

Escuela Politécnica Superior

20
21

Bachelor thesis

Stegano-morphing: Concealing attacks on face identification algorithms



Luis Cárabe Fernández-Pedraza

Escuela Politécnica Superior
Universidad Autónoma de Madrid
C/ Francisco Tomás y Valiente nº 11

**UNIVERSIDAD AUTÓNOMA DE MADRID
ESCUELA POLITÉCNICA SUPERIOR**



Degree on Computer Engineering

BACHELOR THESIS

**Stegano-morphing: Concealing attacks on face
identification algorithms**

**Author: Luis Cárabe Fernández-Pedraza
Advisor: Eduardo Cermeño Mediavilla**

April 2021

All rights reserved.

No reproduction in any form of this book, in whole or in part
(except for brief quotation in critical articles or reviews),
may be made without written authorization from the publisher.

© 3 de Noviembre de 2017 by UNIVERSIDAD AUTÓNOMA DE MADRID
Francisco Tomás y Valiente, nº 1
Madrid, 28049
Spain

Luis Cárabe Fernández-Pedraza
Stegano-morphing: Concealing attacks on face identification algorithms

Luis Cárabe Fernández-Pedraza
C\ Francisco Tomás y Valiente Nº 11

PRINTED IN SPAIN

Figures don't lie, but liars figure.

Mark Twain

RESUMEN

El reconocimiento facial se está convirtiendo en una tecnología muy usada en aplicaciones de control de acceso, ya sea en el mundo real o en el virtual. Los sistemas basados en esta tecnología tienen que hacer frente a las dificultades clásicas de los algoritmos de clasificación y a los retos de los ataques de suplantación de identidad. El morphing suele ser el método preferido para estos ataques, ya que permite modificar progresivamente los rasgos de una cara a partir de un sujeto original para que se parezca gradualmente a otro. Hasta ahora, las publicaciones se han centrado en la suplantación de esta segunda persona, normalmente alguien que tiene permiso para entrar en lugares o aplicaciones restringidas. Sin embargo, en muchas otras aplicaciones no hay una lista de personas autorizadas, sino una lista negra de personas que no pueden entrar, iniciar sesión o registrarse de nuevo. En estos casos, la persona objetivo del morphing no es relevante, y el reto principal es minimizar la probabilidad de ser detectado.

Presentamos una comparación del porcentaje de identificación y el comportamiento de 5 reconocedores (Eigenfaces, Fisherfaces, LBPH, SIFT y FaceNet) contra ataques de morphing tradicionales, en los que sólo se utilizan dos sujetos para crear la imagen alterada: el sujeto original y el objetivo. También introducimos un nuevo método de morphing cuyo funcionamiento se basa en un proceso iterativo de morphing tradicional gradual, combinando el sujeto original con todas las imágenes de los sujetos en la base de datos de entrenamiento. También probamos nuestro método de ataque contra el reconocedor que obtiene mejores resultados contra el morphing tradicional (FaceNet), demostrando que, utilizando nuestro método, podemos multiplicar por ocho las posibilidades de conseguir un ataque de suplantación capaz de engañar a los algoritmos de identificación facial y de detección de morphing simultáneamente.

PALABRAS CLAVE

Aprendizaje profundo, biometría, control de acceso, FaceNet, identificación, morphing, reconocimiento facial, seguridad, suplantación de identidad.

ABSTRACT

Face identification is becoming a well-accepted technology for access control applications, whether in the real or virtual world. Systems based on this technology have to deal with the classic difficulties of classification algorithms and the challenges of impersonation attacks performed by people who do not want to be identified. Morphing is often the preferred method for these attacks, as it allows modifying an image's features progressively from an original subject so that it gradually resembles another. Publications focus on impersonating this other person, usually someone who is allowed to get into a restricted place, building, or software app. However, there is no list of authorized people in many other applications, just a blacklist of people who cannot enter, log in, or register again. In such cases, the morphing target person is not relevant, and the main objective is to minimize the probability of being detected.

We present a comparison of the identification rate and behavior of 5 recognizers (Eigenfaces, Fisherfaces, LBPH, SIFT, and FaceNet) against traditional morphing attacks, in which only two subjects are used to create the altered image: the original subject and the target. We also introduce a new morphing method that works as an iterative process of gradual traditional morphing, combining the original subject with all the subjects' images in the training database. We also test our morphing attack method against the recognizer that obtains better results against traditional morphing (FaceNet), proving that, using our method, we can multiply by eight the chances of a successful and complete impersonation attack, one able to deceive face identification and morphing detection algorithms simultaneously.

KEYWORDS

Access control, biometrics, deep learning, FaceNet, face recognition, identification, morphing, security, spoofing attack.

TABLE OF CONTENTS

1 Introduction	1
1.1 Contributions	2
2 Related work	3
2.1 Face recognition	3
2.2 Morphing	4
2.3 Spoofing attacks	5
3 Concealing attacks on face identification algorithms with morphing	7
3.1 Face identification and Morphing detection	7
3.2 Proposed algorithm	9
4 Experiments	13
4.1 Selection of the facial identification algorithm	13
4.2 Proposed method against face identification and morphing detection	16
4.3 Attack comparison	16
5 Results	19
5.1 Selection of face recognizer	19
5.2 Proposed morphing attack	20
5.3 Attack comparison	22
6 Discussion	25
6.1 Performance of face recognizers against traditional morphing	25
6.2 Results achieved by our proposed method	26
7 Conclusions	29
Bibliography	31
Glossary	37
Acronyms	39
Appendices	41
A Detailed results of the robustness against morphing	43
B Detailed results of the proposed method	49

LISTS

List of figures

3.1	Flowchart of the proposed algorithm	11
4.1	Example of one similar-looking pair	15
4.2	Performance of the morphing detector	17
5.1	Robustness of the recognizers against traditional morphing	19
5.2	Summary of the results of the proposed morphing attack	21
5.3	Comparison of attack methods.....	22
6.1	Initial and final images of subject number 17	27

List of tables

4.1	Similar-looking pairs selected	15
4.2	Subjects selected to test our proposed method	18
6.1	Accuracy of FaceNet using traditional morphing	25
6.2	Comparison of misidentification using the traditional morphing and our proposal	26
6.3	Comparison of complete attacks using the traditional morphing and our proposal	27
A.1	Complete results of the robustness of Eigenfaces against traditional morphing	43
A.2	Complete results of the robustness of Fisherfaces against traditional morphing	44
A.3	Complete results of the robustness of LBPH against traditional morphing	45
A.4	Complete results of the robustness of SIFT against traditional morphing	46
A.5	Complete results of the robustness of FaceNet against traditional morphing	47
B.1	Complete results of the proposed method.	49

INTRODUCTION

Face recognition is gaining momentum. Continuous improvements in this well-known research field ([1, 2, 10, 11, 26]) have led to an increasing number of commercial applications. Today face recognition algorithms are implemented in a wide range of products and solutions. People counting cameras are used to know the number of clients getting into a store and compute some statistics about their age or gender [3]. Most mobile phones in the market have embedded technology to unlock them with a simple look at the device [4]. More and more websites implement "Know your Customer" policies by comparing a photo ID with real-time capture of the applicant [5]. People identification is likely one of the most important uses of this area. Mobile phones or websites are just two examples of everyday life. However, we can also think about access control in offices or airports, places where this technology is very welcome for its ease of use and low intrusiveness.

Like in any other biometric technology, people have tried to deceive face recognition systems [38]. We can find several approaches in the literature. For instance, a person might print a photo of a subject and try to use it to impersonate him [38, 39]. A more sophisticated method implies creating a mask to be able even to deceive 3D face recognition [6]. Another more extravagant technique is the use of a wearable face projector [7].

For some particular applications, like in airports with **Automated Border Control (ABC)**, where nobody can put an image in front of the camera without being noticed, morphing techniques have been studied. Originally, morphing techniques consisted of generating intermediate frames between two images to achieve a smooth transition between them. If we use it on two images of different faces, we could get frames that merge features of both faces in one. Depending on the level of morphing being applied, one person will be recognized better than the other. In the **ABC** scenario, M. Ferrara [8] studied a way to take advantage of morphing to use only one photo ID to successfully verify two different subjects.

The previous approach is interesting because it has shown that it can fool face verification systems. However, the morphing process itself can be discovered, making the spoofing attempt a failure. This work focuses on concealing the attack in such a way that humans or automated systems cannot detect that an image has been altered. As previous work, we have researched how different face identification

methods behave against the morphing process. Face identification is different from face verification because in the latter case we have information about who the subject might be. In some applications this is not the case, for example, if we use the face image to check whether a user has already been registered in a web site.

This paper is divided into seven sections. In Section 2, we present an overview of the state-of-the-art face recognition and morphing software, as well as a brief review of past spoofing attacks to face recognition algorithms. In Section 3, we describe the method used for selecting the most robust algorithm against morphing and the proposed algorithm to defeat it. In Section 4, we explain the implementation of the method. In sections 5 and 6, we present the results of the experiments and their discussion. Finally, in Section 7, we make conclusions about the findings of our experiments.

1.1 Contributions

As far as we know, our work is novel since we have found no other research publication that covers face identification algorithms tested with morphed images and a method specifically designed to deceive the face identification algorithm while passing undetected. Next, we summarize our main contributions.

- We present a study of five state-of-the-art techniques in face identification. Each technique is tested with morphed images to find the more robust one, considering robustness the quality of requiring a higher amount of morphing alteration to misclassify a subject.
- We propose a new method to reduce the amount of morphing alteration required to make a face identification algorithm misclassify a subject.

RELATED WORK

2.1 Face recognition

As seen in [9], the face recognition process involves the location of the face in the image, followed by an analysis of the located face (for instance, extracting its features) and then a comparison of the analysis results against all the faces stored in the database, using a classifier. Face recognition methods can be divided into four main categories: holistic, local, hybrid and deep learning approaches [10], [11]. The local approach classifies according to specific facial features, whereas the holistic approach considers the whole face as a unit. The hybrid approach combines both techniques. Many recent advances have been made in the deep learning approach, using **Convolutional Neural Networks (CNNs)** that offer better speed and accuracy.

The first simple and fast algorithm that worked well in a constrained environment, Eigenfaces, came in 1991 [12], based on the **Principal Component Analysis (PCA)** technique, which is included in the holistic approach. Later, based on Eigenfaces' same principle, Fisherfaces was developed, using **Linear Discriminative Analysis (LDA)** and achieving a better performance over variation in lighting [13]. The third most popular technique in the holistic approach is **Independent Component Analysis (ICA)** [14], which has excellent efficiency. Other methods can be included in this category. Some of them, combined with the three techniques mentioned before, can obtain good recognition performance. For instance, Hafez *et al.* [15] used a Gabor filter and LDA.

In the local approach, we can find a simple method, **Local Binary Pattern (LBP)**, used to extract features from any object. It was G. Zhang *et al.* [16] who first used it for face recognition. Other well-studied feature extractors utilized for face recognition are **Scale-invariant Feature Transform (SIFT)** [17] and **Speeded-up Robust Features (SURF)** [18], inspired by SIFT but with better execution time.

