Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Himali Aryal

Morphing Attacks and Detection using Spectral Images

Master's thesis in Applied Computer Science
Supervisor: Assoc. Prof. Kiran Raja
Co-supervisor: Prof. Raghavendra Ramachandra
June 2022

NTNU
Kunnskap for en bedre verden

Himali Aryal

Morphing Attacks and Detection using Spectral Images

Master's thesis in Applied Computer Science
Supervisor: Assoc. Prof. Kiran Raja
Co-supervisor: Prof. Raghavendra Ramachandra
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Morphing Attacks and Detection using Spectral Images

Master's thesis in Master in Applied Computer Science

Himali Aryal
Supervisor(s): (1) Assoc. Prof. Kiran Raja
(2) Prof. Raghavendra Ramachandra

June 1, 2022

Abstract

Face recognition systems assume that a person's face serves as the unique link to identify them. A morph attack happens when two people with similar facial features morph their faces together, resulting in a face image that can be identified as either of the two contributing individuals. Since the morphed image inherit enough visual traits from both individuals, both humans and automatic algorithms could be deceived by a morphed image. In terms of biometrics, changing one's appearance to impersonate a target identity is a direct attack on the security of face recognition systems. Defending against such attacks necessitates the ability to detect them as distinct identities from their target.

Although they are not always visible in the image domain, many morphing algorithms introduce artifacts in the final image that can be used to detect morph attacks. Since various spectral images allow us to investigate low and high-frequency data separately, we can recognize and isolate these morphing abnormalities in the spatial frequency domain. For this research, we develop a new database that includes the morphed images created using three different techniques and spectral images in different spectral bands. This study studies the potential attack of various efficient face recognition systems from the newly created database using spectral images as a reference set. In addition, this thesis also investigates the human observer's ability to detect the morphed images while examining spectral images. Further, we evaluate the effectiveness of different MAD approaches using spectral bands imaging in order to detect differential morph attacks.

Acknowledgement

I would to express my sincere gratitude to my supervisor Assoc. Prof. Kiran Raja for the continuous guidance and support throughout the thesis works. His competent supervision on a regular basis helped me perform my best everyday and I would forever be indebted for his guidance.

Secondly, I want to acknowledge Prof. Raghavendra Ramachandra, for providing raw spectral images for the research purpose which formed as the base of the experiment performed in this dissertation.

Last but not least, I would like to thank my friends and family for their constant support throughout the process without which this work would not have been possible.

Himali Aryal

Contents

Figures

Tables

Acronyms

ABC Automatic Boarder Control. 1, 15

APCER Attack Presentation Classification Error Rate. 43, 49

BPCER Bonafide Presentation Classification Error Rate. 43, 49

BSIF Binarized Statistical Image Features. 14, 15, 47, 48, 49, 50, 57, 59

COTS Commercial Off-The-Shelf. 3, 29, 31, 34, 35, 56, 59, 60

DET Detection Error Tradeoff. 49, 50

D-MAD Differential Morphing Attack Detection. vii, 9, 14, 16, 18, 39, 42

EER Equal Error Rate. 49

eMRTD electronic machine-readable travel documents. 1

FMMPMR Fully Mated Morphed Presentation Match Rate. viii, 31, 33, 34, 35, 59

FMR False Match Rate. 30

FNMR False Non-Match Rate. 34

FRS Face Recognition System. 1, 3, 8, 9, 10, 18, 21, 29, 31, 32, 34, 35, 36, 56, 59, 60

GAN Generative adversarial networks. 2, 18, 55

GDPR General Data Protection Regulation. 41, 42

HOG Histogram of Gradients. 15

ICAO International Civil Aviation Organization. 1, 55

LBP Local Binary Patterns. 14, 15, 47, 48, 49, 57, 59

LMA Landmark Aligned. 3, 7, 9, 25, 31, 35, 36, 39, 44, 49, 50, 59

MAD Morphing Attack Detection. iii, 3, 4, 9, 13, 14, 18, 19, 24, 43, 48, 49, 50, 59, 60

MIPGAN Morphing through Identity Prior driven GAN. 3, 9

MIPGAN-I Morphing through Identity Prior driven GAN - I. 9, 25, 31, 35, 36, 39, 44, 49, 50, 59, 60

