithm itself are the fingerprint reconstruction errors of the pix2pix models as well as the not ideal fingerprint matching performance of the considered fingerprint recognition systems. Future work will be dedicated to the improvement of the pix2pix-based fingerprint reconstruction models by expanding the minutiae map to a tensor containing minutiae, orientation, and frequency maps and alternatives for minutiae sampling from constituent original fingerprints. In addition, we will also explore methodologies to mitigate potential attacks facilitated by our solution, along with human experiments for validation and refinement.

ACKNOWLEDGMENTS

This paper is based on research performed in the research project GENSYNTH, which has been funded in part by the Deutsche Forschungsgemeinschaft (DFG) under the grant number 421860227.

REFERENCES

[1] Kashif Shaheed, Aihua Mao, Imran Qureshi, Munish Kumar, Qaisar Abbas, Inam Ullah, and Xingming Zhang. A systematic review on physiological-based biometric recognition systems: current and future trends. *Archives of Computational Methods in Engineering*, pages 1–44, 2021.
[2] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. The magic passport. In *Proc of the IEEE Int. Joint Conference on Biometrics*, pages 1–7, 2014.
[3] Renu Sharma and Arun Ross. Image-level iris morph attack. In *Proc of the IEEE Int. Conference on Image Processing (ICIP)*, pages 3013–3017, 2021.
[4] Hui Ye and S. Young. High quality voice morphing. In *Proc of the IEEE Int. Conference on Acoustics, Speech, and Signal Processing*, volume 1, pages I–9, 2004.
[5] Matteo Ferrara, Raffaele Cappelli, and Davide Maltoni. On the feasibility of creating double-identity fingerprints. *IEEE Trans. on Information Forensics and Security*, 12(4):892–900, 2017.
[6] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, and Christoph Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE Trans. on Technology and Society*, 2(3):128–145, 2021.
[7] C. Rathgeb and C. Busch. On the feasibility of creating morphed iris-codes. In *Proc. of the IEEE Int. Joint Conference on Biometrics (IJCB)*, pages 152–157, 2017.
[8] Hui Ye and S. Young. Quality-enhanced voice morphing using maximum likelihood transformations. *IEEE Trans. on Audio, Speech, and Language Processing*, 14(4):1301–1312, 2006.
[9] Asem Othman and Arun Ross. On mixing fingerprints. *IEEE Trans. on Information Forensics and security*, 8(1):260–267, 2012.
[10] Andrey Makrushin, Mark Trebeljahr, Stefan Seidlitz, and Jana Dittmann. On feasibility of GAN-based fingerprint morphing. In *Proc of the 23rd Int. Workshop on Multimedia Signal Processing (MMSP)*, pages 1–6. IEEE, 2021.
[11] A. Makrushin, C. Kauba, S. Kirchgasser, S. Seidlitz, C. Kraetzer, A. Uhl, and J. Dittmann. General requirements on synthetic fingerprint images for biometric authentication and forensic investigations. In *Proc. of the ACM Workshop on Information Hiding and Multimedia Security*, page 93–104, 2021.
[12] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, 2007.
[13] Biometric Data Interchange Formats-Part. 6: Iris image data. *ISO/IEC*, pages 19794–6, 2005.
[14] Arun Ross, Jidnya Shah, and Anil K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.
[15] J. Feng and A. K. Jain. Fingerprint reconstruction: From minutiae to phase. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 33(2):209–223, 2011.
[16] Sheng Li and Alex C. Kot. An improved scheme for full fingerprint reconstruction. *IEEE Trans. on Information Forensics and Security*, 7(6):1906–1912, 2012.
[17] Raffaele Cappelli. SFinGe. In Stan Z. Li and Anil Jain, editors, *Encyclopedia of Biometrics*, pages 1169–1176. Springer US, Boston, MA, 2009.
[18] Afzalul Haque Ansari. Generation and storage of large synthetic fingerprint database. *ME Thesis, Jul*, 2011.
[19] H. Kim, X. Cui, M.-G. Kim, and T. H. B. Nguyen. Reconstruction of fingerprints from minutiae using conditional adversarial networks. In *Proc. of the 17th Int. Workshop on Digital Forensics and Watermarking*, pages 353–362, 2019.
[20] Andrey Makrushin, Venkata Srinath Mannam, BN Meghana Rao, and Jana Dittmann. Data-driven reconstruction of fingerprints from minutiae maps. In *Proc of the 24th Int. Workshop on Multimedia Signal Processing*, pages 1–6, 2022.
[21] Andrey Makrushin, Venkata Srinath Mannam, and Jana Dittmann. Data-driven fingerprint reconstruction from minutiae based on real and synthetic training data. In *VISIGRAPP (4: VISAPP)*, pages 229–237, 2023.
[22] Kai Cao and Anil Jain. Fingerprint synthesis: Evaluating fingerprint search at scale. In *Proc. of the 2018 Int. Conf. on Biometrics (ICB)*, pages 31–38. IEEE, 2018.
[23] V. Mistry, J. J. Engelsma, and A. K. Jain. Fingerprint synthesis: Search with 100 million prints. In *Proc of the IEEE Int. Joint Conf. on Biometrics*, pages 1–10, 2020.
[24] Masud An-Nur Islam Fahim and Ho Yub Jung. A lightweight gan network for large scale fingerprint generation. *IEEE Access*, 8:92918–92928, 2020.
[25] André Brasil Vieira Wyzykowski, Mauricio Pamplona Segundo, and Rubisley de Paula Lemes. Level three synthetic fingerprint generation. In *Proc of the 25th Int. Conf. on Pattern Recognition (ICPR)*, pages 9250–9257. IEEE, 2021.
[26] M. Ferrara, R. Cappelli, and D. Maltoni. Detecting double-identity fingerprint attacks. *IEEE Trans. on Biometrics, Behavior, and Identity Science*, 5(4):476–485, 2023.
[27] Open source computer vision library. https://opencv.org/.
[28] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer, 2 edition, 2009.
[29] Neurotechnology VeriFinger SDK. https://www.neurotechnology.com/verifinger.html, 2022.
[30] Phillip Isola, Jun-Yan Zhu, Tinghui Zhou, and Alexei A Efros. Image-to-image translation with conditional adversarial networks. In *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 1125–1134, 2017.
[31] O. Ronneberger, P. Fischer, and T. Brox. U-net: Convolutional networks for biomedical image segmentation. In *Proc of the 18th Int. Conf. on Medical Image Computing and Computer-Assisted Intervention, Part III 18*, pages 234–241, 2015.
[32] Dario Maio, Davide Maltoni, Raffaele Cappelli, Jim L Wayman, and Anil K Jain. FVC2004: Third fingerprint verification competition. In *Proc. of the Int. Conf. on Biometric Authentication*, pages 1–7, 2004.
[33] M. Ferrara, A. Franco, D. Maltoni, and C. Busch. Morphing attack potential. In *Proc. of the IEEE Int. Workshop on Biometrics and Forensics (IWBF)*, 2022.
[34] IJS Biometrics. ISO/IEC 29794-1: 2016 information technology-biometric sample quality-part 1: Framework. *International Organization for Standardization, Geneva, Switzerland*, 2016.