Hybrid techniques can offer high recognition rates. However, they are more challenging to implement due to their high complexity, which makes them less popular than the others. An example can be found in [19], where A.A. Fathima *et al.* used Gabor wavelet and **Linear Discriminative Analysis**. More examples can be found in [10].

The deep learning approach can be considered as a nonlinear holistic technique [10]. Nevertheless, some references ([11]) define it as a new category due to its newness and great accuracy. A few examples showing very good accuracy with the verification problem in the **Labeled Faces in the Wild (LFW)** database [25] are: deepFace [20], developed in 2014, got an accuracy of 97.35%; DeepID3 [21] (2015, 99.43%), FaceNet [22] (2015, 99.63%), VGGFace [23] (2015, 98.95%), and Arcface [24] (2018, 99.83%).

LFW is an excellent database to test face recognition algorithms because it is an **unconstrained database**. Usually, algorithms struggle with lighting, location, setting, pose, or age variations, as well as occlusions or misalignment [26–28]. However, over time, algorithms have improved significantly in this area, so recent local and deep learning approaches can handle these problems better.

2.2 Morphing

For many years the film and television industries have used morphing to obtain fluid transformations between two different frames using mesh warping methods [29] based on three stages: feature specification, warping and blending. In the first step, correspondence between the two images is created (using a mesh). In the second stage, a geometrical alignment of the mesh is performed using warping [30]. In the latter, all warped images are aligned, so it only remains to merge each pixel's color value, using a cross-dissolve method.

A review of this morphing approach with other first-generation morphing methods such as field morphing or radial basis functions, can be found in [31]. In his work [32], M. Steyvers analyzes field morphing with a greater mathematical perspective. More recently, U. Scherhag *et al.* presented an overview of the publicly available state-of-the-art commercial and open-source face morphing tools [33]. Most of them are based on Delaunay triangulation [49], which we consider the principal approach to morphing until the appearance of **Generative Adversarial Networks (GAN)** that also show promising results [35]. However, to this day, GAN performs worse than the more classic methods against face recognition systems like OpenFace (a face recognition implementation based on FaceNet) [35].

The steps followed by Delaunay triangulation based methods are the same as in mesh warping but using different techniques to achieve each goal. The correspondence between the two images is made by determining face key landmarks (eyes, mouth, nose, face contour ...) either manually or automatically (using software). Then, a Delaunay triangulation is applied using the landmarks as vertices for the non-overlapping triangles. During warping, the corresponding triangles of both images suffer a geometrical transformation in order to be aligned. Finally, a linear blending is applied.

2.3 Spoofing attacks

Attacks on biometric recognition systems are not only carried out on facial recognition devices. In [36], authors conduct spoofing attacks on fingerprint sensors, iris scanners, and facial recognizers. Moreover, they conclude that the method's performance does not correlate with its vulnerability. In fact, in all of them, a satisfactory attack can be achieved. This statement is also supported by A. Hadid *et al.* [38], using 3D masks (face recognition spoofing) and fake fingerprints (fingerprint-recognition spoofing), among others. They also study how anti-spoofing methods can reduce the vulnerability of the systems.

Focusing on the facial recognition attacks, not only morphing poses danger. In [38,39], they explore some databases with presentation attacks. Presentation attacks consist of showing a printed image (or printed mask) to a camera with facial recognition software to fool it. In addition, in [39], they prove that the higher the face verification accuracy, the higher is its vulnerability to presentation attacks. Apart from this, M. Ferrara *et al.* [40] study the effects of geometric distortions (barrel distortion, vertical contraction, and extension) and digital beautification on face recognition accuracy. Other digital manipulation techniques can be very harmful, e.g., face synthesis, attribute manipulation, and identity or expression swap [41].

As mentioned before, M. Ferrara *et al.* [8] were the first to present a successful morphing attack in a simulation of an ABC, using two commercial face recognition software tools. Applying GIMP+GAP, manually morphed images were created to verify the two contributing subjects with the same photo. They were able to achieve that for eleven pairs of subjects in both face verification tools. Moreover, in [40], the authors expand the experiment proving that human experts (border guard group) and non-experts, in most cases, do not detect morphed images. However, in [42], D. J. Robertson *et al.* reveal that although the attack may go more unnoticed in untrained subjects, when the subjects receive morphing training, they tend to detect morphing with higher probability. Nonetheless, in their experiment, they use Psychomorph, which creates lower quality morphings (with more ghost artifacts) than GIMP+GAP. More examples of verification attacks can be found in [43] and [44]. In the first one, they carried out the experiment using FaceNet, utilizing more than 3000 pairs with 22 morphed images between each pair, working with triplets of images (impostor-accomplice-morphing). In the second one, experiments were conducted to prove face verification's vulnerability both with printed and scanned images.

Another morphing attack perspective may be to protect the privacy of the users in video surveillance systems. P. Korshunov and T. Ebrahimi [45] study this problem along with its robustness and reversibility.

Finally, we would like to reference some studies in which we can find out how some parameters can affect the success of a morphing attack [33, 36, 46]. Those parameters are the morphing quality, the similarity between the impostor and the accomplice, or the recognizer's threshold.

CONCEALING ATTACKS ON FACE IDENTIFICATION ALGORITHMS WITH MORPHING

A morphing attack is the alteration of a subject's portrait using morphing techniques leading to his misidentification. In our work, it is complete only when it meets two criteria: first, a face identification algorithm should not identify the morphed image, and second, the morphed image should appear as a genuine image to a potential auditor. Face recognition algorithms might be beaten or defeated by a morphing attack when the image resulting from a morphing process is not identified as the original subject. However, if the resulting image does not appear genuine, the attack cannot be considered complete.

Considering the research done in Section 2.2, we have chosen a morphing method based on Delaunay triangulation [37], hereafter referred to as the traditional morphing method. At the warping and blending steps of the process, a parameter is taken into account. In the case of warping (w), it conditions how much each position of each face's landmarks contributes to the morphed image. If $w = 0$, only the first image's landmarks are taken into account. If $w = 1$, only the landmarks of the second image are considered. The in-between values achieve a linear combination of the positions of the landmarks of both contributing images. The blending step (b) has a similar behavior, the color of all the correlated pixels are combined using a linear transformation. $b = 0$ only considers the first image and $b = 1$ the second.

For simplicity, some implementations only use one parameter α , that reflects the general percentage of contribution of both faces in each step ($w = b = \alpha$). In our study, we use this simplification as a quantifier of the morphing process. For example, a morphing process of 5% means that $\alpha = 0.05$. The first subject of the pair will contribute to the final image by 95% in both the landmarks' position and the pixels' value. The second subject will contribute with the remaining 5%.

3.1 Face identification and Morphing detection

As we have seen in Section 2.1, face recognition is a very active research field, and different approaches are being studied. We have selected the more promising ones with care to include at least one from each category (except hybrid):

- Eigenfaces [12]
- Fishefaces [13]
- LBPH [51]
- SIFT [17]
- FaceNet [22]

However, the experiments found in the literature do not consider morphing attacks against face identification. Our objective is to select the approach that performs better against these attacks. From our perspective, good performance means that the algorithm can correctly identify the original subject in images that have been morphed. Since morphing is an incremental process, we consider an algorithm to be more robust than another when the amount of morphing required to make it fail is higher. Therefore, the selection criteria is related to the frame at which the face recognition algorithm does not recognize the original subject but another (either the target subject or any other person).

The original image is morphed into 100 images with $n\%$ morphing ($n \in \{1, \dots, 100\}$). We consider that the original image has been morphed 0%, the target image has been morphed 100%, and any other image in between has $n\%$ ($n \in \{1, \dots, 99\}$) as the amount of morphing. The higher the percentage required to avoid that the recognizer correctly identifies the original subject, the more robust it will be considered.

We recommend that face recognition algorithms are trained with a database composed of N subjects, with a number of photos per subject between 5 and 20. This quantity helps to avoid imbalanced data and biased results. We have chosen pairs of similar-looking subjects. This should reduce the amount of alteration required to pass from the original image (referred to as A) to the target image (referred to as B).

Since a complete morphing attack has to pass undetected, we need to define a method to detect morphed images. The easy procedure is to invite human experts that will evaluate the resulting image. However, this method might not be the most consistent because the same person can change his evaluation about a particular image or because different people may have different opinions. Therefore, using a morphing detector algorithm seems a good idea.

Although some face anti-spoofing detectors already existed before morphing attacks became a reality [60], the first morphing detector was presented by R. Raghavendra *et al.* [61], which successfully verified all the 450 morphed face images from a database. It belongs to a category of morphing detectors that operate in **Single Image Morphing Attack Detection (S-MAD)** scenarios. It refers to algorithms that only analyze one photograph to verify its morphing. Contrarily, **Differential Morphing Attack Detection (D-MAD)** group algorithms that analyze a pair of images, one of them being a trusted unaltered photograph that the algorithm uses to verify the morphing on the other image. Our scenario falls into

the first category since we only provide one image to the detector to get a morphing verification. Some state-of-the-art **S-MAD** algorithms can be found in [62–66].

3.2 Proposed algorithm

We have approached the problem of concealing morphing attacks as an optimization problem. The universe of potential solutions is searched while trying to minimize the amount of morphing required to beat the face recognition algorithm. This approach makes sense if we assume that the lower the amount of morphing, the higher the chances of passing undetected. Starting with Subject A's original image, potential solutions are created by an iterative process of gradual morphing that combines the original image and all the subjects' images in the database.

The problem can be represented as a **full m -ary tree**, being m the number of images stored in the database. The root vertex would be the unaltered image of Subject A and the other vertices, the morphed images. Each branch would represent an $n\%$ morphing between the parent and a person in the database. The less modification the image has, the less detectable it will be, so the algorithm searches the vertex that causes misidentification with the lowest percentage of morphing (lowest depth) and lowest morphing detection, using a Breadth-first search: it starts at the root, then searches for a misidentification in all of its child nodes' images, then moves to the next depth level, and so on.

We use a morphing detector as an additional evaluator of the probability of a **complete attack**. The resulting solution is the combination of morphing procedures with the lowest amount of alteration and the lowest evidence reported by the morphing detector. In summary, our method requires:

- A robust face recognizer.
- A training database.
- A morphing algorithm.
- A morphing detector (**S-MAD**).

It follows these steps:

1. The original photo is morphed 5% separately with all the photos available in the training database (except the original subject's pictures).
2. The morphed photos are passed on to the face identifier:
 - (a) If in all the images it still identifies the original subject, it goes to Step 3.
 - (b) If a different person is identified in one or more morphed photos, it goes to Step 6.

3. The first ten images that most reduce the identification confidence are selected.
4. The morphing detector evaluates the ten images to get the photo with the least detectable morphing, outputting the one with the least morphing detection confidence. In case of a tie, it is resolved by the alphabetical order of the subjects used.
5. The algorithm goes back to Step 1, replacing the original photo of the subject with the surviving image.
6. The morphing detector also evaluates those images to get the resulting photo with the least detectable morphing, ending the algorithm.

When we say that the original image is morphed 5%, we mean that the first face of each morphing contributes 95% to the warping and blending process. For each iteration, the original image's contribution is reduced by the formula:

$$\% \text{ of original image's contribution} = 0.95^t, t \in \mathbb{N}, \quad (3.1)$$

being t the number of iterations performed. For instance, in the third iteration $t = 3$, three morphings have taken place, so the original subject's contribution is $95\%^3 \approx 85.74\%$.