MMPMR Mated Morphed Presentation Match Rate. viii, 31, 32, 33, 34, 35, 36, 59

NIR Near-infrared. 2, 21

NTNU Norges Teknisk-Naturvitenskapelige Universitet. 9, 41, 42

RBF Radial Basis Function. 47, 48

RGB Red Green Blue. 3, 19, 21, 22, 24, 30, 39, 42, 43, 48, 56, 57

RMMR Relative Morph Match Rate. viii, 31, 34

SIFT Scale Invariant Feature Transform. 15

S-MAD Single Morphing Attack Detection. 9, 18

SURF Speeded Up Robust Features. 15

SVC Support Vector Classifier. 47

SVM Support Vector Machine. 15, 47, 48, 57

UBO University of Bologna. 3, 9, 25, 31, 34, 35, 36, 39, 44, 50, 59

VIS visible spectrum. 2, 21

Chapter 1

Introduction

1.1 Introduction and Problem statement

Face recognition is an essential biometric technique that has been widely utilized in identity verification, such as in banking, hotels, transit, and other areas. Face recognition technology was gradually implemented in the Automatic Border Control (ABC) system after the International Civil Aviation Organization (ICAO) [1] approved the human face as a biometric feature in electronic machine-readable travel documents (eMRTD). Recently, many attacks against face recognition systems have been discovered, the most significant of which is the face morphing attack, which poses a severe threat to existing face recognition systems (FRS) [2].

Face, fingerprint, and iris are some features that distinguish one individual from another, and the measurement and statistical analysis of these features is known as biometrics. Based on the biometrics data, a biometric recognition system is perceived, which refers to the identification and authentication of the user with unique biometrics attributes. Similarly, the Face Recognition System (FRS) is a system that uses facial characteristics to identify or verify a user's identity. It aims to extract distinguishing aspects from the face and authenticate user identity using facial attributes such as the distance between the shape of the chin, depth of eye sockets, distance between forehead and chin, curves of lips, ears, and chin, or chin mapping. Analyzing the current biometrics recognition scenario, face recognition systems (FRS) are becoming popular in image-based identity management systems globally, such as passport, national ID cards, border access control, surveillance, banking services, smartphone authentication, and so on. According to ICAO [1], face image is required in all passports, and most European nations have national ID cards that use a facial image as the primary mode of identification. Face image has also become a standard modality for issuing ID cards in big ID management systems in some countries. All of this makes FRS highly relevant to present and future use. Furthermore, automatic facial recognition is already the principal mode of identification verification for most automated border controls across the world. While live enrollment is preferred when granting travel or identity documents, some countries still require applicants to submit a passport photo,

thus making the system vulnerable to face morphing attack.

Face morphing is an image transformation technique that combines the faces of two people with similar facial traits, resulting in a morphed image that looks like both contributing subjects. As morphed image can look similar to both people whose face is morphed, it can be challenging to human as well as face recognition algorithms to detect the morphed image. If morphing images are utilized in travel or identity documents, several subjects will be able to authenticate their identity against the document's owner. Thus, face morphing poses a significant security threat to the immigration system and other identity verification areas. For example, face morphing in passport enrollment procedure allows a criminal to morph his face into that of an accomplice, who can then apply for a passport with the morphed face image. This way, the criminal acquires a genuine travel document that allows them to travel borders and enter restricted areas that would otherwise be closed to them. Since a morphed passport photo allows someone who is not previously authorized to enter a country undetected, face morphing attacks have become a serious security threat for face recognition systems, which assume that a person's identity is linked to their face.

1.2 Justification, Motivation and Benefits

The face morphing technique combines two face images of distinct people into one image using a similar set of facial feature points such as iris, eyes, nose, face shape, etc. The resulting morphed image looks similar to both contributing images such that it is difficult to assert them apart with human eyes.

Although morphed images are not always visible to the naked eye, many automatic face morphing algorithms, such as landmark manipulation and Generative adversarial networks (GAN) generation, introduce artifacts in the final image that indicate an image was morphed. These morphing artifacts are mainly found at very high or low-frequency spectra. The spectral camera captures the spectral images based on an object's reflectance and emittance properties, a spectral imaging sensor extracts the characteristic spatio-spectral data across the spectral images in different Visible (VIS) and Near Infrared (NIR) spectrums. Moreover, the spectral imaging technique obtains complementary image information (i.e., reflectance or emittance) across discontinuous spectral bands such that the characteristic discriminative features can be obtained. Taking into consideration that spectral bands images allow to evaluate the spatio-spectral data at different frequency levels independently, this thesis is especially focused on detecting these morphing artifacts in spectral imaging. Thus, even though morphing artifacts are often undetectable in the image domain, different spectral bands ranging from Visible (VIS) and Near Infrared (NIR) have been explored for detecting image morphing. This thesis builds upon this and looks for the possibility of detecting morph attacks using the spectral images.