Dealing with all the possible morphing paths has an exponential complexity over the database size. Suppose the database size is m (with N subjects, $N < m$), the database size without the original subject's pictures is m' . If the algorithm needs t iterations to finish, the complexity would be $O((m')^t)$. This is because, in each iteration, all the images of the previous iteration would be morphed with all the training database. To reduce that computational cost, we have implemented a **heuristic**. It is reflected in steps 3–4 and manages to reduce to one the number of images that pass to the successive iteration. The **heuristic** chooses the photo that is closest to the goal in each iteration, and the complexity becomes linear ($O(t \cdot m')$).

Additionally, the morphing detector is also used in the sixth step to make sure that we select the picture that gets closer to a **complete attack**. Fig. 3.1 shows a flowchart of the process.

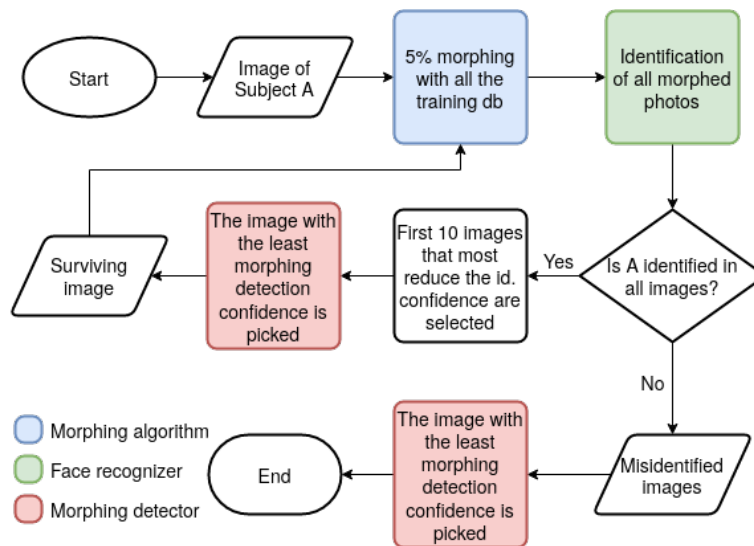


Figure 3.1: Flowchart of the proposed algorithm.

EXPERIMENTS

We have carried out experiments to compare the morphing robustness of face identification algorithms in order to select the best one. We have also tested our proposed attack method on the face identifier selected, and compared the results obtained with the traditional attack.

All the experiments have been performed in an HP Pavilion x360 14-cd0005ns laptop, with 8 Gbs of RAM and an Intel Core i3-8130U chip, running Ubuntu 18.04.5 LTS with bash 4.4.20(1)-release, Python 3.6.9 and Python 2.7.17. The versions of the libraries used are:

- OpenCV [34]: 3.4.2.
- Scikit-learn [54]: 0.21.3 in Python3 and 0.20.4 in Python2.
- Tensorflow [56]: 1.14.0 in Python3 and 1.7.0 in Python2.
- Numpy [68]: 1.18.2 in Python3 and 1.16.6 in Python2.
- Dlib [50]: 19.18.0.

4.1 Selection of the facial identification algorithm

We have chosen different solutions for each face recognition algorithm category (except hybrid). Within the holistic approach, Eigenfaces [12] and Fisherfaces [13] have been selected. As representatives of the second category (local approach), we have picked **Local Binary Patterns Histogram (LBPH)** [51] and **SIFT** [17]. The **LBPH** algorithm works by creating histograms of the binary patterns extracted by **LBP** [16]. As seen in [10, 13, 17, 47], these techniques have been well studied and have good performance when using frontal views of faces. **FaceNet** [22] has been selected out of the deep learning category due to its excellent performance [11].

For the first three algorithms (Eigenfaces, Fisherfaces, and **LBPH**), we have employed a Python implementation of R. Raja [52] that uses the Face library of OpenCV to cover the feature extraction and classification. Besides, a Haar cascade classifier [53] is used for face detection. Slightly modifying the previous implementation, we have gotten a **SIFT** deployment, using the `xfeatures2d` OpenCV class to

perform the **SIFT** feature extraction and the Scikit-learn library for classification using a **Support Vector Machine (SVM)** [55]. In addition, we have used a Tensorflow implementation of FaceNet [57] written in Python. It uses a pre-trained model that employs VGGFace2 [58] as the training dataset and the Inception-ResNet-v1 architecture [59], achieving an **LFW** accuracy of 99.65+-0.00252%. It also uses an **SVM** for classification.

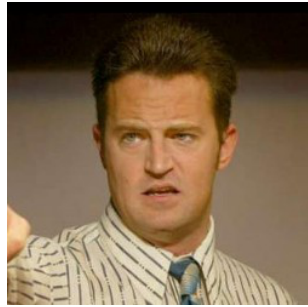
All the recognizers expect the testing subjects to be included in their training database, which is known as closed-set identification. We have also made small changes in the code files to get similar behavior in all the implementations. Every algorithm used can output the top 5 identification matches of the face presented. The parameters of the Haar cascade classifier that worked better with our database were *scaleFactor=1.001*, *minNeighbors=2*, *minSize=(90,90)*, *outputRejectLevels=True*. Regarding the **SVM** used on **SIFT**, we have employed the settings *kernel="poly"*, *C=10*, *gamma=0.0001*. We have left all the other configurations according to the original sources.

As we have seen, we need a fully automatic morphing implementation. We have used the Python code presented by S. Patel [48], based on OpenCV functions [37]. In order to find the face landmarks, it uses Dlib's facial landmark detector. Then, as we have seen, those landmarks are employed as vertices of the Delaunay triangles. Using the corresponding triangles, it performs warping and blending to obtain all the intermediate frames.

We have created a database based on **LFW** [25]. As seen in [11], it is a widely used database to test state-of-the-art face recognizers. The database has 5749 subjects, but, as mentioned earlier, we want only the ones that have between 5 and 20 images each (both numbers included). That filters the database to 366 people with a total number of 3062 images. The Haar cascade face detector does not correctly detect the subject face in 5 of the 3062 images because those images have more than one face present and the wrong face is detected. We deleted those images from the database. The deleted images are *Erika_Harold_0003*, *Hugh_Grant_0008*, *Igor_Ivanov_0014*, *Jean_Charest_0004*, and *Joe_Lieberman_0004*. That implies that Erika Harold now has four images instead of 5, considering this an exception.

To determine the pairs of subjects who look more alike, we have used the **Similar-looking LFW (SLLFW)** database [67], which offers 3000 pairs of similar-looking faces (using the images of **LFW**). We have picked 25 pairs of images from it, taking into account two factors. First, the individuals must be included in our 366 subjects database. Second, the subjects need to have more than five photos to train once the similar-looking images selected are removed from the training database. Fig. 4.1 shows an example of one selected pair.

Considering all the pairs, there are 49 different images (*Renee_Zellweger_0009* appears twice). The training database of the morphing robustness comparison and selection experiments consists of $3062 - 5 - 49 = 3008$ images of 366 subjects. In Table 4.1, we provide all the pairs used.



(a) Matthew_Perry_0007.



(b) Rubens_Barrichello_0011.

Figure 4.1: Similar-looking pair.

No.	Original subject	Target subject
1	Amelia_Vega_0003	Norah_Jones_0015
2	Ana_Guevara_0002	Ian_Thorpe_0006
3	Andy_Roddick_0008	Richard_Virenque_0004
4	Angelina_Jolie_0002	Britney_Spears_0004
5	Anna_Kournikova_0011	Jelena_Dokic_0007
6	Ben_Affleck_0002	Ian_Thorpe_0007
7	Bill_McBride_0010	Jon_Gruden_0002
8	Bill_Simon_0011	Ron_Dittemore_0001
9	Catherine_Zeta-Jones_0001	Salma_Hayek_0001
10	Edmund_Stoiber_0004	John_Snow_0003
11	Eduardo_Duhalde_0006	George_HW_Bush_0005
12	Fidel_Castro_0018	Mohamed_ElBaradei_0003
13	Hillary_Clinton_0010	Renee_Zellweger_0009
14	Howard_Dean_0003	Kevin_Costner_0005
15	James_Blake_0006	Mark_Philippoussis_0003
16	Jason_Kidd_0003	Leonardo_DiCaprio_0003
17	Jean-Pierre_Raffarin_0001	Joschka_Fischer_0012
18	Jimmy_Carter_0006	John_Snow_0004
19	Joan_Laporta_0007	Pierce_Brosnan_0006
20	John_Kerry_0005	Robert_Redford_0002
21	Julianne_Moore_0019	Nancy_Pelosi_0002
22	Kate_Hudson_0008	Mariah_Carey_0006
23	Matthew_Perry_0007	Rubens_Barrichello_0011
24	Mike_Martz_0005	Paul_O'Neill_0003
25	Renee_Zellweger_0009	Sheryl_Crow_0001

Table 4.1: Similar-looking pairs selected.

4.2 Proposed method against face identification and morphing detection

Our aim is to evaluate the performance of our method as a **complete attack** system. Therefore, we have tested it with the most robust face recognition system selected in the previous part and a morphing detector.

The basic morphing operation required in the algorithm is implemented with the traditional morphing processing technique based on Delaunay Triangulation.

Regarding the **Single Image Morphing Attack Detection**, we have tried the algorithms of [64–66]. The one that had the best performance and integration in our scenario has been the detector presented by R. Raghavendra *et al.* [65], which has better results than other state-of-the-art alternatives. Although it is designed to detect morphing in printed-scanned photographs, it achieves excellent detection results in our scenario (Fig. 4.2), and therefore, it is the morphing detector used.

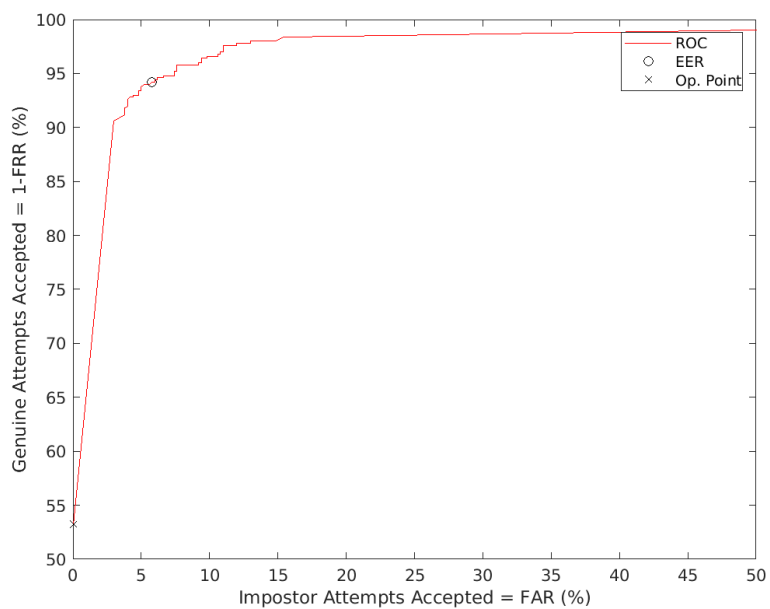
In the testing of our proposed method, we no longer use the Haar cascade classifier, so there is no need to delete its five undetected faces. We start with the filtered **LFW** database of 366 subjects with a total of 3062 images (with between 5 and 20 photos per subject). We have deleted 182 images because the morphing algorithm throws exceptions on them.

We have tested the proposed morphing attack in 25 subjects based on the first image of the similar-looking pairs used in Experiment 1. However, we have changed some images due to morphing or recognition problems (we want the first image to be correctly identified in all cases). Therefore, the training database contains $3062 - 182 - 25 = 2855$ images. Table 4.2 presents all the participants.

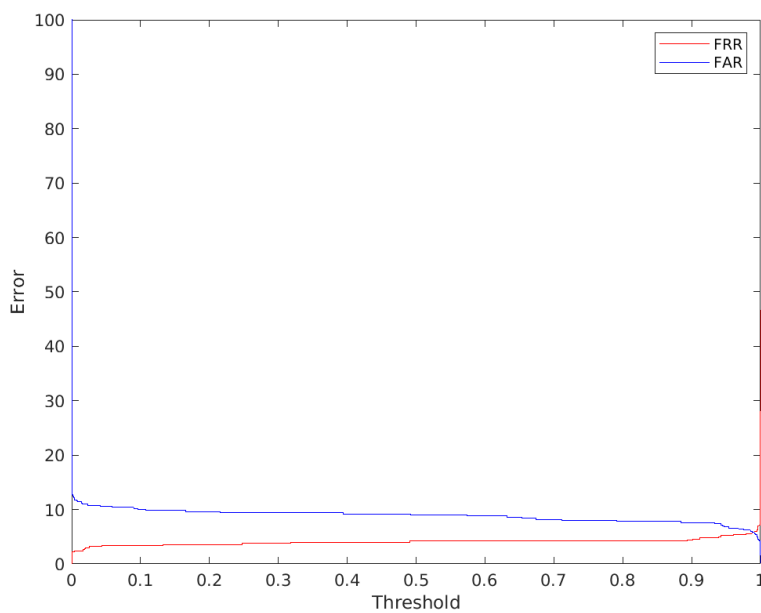
To train and test the morphing detector, we have picked the **LFW** subjects' images not used in the experiments (people with n images, $n < 5$ or $n > 20$). We have split the subjects randomly into two groups, one for testing and the other one for training. Due to Matlab memory limitations, we have trained the detector using 3000 bonafide (not altered) images from the training group and 3500 morphed images. The morphed images were created randomly using pairs from the subjects included in the training group, covering all percentages between 1 and 99. Analogously, we have tested the detector using 500 bonafide images and 500 morphed images. Fig. 4.2 represents the **ROC curve** and the **FAR vs. FRR curve** obtained, showing the excellent performance achieved.

4.3 Attack comparison

We have conducted experiments comparing the proposed method with the traditional morphing attack to have a better feeling of its concealing features.



(a) ROC curve.



(b) FAR vs. FRR curve.

Figure 4.2: Performance of the morphing detector.

No. Subject	No. Subject
1 Amelia_Vega_0004	14 Howard_Dean_0003
2 Ana_Guevara_0002	15 James_Blake_0006
3 Andy_Roddick_0008	16 Jason_Kidd_0003
4 Angelina_Jolie_0002	17 Jean-Pierre_Raffarin_0007
5 Anna_Kournikova_0011	18 Jimmy_Carter_0006
6 Ben_Affleck_0001	19 Joan_Laporta_0007
7 Bill_McBride_0010	20 John_Kerry_0005
8 Bill_Simon_0011	21 Julianne_Moore_0019
9 Catherine_Zeta-Jones_0001	22 Kate_Hudson_0005
10 Edmund_Stoiber_0004	23 Matthew_Perry_0007
11 Eduardo_Duhalde_0006	24 Mike_Martz_0005
12 Fidel_Castro_0018	25 Renee_Zellweger_00012
13 Hillary_Clinton_0010	

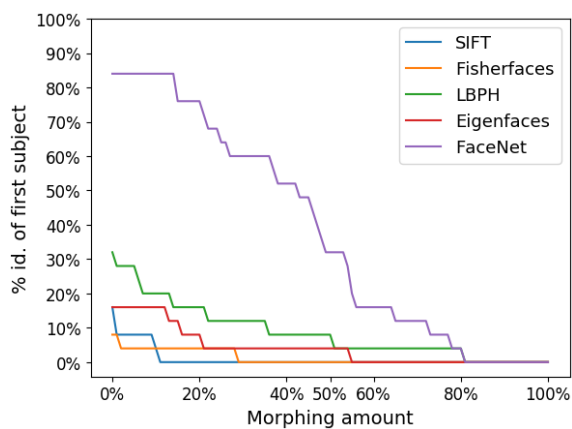
Table 4.2: Subjects selected to test our proposed method.

We have used the face identifier, training database, and morphing detector previously employed to evaluate our proposed method (Section 4.2).

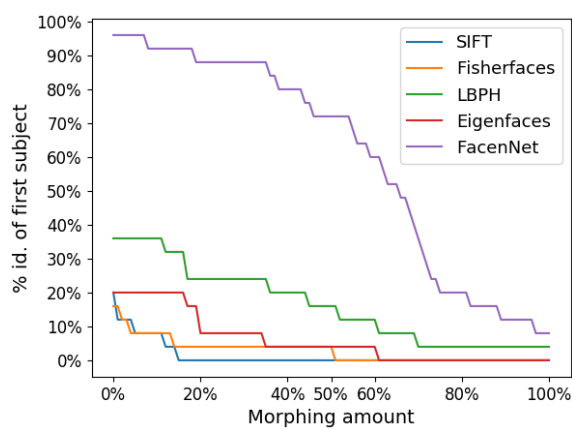
To select the testing subjects, we have used the common individuals from the two lists already seen (tables 4.1 and 4.2). That is all the original subjects except for numbers 1, 6, 17, 22, and 25. We have used the morphed images previously generated. In the case of the traditional attack, we have used the similar-looking pairs and, in the case of our proposed method, the iterative morphing procedure. We have compared the percentage of alteration needed to cause misidentification, and the morphing detected in the misidentified images using both morphing attack techniques.

RESULTS

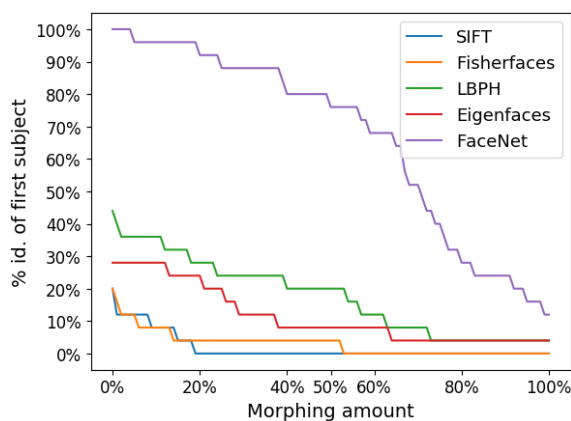
5.1 Selection of face recognizer



(a) Top 1.



(b) Top 3.



(c) Top 5.

Figure 5.1: Percentage of morphed images identified as the original subject for each level of morphing.

Fig. 5.1 shows the face identification algorithms comparison of their robustness against morphing. It is divided into three plots. Fig. 5.1(a) exhibits the face recognizers' comparison analyzing the top 1

identification matches. Fig. 5.1(b) analyzing the top 3. Fig. 5.1(c) the top 5. Their x-axes represent the level of morphing in the pairs. 0% morphing symbolizes the unaltered image of the first subject of the pair (original subject), 100% the second subject, and the rest of percentages the in-between morphings. Their y-axes reflect the percentage of couples who still have their original subject identified within the top for each morphing level.

We can observe that the identification percentages rise as we increase the top analyzed. However, the three graphs show a similar robustness ranking:

1. FaceNet
2. LBPH
3. Eigenfaces

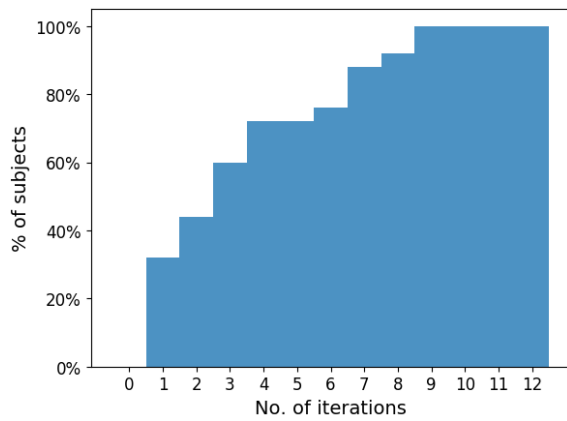
By far, FaceNet is above all the other recognizers. It is the one who takes the longest to misidentify the original subject. LBPH is in second place, having a distance with FaceNet of more than 50% of misidentification in some cases. Eigenfaces is in the third position, followed by Fisherfaces and SIFT, which are the last ones and have a very similar performance (especially analyzing the top 3 and 5). These positions are maintained in practically all the three graphs' morphing levels, except for some ties, e.g., beyond 80% morphing in Fig. 5.1(a).

Each top's best identification scores are achieved, with 0% morphing, by FaceNet, being 84%, 96%, and 100%, respectively. Not even LBPH passes the 50% of identification of the original subject. However, once the 100% morphing is reached, only in the top 3 and 5 the original subject is still identified in some pairs of FaceNet, LBPH, and Eigenfaces.

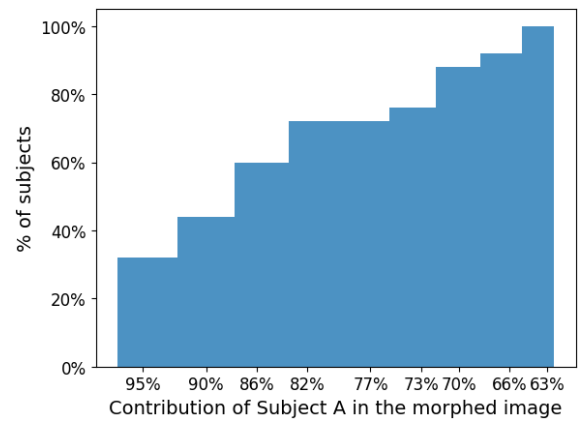
It is clear that the most robust face recognizer is FaceNet, so it is the algorithm selected. These experiments' complete results can be found in Appendix A, reflecting all the percentages where Subject A (first member of the pair) or B (second member) are recognized for every pair of images.