1.3 Research Questions

The thesis aims to formulate two critical research questions on morphed attack detection using spectral images:

- Can spectral imaging helps in detecting morphing attacks?
- What proficiency does a novice Human observer have in spotting morphed images from spectral images?

1.4 Contributions

In terms of contribution, this thesis is divided into four areas. We started by creating databases in which morphed images were generated utilizing three different morphing generation approaches. Second, we investigated the vulnerability of various commercial and deep learning-based FRSs in order to determine how well they can detect morphed images from spectral images. This is followed by a human observer analysis of the detection of morphed images from spectral images. Finally, we studied various MAD algorithms for detecting morphed images when spectral images are provided. The main contributions of this thesis are summarized below:

- Provides a new database that includes morphed images generated using three different techniques, including two landmark-based approaches: LMA, UBO, and one Deep Learning-based morphed generation technique (MIPGAN-I).
- Presents the vulnerability study to measure the attack success rate on two commercial FRSs, COTS (Neurotech and Cognitec) and deep learning-based FRSs (ArcFace, ArcFacePlus, CosFace, and CosFacePlus), using the newly generated dataset.
- Human observer analysis for detecting morphs images from spectral and regular (RGB 3-channels) images and its comparison with the automated FRSs.
- Extensive study on the Morphing attack detection utilizing the generated morphed images with spectral band images.

1.5 Paper Outline

The rest of the paper is organized as follows:

Chapter 2 provides an overview of face morphing and morphing attack, building the theoretical knowledge base required for this study. This is followed by chapter 3, which details the state-of-the-art works in Morphing attack detection, MAD databases, and human observer analysis on detecting morphed images including related researches with their contribution in the area. Chapter 4 presents the creation of the morphing database used in this thesis. It details the selection of the images and the post-processing and pre-processing techniques employed

during its creation. Furthermore, the potential attack of new database on various facial recognition systems is presented in chapter 5. The chapter 6, beneath it details an empirical study that has been conducted to identify the human observer's ability to detect when presented with spectral images. chapter 7, on the other hand, describes the different MAD techniques utilized to detect the morphing attack detection along with a discussion on results obtained from different techniques. Chapter 8 presents the discussion on different observations made in this research work. Finally, chapter 9 concludes this thesis by summarizing the contributions and findings as well as directions for further work.

Chapter 2

Morphing Attack and Morphing Attack Detection

2.1 Face Morphing and Face Morphing Attack

Face morphing and morphing attack are discussed in this chapter [1]. It also covers the background information necessary for understanding morphing attacks. Face morphing is a technique that uses a combination of feature points such as the eye, nose, mouth, and face shape to combine two facial photographs of different people into a single image. It is almost impossible or very challenging to distinguish between the created morphing images and the originals with human eyes. The Figure 2.1 depicts a morphed image subjects 1-vs-2 created using actual photographs of subjects-1 and subject-2. As we can see in the Figure 2.1, the morphed image appears to be similar to both authentic pictures. Similarly, a face morphing attack attempts to manipulate a biometric facial recognition system into identifying two different people with the same morphed face image. Because a morphed image appears to be real to both images, it can be used to authenticate image-based identification documents such as passports. Thus, a face morphing attack puts organizations that rely on face images to confirm a person's identity in jeopardy, such as the Automatic Border Control system.

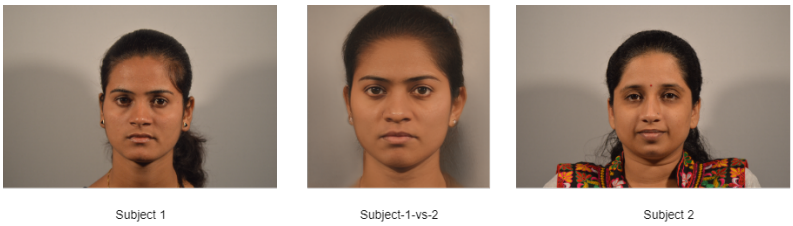


Figure 2.1: An example of a morphed image

[1]The content from this chapter has been used by the author for Advane Project Work course.