5.2 Proposed morphing attack

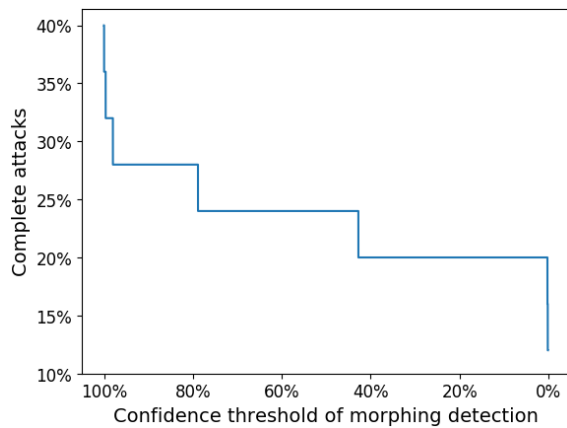
Fig. 5.2 presents the summary of the results of our proposed morphing attack. It contains four plots. The first one (Fig. 5.2(a)) represents the number of iterations required to make FaceNet misidentify the original subject. The second plot (Fig. 5.2(b)) presents the necessary decrease in the original subject's contribution to the morphing in order to achieve the misidentification. Fig. 5.2(c) shows the percentage of complete (undetected) attacks depending on the morphing detector's confidence **threshold**. The **threshold** is the confidence needed to classify an image as morphed. The last plot (Fig. 5.2(d)) displays the relation between the number of iterations and the morphing detection confidence, showing the percentage of subjects per tuple iterations-morphing detection. For example, 12% of the subjects



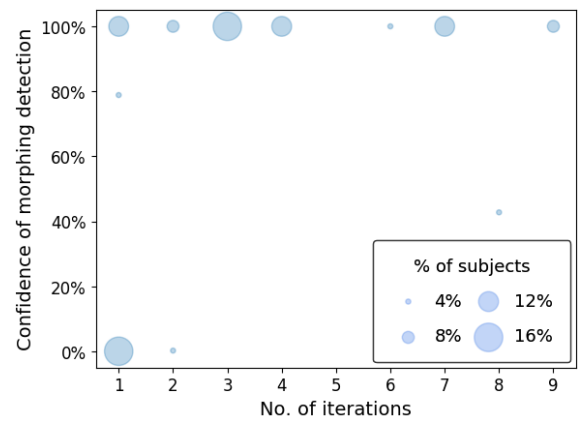
(a) Percentage of subjects that are misidentified by FaceNet.



(b) Percentage of subjects that are misidentified by FaceNet.



(c) Percentage of complete attacks depending on the morphing detector's classification threshold, i.e., the confidence needed to classify an image as morphed.



(d) Scatter plot that reflects the relation between the number of iterations and morphing confidence. The size of the point measures the % of subjects that share the same relation. (Some percentages on the y-axis have been rounded +2% for clarity.)

Figure 5.2: Summary of the results of the proposed morphing attack.

needed four iterations to achieve the misidentification, and their misidentified images have morphing confidence of 100%.

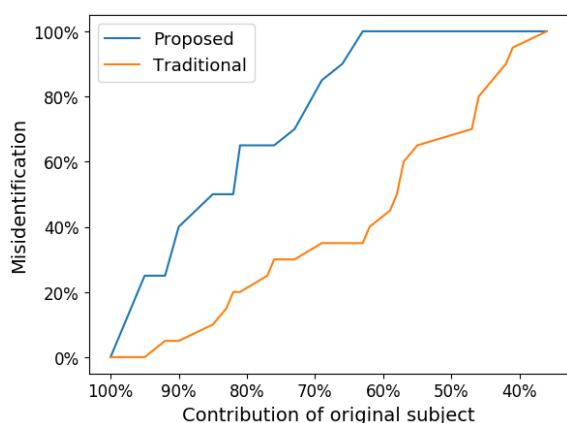
We can see that most images needed four iterations or less to finish, being one iteration the most common case (32% of the images). This means that in many cases, 5% of modification is enough to cause misidentification. Only 28% of the subjects needed more than six iterations. The maximum number of iterations required has been nine, so, if the subject contribution is down to 63% (0.95^9 , Eq. 3.1), all the images obtain the original subject's misidentification.

With a 100% confidence **threshold** of morphing detection, 40% of the subjects achieve a **complete attack**. However, this percentage drops to 32% with a **threshold** of 98%. This reflects the excellent performance of the morphing detector. Nevertheless, it is not infallible, and we can conceal 24% of the attacks if the **threshold** is set to 50%. Even with a **threshold** near 0% we can achieve a 20% of **complete attacks**.

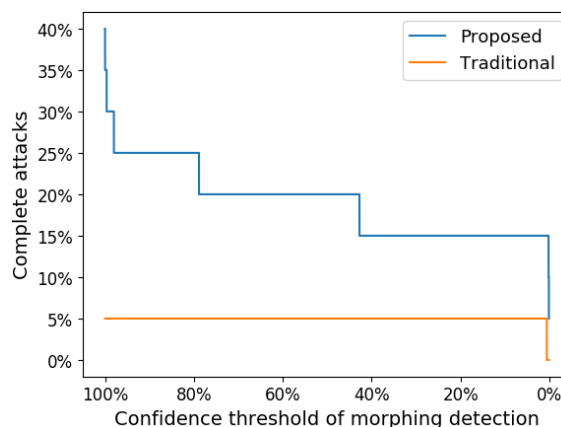
If we observe the relation between iterations and the morphing detected, we notice that even some portraits that only needed one iteration get a 100% of morphing detection. However, all the images with morphing detection confidence near 0% are cases with one or two iterations. Every image with three or more iterations has morphing detection confidence of almost 100%, except one subject with eight iterations that have a 42.75% detection rate.

The experiments' complete results, including the initial and final image of each subject can be found in Appendix B.

5.3 Attack comparison



(a) Percentage of subjects that are misidentified by FaceNet.



(b) Percentage of **complete attacks** depending on the classification **threshold** of the morphing detector.

Figure 5.3: Comparison of attack methods.

Fig. 5.3 displays the comparison of the traditional morphing attack technique and our proposed method. It is divided into two plots. The first one (Fig. 5.3(a)) compares the percentage of subjects misidentified by FaceNet for each level of contribution of the original subject in the morphed image. In the second plot (Fig. 5.3(b)), we can see the comparison of the percentages of complete (undetected) attacks depending on the morphing detector's confidence **threshold**.

The new method achieves misidentification much faster than the traditional method. With the subject's contribution down to 63%, they get 100% and 35% of misidentification, respectively. The traditional method needs the contribution to go down to 36% so that the misidentification reaches 100%. Our method also achieves a higher percentage of **complete attacks**, between 40% and 5% depending on the **threshold**, compared to the 5% that the traditional attack accomplishes at most.

DISCUSSION

6.1 Performance of face recognizers against traditional morphing

The results obtained in facial identification on the **LFW** database are notably worse than those obtained in verification. This might be expected since, for identification, we work 1 vs. N ($N = 366$ in our database), and regarding verification, we work 1 vs. 1. Thus, as mentioned in [69], the difficulty of identification is related to the number of subjects contained in the database. Some examples are Eigenfaces, in which we have obtained 16% of identification accuracy in contrast with 60.02% of verification accuracy [69], and FaceNet, with 84% and 99.6% of identification and verification accuracy, respectively [69].

FaceNet obtains a good performance identifying the in-between morphed images correctly. This means that in the case of a real attack on FaceNet, the attacker would need to significantly alter the image to fool the recognizer. Taking a look at Table 6.1, we can see that analyzing the top 1, the attacker would need a 43% morphing alteration to have more than a 50% chance of the attack being successful. If we analyze the top 3, the required morphing alteration is higher than 66%. Finally, if we analyze the top 5, the alteration needed rises to 71%. FaceNet shows such good results that some attacks will fail even with the original image wholly modified (100% morphing) if we consider top 3 or top 5 lists.

	% of morphing					
	0%	43%	50%	66%	71%	100%
Top 1	84%	48%	32%	12%	12%	0%
Top 3	96%	80%	72%	48%	32%	8%
Top 5	100%	80%	76%	64%	48%	12%

Table 6.1: Accuracy of FaceNet at different percentages of morphing using the traditional method.

Since the morphing process converts the original image progressively into the target one, we may expect to obtain identification results transitioning from the former to the latter. However, this only happens with FaceNet and only with some pairs. The other recognizers studied have behaviors such that

they identify other subjects in some intermediate morphings, and they might even recognize the original subject intermittently. For example, Table A.2 shows that in the fourth pair, Fisherfaces recognize the original subject in 0–28% and 34–36% of morphing. On the contrary, FaceNet has a much more regular and expected performance. For instance, Table A.5 exhibits that in the case of the fourth pair, the original subject is identified in the top 1 in 0–54% morphing, then she goes to the second and third position in the top in 55–58% morphing and finally to the fourth and fifth position in 59–64% morphing. On the contrary, the target appears in the fourth and fifth position in 44–53% morphing. Then she goes up to the second and third position at 54–59% morphing. Finally, she remains in the top 1 in 60–100% morphing.

The percentage considered for the results has been the first percentage at which the original subject ceases to be recognized, regardless of whether he is recognized again in later percentages or not. Another interesting approach could be to study all these intermediate percentages where the original subject is identified again.

6.2 Results achieved by our proposed method

Our morphing method requires a considerably lower amount of morphing process to fool FaceNet. Table 6.2 shows that FaceNet misidentifies 25% of the images where the original subject contributes with 95% of the information. This is especially interesting if we consider that with the traditional morphing technique, the success rate is 0%. Moreover, our method successfully beats FaceNet in all the cases when the original subject contributes with 63% or less to the morphed image. The traditional method is much less capable since it requires that only 36% of the original image remains to get all the attacks passed by.

	Contribution of the original subject								
	100%	95%	90%	85%	81%	73%	63%	58%	36%
Trad.	0%	0%	5%	10%	20%	30%	35%	50%	100%
Ppsd.	0%	25%	40%	50%	65%	70%	100%	100%	100%

Table 6.2: Comparison of misidentification of the original subject by FaceNet for each level of his contribution on the image using the traditional (trad) morphing and our proposal (ppsd). Higher is better.

Moreover, the performance of the morphing detector is also remarkable. The traditional morphing is not able to reach more than 5% of **complete attacks** (Table 6.3). This means that the morphing detector can detect 95% of the attacks unless the confidence required is lowered to meaningless values (0.2% confidence in the classification). Our method improves these results in a very significant way. For example, when 100% confidence is required we can achieve 40% of **complete attacks**, eight times more than the traditional morphing technique. The improvement decreases with the demanded confidence

such that when only a certitude of 42% is required, we achieve 15% of **complete attacks** versus 5% from the other method, three times more.

	Threshold				
	100%	98%	78%	42%	0.2%
Trad.	5%	5%	5%	5%	0%
Ppsd.	40%	25%	20%	15%	10%

Table 6.3: Comparison of **complete attacks** depending on the morphing detector's classification **threshold** of the morphing detector using the traditional (trad) morphing and our proposal (ppsd). Higher is better.

If we consider the option of a human being as a morphing detector, the detection accuracy might be lower, and therefore the number of **complete attacks** could be higher. Fig. 6.1 shows two images that most people would consider equal, whereas the morphing detector is 100% sure that Fig. 6.1(b) has been morphed.

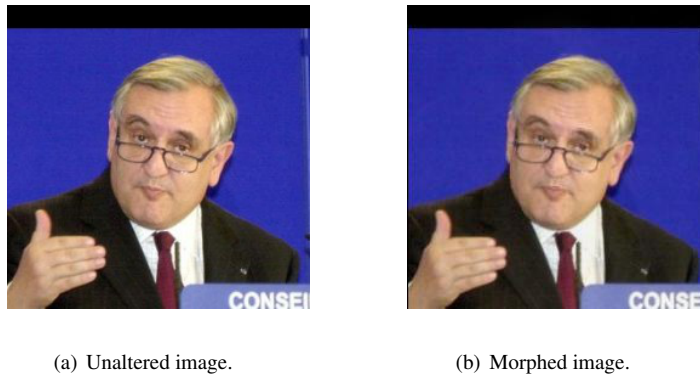


Figure 6.1: Initial and final (misidentified) images of subject number 17.