2.2 Face Morphing Generation Technique

There are two common techniques to creating face morphs: 1) Landmark-based approaches, and 2) Generative model-based approaches

2.2.1 Landmark Based Morphing Methods

The landmarks of facial photos are obtained for two images in landmark-based morph creation. The landmark points obtained from both images are wrapped by moving pixels to other, more averaged positions. The delaunay triangulation, or triangular mesh, is created from landmark points of both photographs and then blended to generate a single altered image.

There are three main processes in the landmark-based morphing pipeline: 1) correspondence, 2) warping and 3) mixing [3].

The initial stage (correspondence stage) is to define landmarks on the original facial images. As illustrated in the Figure 2.3, these landmarks correspond to key points on the facial characteristics that form and structure the face (such as eyes, nose, mouth, etc.). Landmarks can be defined manually [2], or they can be detected automatically. The dlib landmark detector [4] is one of the most commonly used models [5–7] for this.

Wrapping of the correspondence points defined earlier is the next step, in which delaunay triangulation [8] or triangle mesh [8] wraps landmark points. Wrapping involves adjusting the images so that the correspondence points (landmarks) between two images are aligned. Each image is aligned according to α factor (ranges from 0 to 1) that determines the amount of contribution each subject makes to the morph. For example, the α value of 0 represents that image B

Figure 2.2: Examples of landmarks based approach

will be wrapped around the landmarks of image A, α value of 1 means that image A will be twisted around the landmarks of image B, and a value of 0.5 indicates

that both images will contribute equally [9]. Naturally, α value of 0.5 makes the most sense for creating a morph that is comparable to both faces [5–7, 10]. The figure shows an example of morphed images with different alpha values: $\alpha = 0.3$, o.5 and 0.7 respectively.

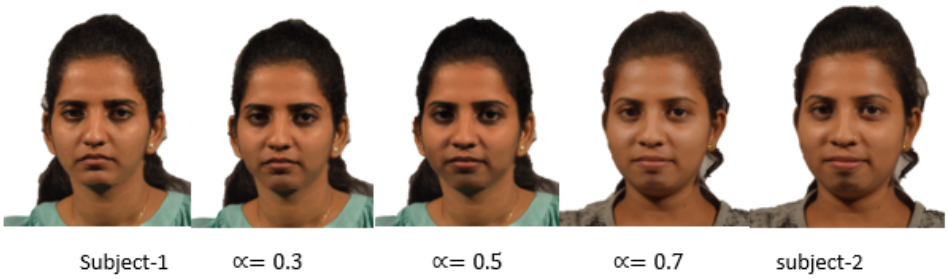


Figure 2.3: An example of morphed images with different α values

The final step is the Blending. In this stage, a morph image is formed as a weighted average of the two aligned (wrapped) images. At a weight of 0.5, this is the same as averaging the two images. Traditionally, the weight used for each image is the same as α value. However, a research [11] has shown promising results by isolating α into two different variables for wrapping and blending (α W, α B).

Since pixel positions were modified while generating the morphed images, some pixel misalignment may occur, making the image appear unrealistic. Thus, image pre-processing such as image smoothing, image sharpening, edge correction, histogram equalization, manual retouching, and image enhancement are essential for landmark-based approach. The Figure 4.5 illustrates morphed image generation technique using landmark based approach. OpenCV and other open-source programs such as FaceMorpher and WebMorph use a landmarks-based technique to generate morph face [12].

2.2.2 Deep Learning (GAN) Based Morphing Methods

In addition to the LMA, deep learning based approach has also become a common alternative for building morphing faces, as deep learning models have improved steadily over the years. By combining two facial images in the latent space, Damer et al. [10] proposed a Generative Adversarial Network (GAN), which eliminates the time-consuming, partially manual process of building morphed images and enables a completely automated morphed generation technique.

GANs are made up of two networks: a Generator and a Discriminator. They both engage in an adversarial game in which the generator attempts to deceive the discriminator by producing data that is comparable to the training set. The Discriminator seeks to avoid being duped by distinguishing between fake and real

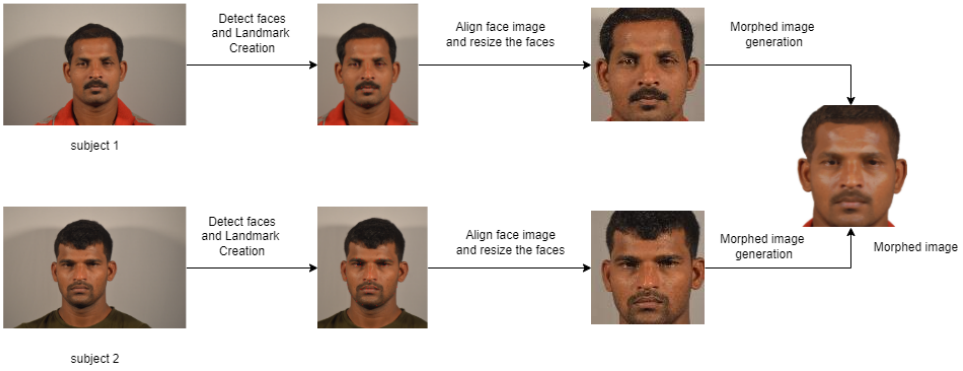


Figure 2.4: Illustration of morphed image generation process

data. They both learn and train complicated data such as audio, video, and image files at the same time. The generator model learns how to make realistic images by generating images from random noise. Random noise is sampled using a uniform or normal distribution before being fed into a generator which generates an image. The discriminator learns how to distinguish fake images from real photos by feeding the generator output, which includes fake images and actual images from the training set, as shown in Figure 2.5. The chance that the input is real is represented by the output Discriminator. Discriminator should be 1 if the input is real, and 0 if the input is generated.

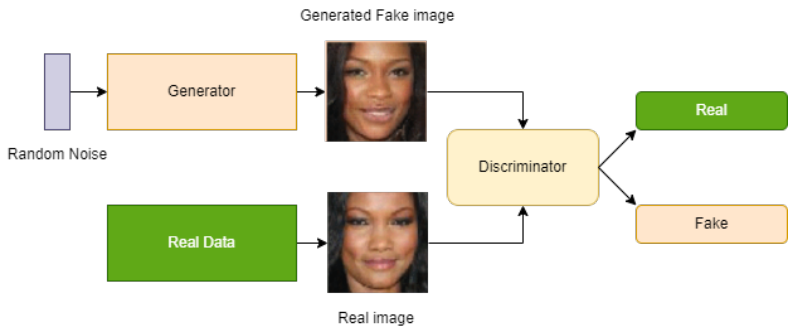


Figure 2.5: Illustration of GAN based approach

The proposed MorGAN model has trained the generator to create images at a resolution of 64×64 pixels. However, the evaluation of altered images generated using this technique against two commercial FRS fails to meet both necessary standards and the FRS verification level in vulnerability analysis [8]. The StyleGAN [13] architecture was designed to address this concern by increasing the spatial dimension to 1024×1024 and thereby improving the quality of the facial image. The StyleGAN was able to achieve better spatial resolution than the MorGAN by embedding the photographs in the intermediate latent space [9].

Furthermore, using an Identity Prior Driven Generative Adversarial Network,

a new technique called MIPGAN (Morphing through Identity Prior driven GAN) [14] has been developed. This model was derived from the StyleGAN, but with a novel loss function that uses perceptual quality and the identity factor to produce a high-quality morphed face image with few artifacts and high resolution. The proposed morph generation method poses a severe threat to FRS, as demonstrated by this model. Moreover, Damer et al. [15] produced ReGenMorph, which employs a GAN-based generation to reduce landmark-based morph (LMA) blending artifacts and manipulation in the latent space, resulting in noticeably realistic morphed images as compared to the earlier works.

In this work, both landmark-based technique and deep learning based techniques have been utilized for generating morphed images. Two approaches: (UBO), developed by University of Bologna [2] and LMA, developed by Norwegian Biometric Lab, NTNU [16] will be employed for the landmark-based approach, while the MIPGAN-I [14] would be used for the deep learning-based method.

2.3 Face Morph Attack Detection Techniques

The two types of MAD approaches are offered: single image-based MAD (S-MAD) and differential image-based MAD (D-MAD).

In the S-MAD based morphing attack, a single image is provided to the algorithm, and the algorithm detects the potential attack based on that single image, as shown in the Figure 2.7. The implementation of S-MAD is complex since it should address a wide range of use case scenarios, including image quality variations, resilience for photographs captured by various types of cameras, different print-scan procedures, etc.