The experiments' results are also conditioned by other parameters such as the size of the database or the amount of morphing per iteration. The bigger the database, the more possible morphing combinations. With a smaller percentage of morphing added at each iteration, we could get closer to an optimal result in exchange for increasing the number of iterations.

CONCLUSIONS

In the literature, one can find several approaches to deal with impersonation in facial verification systems. However, it is not the case when face identification is required. Our experiments show that some well-known methods like EigenFaces, FisherFaces, or SIFT completely fail in such a task.

More recent techniques based on Deep Learning like FaceNet offer better results than the others. FaceNet can robustly identify images that have less than 15% morphing alteration. When dealing with images with higher morphing alteration, we propose the addition of an S-MAD. This combination offers a highly secure and robust solution that can be used to prevent attacks, for example, in online registration processes.

Moreover, we have presented a new way of attacking face identification systems that minimizes the chances of being detected by both face identification and morphing detectors: stegano-morphing. The results outperform previous morphing techniques by 700% in the best case and 200% in the worst one. A soft modification of 30% of the original image is enough to make the best identification algorithm misclassify almost 90% of the subjects.

In this work, we have tested recognition algorithms from different types. It seems that the ones based on Deep Learning outperform other families by far. In future work, we propose to evaluate other Deep Learning-based facial recognition algorithms.

BIBLIOGRAPHY

- [1] S. F. Kak, F. M. Mustafa, P. Valente, "A review of person recognition based on face model," *Eurasian Journal of Science & Engineering*, vol. 4, issue 1, pp. 157–168, 2018. [Online]. Available doi: 10.23918/eajse.v4i1sip157.
- [2] A. Shwetank, P. Neeraj, and B. Karamjit, "Future of face recognition: A review," *Second International Symposium on Computer Vision and the Internet*, vol. 58, pp. 578–585, 2015.
- [3] E. P. Ijjina, G. Kanahasabai and A. S. Joshi, "Deep learning based approach to detect customer Age, gender and expression in surveillance video," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1–6. [Online]. Available doi: 10.1109/ICCCNT49239.2020.9225459.
- [4] V. Mirchandani, *17 Best Smartphones with Face Unlock You Can Buy Right Now*, Beebom, March 2019. Accessed on: Nov. 18, 2020. [Online]. Available [here](#).
- [5] "System, method, and computer program product for verifying the identity of social network users," by S. Ufford and J. Tanis (2012, Nov. 20). U.S. Patent No 8,316,086. Accessed 18 Nov. 2020. [Online]. Available [here](#).
- [6] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084–1097, July 2014. [Online]. Available doi: 10.1109/TIFS.2014.2322255.
- [7] "Anonymous," HKU University of the Arts Utrecht. Accessed on: Nov. 16, 2020. [Online]. Available [here](#).
- [8] M. Ferrara, A. Franco and D. Maltoni "The magic passport," in *IEEE International Joint Conference on Biometrics*, Clearwater, FL, 2014, pp. 1–7. [Online]. Available doi: 10.1109/B-TAS.2014.6996240.
- [9] A. Agrawal and S. Samson, "A review on feature extraction techniques and general approach for face recognition," *International Journal of Computer Applications Technology and Research*, vol. 5, issue 3, pp. 156–158, 2016.
- [10] Y. Kortli, M. Jridi, A. Al Falou and M. Atri, "Face recognition systems: A survey," *Sensors*, vol. 20, no. 2:342, 2020. [Online]. Available doi: 10.3390/s20020342.
- [11] M. Wang and W. Deng, "Deep face recognition: A survey," 2018, *arXiv:1804.06655*. [Online]. Available [here](#).
- [12] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," in *Proceedings of Computer Vision and Pattern Recognition IEEE Computer Society*, June 1991, pp. 586–591.
- [13] P. N. Belhumeur, J. P. Hespanha and D. J. Kriegman, "Eigenfaces vs fisherfaces: Recognition using class specific linear projection," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 711–720, 1997. [Online]. Available doi: 10.1109/34.598228.

- [14] M. S. Bartlett, J. R. Movellan and T. J. Sejnowski, "Face recognition by independent component analysis," *IEEE Trans. Neural Networks*, vol. 13, no. 6, pp. 1450–1464, Nov. 2002. [Online]. Available doi: 10.1109/TNN.2002.804287.
- [15] S. F. Hafez, M. M. Selim and H. H. Zayed, "2D face recognition system based on selected gabor filters and linear discriminant analysis LDA," *IJCSI International Journal of Computer Science Issues*, vol. 12, no. 1, pp. 33–41, 2015.
- [16] G. Zhang, X. Huang, S. Z. Li, Y. Wang and X. Wu, "Boosting local binary pattern (LBP)-based face recognition," in *Proc. of the 5th Chinese conference on Advances in Biometric Person Authentication*, 2004, pp. 179–186. [Online]. Available doi: 10.1007/978-3-540-30548-4_21.
- [17] M. Bicego, A. Lagorio, E. Grosso and M. Tistarelli, "On the Use of SIFT Features for Face Authentication," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, New York, NY, USA, 2006, pp. 35–35. [Online]. Available doi: 10.1109/CVPRW.2006.149.
- [18] G. Du, F. Su and A. Cai, "Face recognition using SURF features," in *MIPPR 2009: Pattern Recognition and Computer Vision*, International Society of Optics and Photonics; SPIE, vol. 7496, 2009, pp. 749628.1–749628.7. [Online] Available doi: 10.1117/12.832636.
- [19] A. A. Fathima, S. Ajitha, V. Vaidehi, M. Hemalatha, R. Karthigaiveni and R. Kumar, "Hybrid approach for face recognition combining gabor wavelet and linear discriminant analysis," in *2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)*, Bhubaneswar, 2015, pp. 220–225. [Online]. Available doi: 10.1109/CGVIS.2015.7449925.
- [20] Y. Taigman, M. Yang, M. Ranzato and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2014, pp. 1701–1708. [Online]. Available doi: 10.1109/CVPR.2014.220.
- [21] Y. Sun, D. Liang, X. Wang and X. Tang, "Deepid3: Face recognition with very deep neural networks," *arXiv preprint arXiv:1502.00873*, 2015.
- [22] F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823. [Online]. Available doi: 10.1109/CVPR.2015.7298682.
- [23] O. M. Parkhi, A. Vedaldi and A. Zisserman, "Deep face recognition" in *Proc. British Machine Vision Conf.*, Jan. 2015, pp. 41.1–41.12.
- [24] J. Deng, J. Guo, N. Xue and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4690–4699. [Online]. Available doi: 10.1109/CVPR.2019.00482.
- [25] G. B. Huang, M. Ramesh, T. Berg and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," University of Massachusetts, Technical Report 07-49, Oct. 2007.
- [26] A. K. Agrawal and Y. N. Singh, "Evaluation of face recognition methods in unconstrained environments," *Procedia Computer Science*, vol. 48, pp. 644–751, 2015.
- [27] X. Zhang and Y. Gao "Face recognition across pose: A review," *Pattern Recognition*, vol. 42, no.

- 11, pp. 2876–2896, 2009. [Online]. Available doi: 10.1016/j.patcog.2009.04.017.
- [28] G. H Givens, J. R. Beveridge, P. J. Phillips, B. Draper, Y. M. Lui and D. Bolme, “Introduction to face recognition and evaluation of algorithm performance,” *Computational Statistics and Data Analysis*, vol. 67, pp. 236–247, 2013. [Online]. Available doi: 10.1016/j.csda.2013.05.025.
- [29] D. B. Smythe, “A Two-Pass Mesh Warping Algorithm for Object Transformation and Image Interpolation,” Technical Memo 1030, Industrial Light and Magic, Computer Graphics Department, Lucasfilm Ltd., 1990.
- [30] G. Wolberg, *Digital Image Warping*, IEEE Computer Society Press, Los Alamitos, California, 1990.
- [31] G. Wolberg, “Image morphing: A survey,” *The Visual Computer*, vol. 14, no. 8–9, pp. 360–372, 1998.
- [32] M. Steyvers, “Morphing techniques for manipulating face images,” *Behavior Research Methods*, vol. 31, no. 2, pp. 359–369, 1999. [Online]. Available doi: 10.3758/BF03207733.
- [33] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt and C. Busch, “Face recognition systems under morphing attacks: A survey,” *IEEE Access*, vol. 7, pp. 23012–23026, 2019. [Online]. Available doi: 10.1109/ACCESS.2019.2899367.
- [34] G. Bradski and A. Kaehler, *Learning OpenCV: Computer Vision with the OpenCV Library*. Sebastopol, CA, USA: O’Reilly Media, 2008.
- [35] N. Damer, A. M. Saladié, A. Braun and A. Kuijper, “MorGAN: Recognition Vulnerability and Attack Detectability of Face Morphing Attacks Created by Generative Adversarial Network,” *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Redondo Beach, CA, USA, 2018, pp. 1–10. [Online]. Available doi: 10.1109/BTAS.2018.8698563.
- [36] M. Gómez-Barrero, C. Rathgeb, U. Scherhag and C. Busch, “Is your biometric system robust to morphing attacks?,” in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, Coventry, 2017, pp. 1–6. [Online]. Available doi: 10.1109/IWBF.2017.7935079.
- [37] S. Mallick, *Face Morph Using OpenCV - C++/Python*, Learn OpenCV, March 11, 2016. Accessed on: January 21, 2021. [Online]. Available [here](#).
- [38] A. Hadid, N. Evans, S. Marcel and J. Fierrez, “Biometrics systems under spoofing attack: An evaluation methodology and lessons learned,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 20–30, Sept. 2015. [Online]. Available doi: 10.1109/MSP.2015.2437652.
- [39] A. Mohammadi, S. Bhattacharjee and S. Marcel, “Deeply vulnerable: A study of the robustness of face recognition to presentation attacks,” *Institution of Engineering and Technology Biometrics*, vol. 7, issue 1, pp. 15–26, 2018. [Online]. Available doi: 10.1049/iet-bmt.2017.0079.
- [40] M. Ferrara, A. Franco and D. Maltoni, “On the effects of image alterations on face recognition accuracy,” in *Face Recognition Across the Image Spectrum*. Springer Nature, 2016, pp. 195–222.
- [41] R. Tolosana, R. Vera-Rodríguez, J. Fierrez, A. Morales and J. Ortega-García, “DeepFakes and beyond: A survey of face manipulation and fake detection,” *arXiv preprint arXiv:2001.00179*, 2020.
- [42] D. J. Robertson, R. S. S. Kramer and A. M. Burton, “Fraudulent ID using face morphs: Experiments on human and automatic recognition,” *PLoS ONE*, vol. 12, no. 3:e0173319. [Online]. Available doi:

doi:10.1371/journal.pone.0173319.

- [43] L. Wandzik, R. V. García, G. Kaeding and X. Chen, “CNNs under attack: On the vulnerability of deep neural networks based face recognition to image morphing,” in *Proc. 16th Int. Workshop on Digital Forensics and Watermarking*, 2017, pp. 121–135.
- [44] U. Scherhag, R. Raghavendra, K.B. Raja, M. Gómez-Barrero, C. Rathgeb and C. Busch, “On the vulnerability of face recognition systems towards morphed face attacks,” in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, Coventry, 2017, pp. 1–6. [Online]. Available doi: 10.1109/IWBF.2017.7935088.
- [45] P. Korshunov and T. Ebrahimi, “Using face morphing to protect privacy,” in *2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance*, Krakow, 2013, pp. 208–213. [Online]. Available doi: 10.1109/AVSS.2013.6636641.
- [46] U. Scherhag *et al.*, “Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting,” in *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, 2017, pp. 1–7. [Online]. Available doi: 10.23919/BIOSIG.2017.8053499.
- [47] M. Sharif, F. Naz, M. Yasmin, M. A. Shahid, and A. Rehman, “Face recognition: A survey,” *Journal of Engineering Science and Technology Review*, vol. 10, no. 2, pp. 166–177, 2017.
- [48] S. Patel, *Face Morphing*, Github, 2018. Accessed on: Nov.29, 2020. [Online]. Available [here](#).
- [49] B. Delaunay “Sur la sphère vide. A la mémoire de Georges Vorono,” *Bulletin de l’Académie des Sciences de l’URSS. Classe des sciences mathématiques et naturelles* vol. 6, p. 793, 1934.
- [50] D. E. King, “Dlib-ml: A machine learning toolkit,” *Journal of Machine Learning Research (JMLR)*, vol. 10, pp. 1755–1758, 2009.
- [51] T. Ahonen, A. Hadid and M. Pietikainen, “Face Description with Local Binary Patterns: Application to Face Recognition,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037–2041, Dec. 2006. Available doi: 10.1109/TPAMI.2006.244.
- [52] R. Raja, *Face Recognition with OpenCV and Python*, Github, 2017. Accessed on: Nov. 29, 2020. [Online]. Available [here](#).
- [53] V. Garg and K. Garg, “Face recognition using haar cascade classifier,” *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 3, no. 12, December 2016.
- [54] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, *et al.* “Scikit-learn: Machine learning in Python,” *the Journal of machine Learning research*, vol. 12, pp. 2825–2830, 2011.
- [55] W. Noble, “What is a support vector machine?,” *Nature Biotechnology*, vol. 24, pp. 1565–1567, 2006. [Online]. Available doi: 10.1038/nbt1206-1565.
- [56] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis *et al.* “Tensorflow: A system for large-scale machine learning,” in *12th USENIX symposium on operating systems design and implementation (OSDI 16)*, 2016, pp. 265–283.
- [57] D. Sandberg, *Face Recognition using Tensorflow*, Github, 2016. Accessed on: Nov. 29, 2020.

- [Online]. Available [here](#).
- [58] Q. Cao, L. Shen, W. Xie, O. M. Parkhi and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*, Xi'an, 2018, pp. 67–74. [Online]. Available doi: 10.1109/FG.2018.00020.
- [59] C. Szegedy, S. Ioffe, and V. Vanhoucke, "Inception-v4, inception-resnet and the impact of residual connections on learning," *arXiv preprint arXiv:1602.07261*, 2016.
- [60] J. Galbally, S. Marcel and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014. [Online]. Available doi: 10.1109/ACCESS.2014.2381273.
- [61] R. Raghavendra, K. B. Raja, and C. Busch. "Detecting Morphed Face Images," in *8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pp. 1–8, 2016.
- [62] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch and A. Uhl, "Detection of face morphing attacks based on PRNU analysis," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 4, pp. 302–317, Oct. 2019. [Online]. Available doi: 10.1109/TBIOM.2019.2942395.
- [63] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in *Digital Forensics Watermarking*. Cham, Switzerland: Springer, 2017, pp. 107–120.
- [64] L. Zhang, F. Peng and M. Long, "Face morphing detection using Fourier spectrum of sensor pattern noise," in *2018 IEEE International Conference on Multimedia and Expo (ICME)*, San Diego, CA, 2018, pp. 1–6. [Online]. Available doi: 10.1109/ICME.2018.8486607.
- [65] R. Raghavendra, K. Raja, S. Venkatesh and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, Denver, CO, 2017, pp. 555–563. [Online]. Available doi: 10.1109/BTAS.2017.8272742.
- [66] L. Spreeuwers, M. Schils and R. Veldhuis, "Towards robust evaluation of face morphing detection," in *2018 26th European Signal Processing Conference (EUSIPCO)*, Rome, 2018, pp. 1027–1031. [Online]. Available doi: 10.23919/EUSIPCO.2018.8553018.
- [67] W. Deng, J. Hu, N. Zhang, B. Chen and J. Guo, "Fine-grained face verification: FGLFW database, baselines, and human-DCMN partnership," *Pattern Recognition*, vol. 66, pp.63–73, 2017.
- [68] C. R. Harris, K. J. Millman, S. J. van der Walt *et al.* "Array programming with NumPy," *Nature*, vol. 585, num. 7825, pp. 357–362, 2020. [Online]. Available doi: 10.1038/s41586-020-2649-2.
- [69] E. Learned-Miller, G. Huang, A. RoyChowdhury, H. Li, Haoxiang and G. Hua., "Labeled Faces in the Wild: A Survey," in *Advances in Face Detection and Facial Image Analysis*, 2016, pp. 189–248. [Online]. Available doi: 10.1007/978-3-319-25958-1_8.

TERMINOLOGY

complete attack A morphing attack that manages to fool both the facial identification algorithm and the morphing detector.

FAR vs. FRR curve It represents, for each **threshold** value, the **False Acceptance Rate (FAR)** and the **False Rejection Rate (FRR)**. That is to say, in the case of the morphing detector, for each **threshold** confidence, the percentage of genuine images that are classified as morphing (**FAR**) and the percentage of morphed images that are classified as genuine (**FRR**).

full m -ary tree Rooted tree where each node has 0 or m child nodes.

ghost artifact Part of a morphed image that, due to mismatched or unaligned elements of the two subjects involved, appears blurred or shaded.

heuristic A method designed to solve more efficiently a complex and costly problem. It does not necessarily find the most optimal solution but an approximation.

ROC curve The **Receiver Operating Characteristic (ROC)** curve represents the **FAR** against the **True Acceptance Rate (TAR)**. That is to say, in the case of the morphing detector, the percentage of genuine images that are classified as morphing (**FAR**) against the percentage of morphed images that are classified as morphing ($TAR = 1 - FRR$).

threshold The confidence that must be exceeded to classify the entry with a certain label.

unconstrained database Database containing images taken in uncontrolled scenarios. The photos may present different conditions of lighting, background, occlusions, or poses.

ACRONYMS

ABC Automated Border Control.

CNNs Convolutional Neural Networks.

D-MAD Differential Morphing Attack Detection.

FAR False Acceptance Rate.

FRR False Rejection Rate.

GAN Generative Adversarial Networks.

ICA Independent Component Analysis.

LBP Local Binary Pattern.

LBPH Local Binary Patterns Histogram.

LDA Linear Discriminative Analysis.

LFW Labeled Faces in the Wild.

PCA Principal Component Analysis.

ROC Receiver Operating Characteristic.

SIFT Scale-invariant Feature Transform.

SLLFW Similar-looking LFW.

S-MAD Single Image Morphing Attack Detection.

SURF Speeded-up Robust Features.

SVM Support Vector Machine.

TAR True Acceptance Rate.

APPENDICES

DETAILED RESULTS OF THE ROBUSTNESS AGAINST MORPHING

In tables A.1 to A.5, all the results of the face recognizers' comparison against traditional morphing are presented. For each recognizer, the tables show in what percentages of morphing alteration is the original or the target subject identified (Column A for the original subject and B for the target). Column No. reflects the pair number (to see the individuals' names check Table 4.1). Pos. 1, Pos. 2–3 and Pos. 4–5 represent the first, second and third, fourth and fifth positions (respectively) of each face recognition algorithm's top identification matches. For clarity, rows of couples that have not been identified within the top 5 at any percentage have been deleted.

No.	Pos. 1		Pos. 2–3		Pos. 4–5	
	A	B	A	B	A	B
1	72–100	–	70–71	98–100	69	94
2	–	–	–	–	–	72–76
4	0–20	–	21–34	–	35–37	–
5	100	–	91–92, 95–99	95–100	93–94	92, 94
6	–	–	–	–	–	94–95, 97–100
8	0–15	72–89	16–19	52–71, 90–100	20–28	48–51
10	43–92	–	9–42, 93–97, 100	–	0–8, 98–99	–
13	–	–	0–16,38	–	17–20, 27, 29–30, 35, 39–41, 43–44	–
15	–	95–100	–	82–94	0–12, 14–16	77–81
16	–	–	–	56, 59–69, 71–82	–	51–55, 57–58,70, 83–89, 91–92
18	30–31, 33–38, 40–44, 46–47, 53, 55, 60–62, 74	–	25–29, 32, 39, 45, 48–52, 54, 56–59, 63–73, 77	–	22–24, 75–76,78, 80, 86–89, 91–92, 98–100	–
19	–	–	–	89, 91	–	71–88, 90, 92–100
20	0–12, 15	–	13–14, 16–19	–	20–25, 54, 56, 58, 63	–
22	–	–	–	–	–	40–41, 49, 51–54
24	0–54	–	55–60	14–19	61–63	0–13, 20–22
25	–	–	–	64, 67–71, 73, 77, 80–83	–	61–63, 65–66, 72, 75–76, 78–79, 84–90, 92–93

Table A.1: Complete results of the robustness of Eigenfaces against traditional morphing.

No.	Pos. 1		Pos. 2-3		Pos. 4-5	
	A	B	A	B	A	B
4	0-28, 34-36	-	29-33, 37-50	-	51-52, 59	-
7	-	-	-	-	-	53-54, 58-59, 62-68, 70-75, 77-81, 83-93, 95, 98-99
12	33, 69, 81	-	70-74, 77, 79, 84, 86-87	-	41, 50, 65-68, 75-76, 78, 80-81, 83, 85, 89, 91, 93	-
13	-	-	-	-	-	87, 99
15	-	-	0-1	-	-	-
16	-	-	-	100	-	-
17	-	-	-	50-51, 94	-	52-57, 60, 62-63, 81, 83, 96, 99-100
18	-	-	25-26	-	-	27
19	0-1, 3, 6	28-29, 77-78	2, 4-5, 7-13, 16-17, 19	25-26, 31, 33, 35, 75-76	15	15, 24, 27, 30, 32, 74, 83, 85
20	-	-	0-4	-	5, 11, 55, 60-62	-
25	-	-	2	-	0	-

Table A.2: Complete results of the robustness of Fisherfaces against traditional morphing.

No.	Pos. 1		Pos. 2-3		Pos. 4-5	
	A	B	A	B	A	B
1	38-39, 47-48, 50	-	40-41, 45, 49, 51, 53-55, 65, 75, 78-79, 81-90, 92, 94	-	25, 30, 35-36, 42-44, 52, 56-60, 64, 77, 80, 91, 93	90, 100
2	-	37-38, 40-100	-	34-36, 39	28	-
3	-	-	-	-	30	-
4	-	95-96	6	69-81, 83-86, 88, 90-94	1-2, 44, 47, 51-52, 54-56, 66-67, 90-94, 97-100	82, 87, 89
5	90-95, 97-98	-	67-68, 70-79, 83-85, 87-89, 96, 99-100	-	61, 63-66, 69, 81-82, 86	-
7	-	-	17, 26-27, 29, 31, 33, 36, 44	-	22, 24, 30, 37, 39, 41, 43, 45	-
8	0-6, 8-19, 23-24	85-86, 97-100	7, 20-22, 25-35, 39	82-84, 87-92, 94-96	36-38, 46	93
9	-	-	-	-	0, 3, 20-22, 24-32, 36, 40, 44, 51-52, 63, 78, 80-82, 84, 87	-
12	5-6	46, 54-85, 96	4	44-45, 47-53, 86-95, 97-100	2-3	37, 42-43
13	0-5, 7-15, 22, 44, 51-57	98-100	6, 16-21, 23-43, 45-50, 58-60	78, 80, 83-90, 92-97	61-62	76-77, 79, 81-82, 91
14	-	-	-	-	0-1, 3, 7-14, 20-23, 25-26, 28	-
15	0-21, 26-32, 34-35, 37, 39-42	43-100	22-25, 33, 36, 38, 43-44, 49-52, 70, 74, 85, 87, 90	41	45-48, 53, 71, 76, 82, 86, 88, 91	31-40, 42
16	0-13, 15	56, 63-64, 70, 77, 79, 81-100	14, 16, 20	49, 53-55, 57-62, 65-67, 69, 71-76, 78, 80	17, 19, 21	50-51, 68
17	-	23-25, 27-28, 30-71, 73-100	-	20-22, 26, 29, 72	10	16-19
18	0-80, 83-85, 87-94	-	81-82, 86, 95-100	82, 86, 89-92	-	47-48, 59, 61-81, 83-85, 87-88, 93-97
19	0-1, 3-11	31, 42, 44, 57-58	2, 18-19, 21-23, 28	9-11, 14, 32-40, 46-48, 59, 65-67, 71-95, 99-100	14-17, 20, 24-27	7, 12-13, 15-16, 19, 24, 28-30, 41, 45, 49-51, 54-55, 61-64, 68, 70, 96-98
20	0-35, 37-54, 56-67	81, 86, 91-97, 99-100	36, 55, 68-69	85, 87, 89-90, 98	70-72, 74, 76	84, 88
22	-	-	-	45, 48-49, 51-63	-	46-47, 50, 64
24	0-50	-	51, 53, 55-56	-	52, 54, 58	-
25	2	-	0-1, 3-16, 19-22, 31, 33	94-99	17-18, 23, 32, 34, 36	86

Table A.3: Complete results of the robustness of LBPH against traditional morphing.

No.	Pos. 1		Pos. 2-3		Pos. 4-5	
	A	B	A	B	A	B
1	-	55, 71, 75, 86, 95-96	-	39, 59, 62, 64-65, 67, 69-70, 72-74, 82, 76-79, 88, 90, 94, 97	-	61, 84-85, 93, 98
3	43-44	-	38, 46-47, 49, 52, 55, 97	-	37, 42, 53, 57	-
4	-	67, 81, 86-87, 89-100	-	58, 66, 69-70, 78-80, 82-84, 88	9	55, 85
5	34, 79, 81	-	33, 82	-	21, 29, 73, 83	-
6	-	-	5	-	-	-
8	68-69, 80, 82, 84-85	-	23, 72, 75, 79, 96	63	5, 24, 86	-
9	39	10, 33-37, 39-40, 50, 54, 57-59, 64-65, 67-68, 70, 86-87, 93	49	31-32, 38, 41-43, 45, 51, 53, 56, 60-63, 69, 71-73, 75, 83-84, 94, 96, 99	-	49, 95
10	-	32, 34, 50	-	33, 36	-	-
11	10	70	4, 11	-	-	-
12	18, 20, 22, 28-29, 38	-	1-2, 8, 12-14, 19, 25-27, 30-31, 33-34, 75	55, 60, 76, 80	0, 4, 10	-
13	0-9, 11, 13-14, 16, 18, 30-31	-	10, 15, 17, 20-22, 27, 29, 32	43, 80, 91	12, 25	-
15	3, 11-12, 14, 16-19, 21, 27-33, 35-43, 45-49, 51-52, 56, 60	55-56, 59-100	0-2, 4, 7-8, 10, 22-26, 34, 44, 50, 58-59, 61-62, 69, 71, 77, 80, 81-87, 91-94, 99-100	50, 54, 58	5-6, 67, 89	52, 57
16	0, 10, 14, 17-19, 22, 27	-	6, 9, 15-16, 20, 23-24, 28-30, 33	-	25-26, 32	-
17	-	33-40, 42-44, 47-53, 56, 58, 61, 66-68, 70-100	-	0, 13, 41, 46, 54, 57, 62, 65	-	8, 32, 45, 69
18	0-10, 12, 13, 16-18, 20, 23, 25, 28-30, 34, 39, 43-51, 53-54, 57, 64	62, 73, 77, 81	11, 14, 27, 33, 35-37, 52, 55, 59	56, 65, 76, 79-80	38	83
19	-	-	12	-	-	45
20	6, 8, 11, 13-15, 21, 25, 27, 29	-	7, 10, 16, 19-20, 31, 53	-	9, 28, 38	-
21	0, 3, 20, 27	72	13, 15-16, 18-19, 21-22, 26-26	73-75	-	0
22	-	-	-	18, 36, 47	-	34, 48
23	-	-	15, 18, 44	-	-	-
24	-	76	-	75, 84, 95, 99	8	-
25	10, 18, 94	-	11-12, 14-17, 19-20, 30, 51, 91, 95-96	-	13, 31-32, 45	-

Table A.4: Complete results of the robustness of SIFT against traditional morphing.


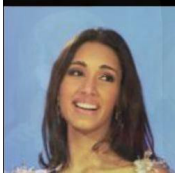


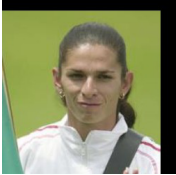








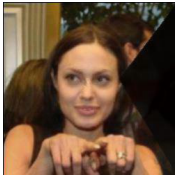
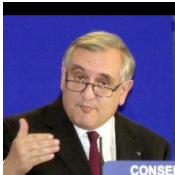

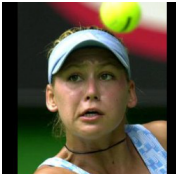
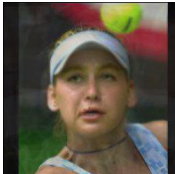
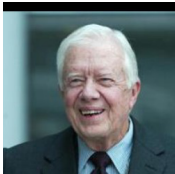

	Pos. 1		Pos. 2-3		Pos. 4-5	
1	-	45-100	0-7	32-44	8-19, 21	20, 22-31
2	0-24	25-100	25-43	8-24	44-49	4-7
3	0-72, 74	75-100	73, 75-100	65, 68, 71-74	-	18, 20-21, 23-25, 33-34, 36-39, 42-64, 66-67, 69-70
4	0-54	60-100	55-58	54-59	59-64	44-53
5	0-77	78-100	78-100	0-77	-	-
6	-	41-100	-	37, 39-40	0-4, 6	33-34, 36, 38
7	0-64	71-100	65-68	69-70	69-73	63, 65-68
8	0-36	37-39, 41, 75-100	37	30-36, 40, 42-74	38-39, 41-44	10, 17-29
9	0-14, 18	66-100	15-17, 19-70, 72-73	47, 49-65	71, 74-79	27-46, 48
10	0-47	67-100	48-62	56-66	63-66	54-55
11	0-48, 52	53, 55-100	49-51, 53-65	47-52, 54	66	41-46
12	0-46, 48	47, 49-100	47, 49-54, 56	32, 34-46, 48	55, 57-58	29-31, 33
13	0-37, 39	38, 40-100	38, 40-72, 74	17-37, 39	73, 75-76	10-16
14	0-21, 35	78-100	22-34, 36-67	68-77	68-71, 73-75	66-67
15	0-54	55-100	55-96, 98-99	21-22, 26-54	97, 100	14-17, 19-20, 23-25
16	0-55	65-100	56-61, 63	55, 57-64	62, 64-70	41, 45-54, 56
17	5, 7-36	37-100	0-4, 6, 37-74, 78	0-3, 5-36	75-77, 79-94	4
18	0-53	54-100	54-71	50-53	72-75, 77-80, 82	46-49
19	0-42	49, 52-100	43-69	22-48, 50-51	70-82	16, 19-21
20	0-14, 16-19, 21-24	20, 25-54, 56-57, 59, 61-100	15, 20, 25-35	21-24, 55, 58, 60	36-38, 40, 42-48, 52, 60-67, 69-70	12-19
21	0-45	46-100	46-81	21-45	82-91	14, 16-20
22	-	62, 64-100	0-18	33-61, 63	19-24	25-32
23	0-26	-	27-55	-	56-67	69-70, 73-100
24	0-20, 22-25	21, 26-100	21, 26-45	0-20, 22-25	46-56, 58	-
25	0-80	81-100	81-88	34-80	89-98	1-33










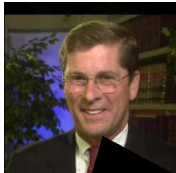

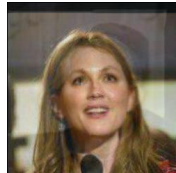



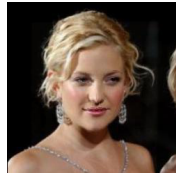










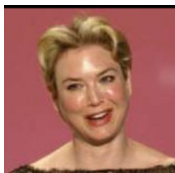

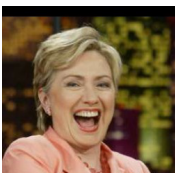
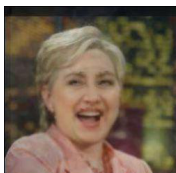
Table A.5: Complete results of the robustness of FaceNet against traditional morphing.

DETAILED RESULTS OF THE PROPOSED METHOD

Table B.1 presents the results of our proposed morphing attack. It shows all the original subjects' portraits and their respective images produced by our method that achieve misidentification with FaceNet and reduces the amount of morphing needed. Column *No.* reflects the image number (check Table 4.2), *It.* the number of iterations needed to get the misidentification and *Mor. conf.* the morphing detector confidence of the misidentified image.

Table B.1: Complete results of the proposed method.

No.	Initial image	Final image	It.	Mor. conf.	No.	Initial image	Final image	It.	Mor. conf.
1			3	100	14			1	98
2			4	100	15			2	100
3			2	0.2	16			7	100
4			3	100	17			1	100
5			8	42.75	18			6	100

6			1	0	19			4	100
7			2	99.63	20			1	78.85
8			1	0.13	21			7	100
9			3	99.98	22			1	0
10			7	100	23			1	0
11			4	100	24			1	100
12			9	100	25			3	100
13			9	100					

UAM

UNIVERSIDAD AUTONOMA
DE MADRID