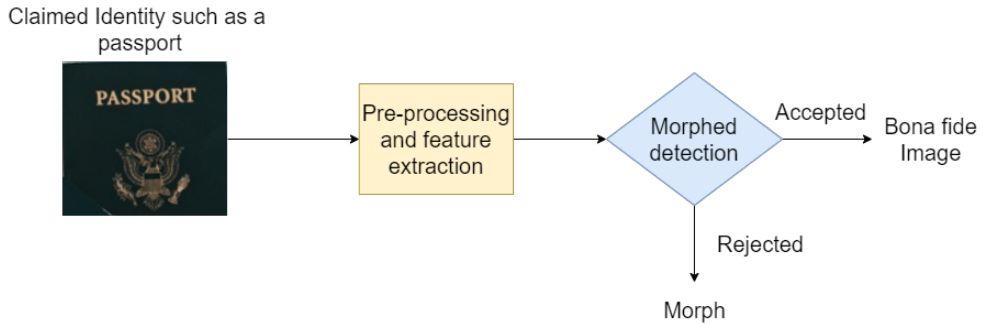


Figure 2.6: Illustration of S-MAD approach

On the other hand, the D-MAD algorithm uses the live image or reference image to determine whether the suspected image has been altered or is authentic. The D-MAD approach is demonstrated in the figure with a border crossing scenario where the suspected morph picture may be derived from the passport and compared to the live captured facial image.

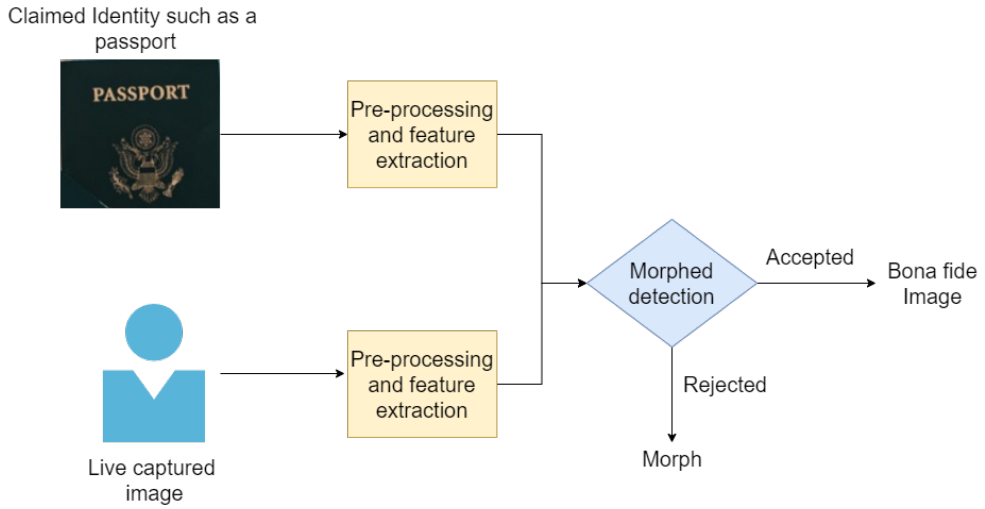


Figure 2.7: Illustration of D-MAD approach

2.4 Vulnerability Analysis

The vulnerability analysis evaluates whether all contributory data subjects could be validated against the altered facial photos. The FRS must successfully verify all contributory subjects that fulfill the verification threshold when a morphing face image is placed in it and tested with another image from a contributing subject [9].

The vulnerability plots, which depict the scattered data of FRS comparison scores, are shown in the figure. The plot is divided into four quadrants. The first quadrant (QI) score indicates that the morphed image is not validated to belong to the two contributing data subjects, thus score in this quadrant does pose a threat to FRS. Similarly, it can only verify the morphing image as one of the contributing subjects, data subject-2 and subject-1, in the second (QII) and fourth (QIV) quadrants, respectively. Hence, a large number of comparison scores in the second and fourth quadrant imply that the morphing images do not constitute a severe threat to FRS. On the other hand, the third quadrant (QIII) specifies that the morphing image is validated as both contributing data subjects as subject-1 and subject-2. Hence, the more comparison scores in this quadrant, the greater the threat posed by the studied FRS to morphed photos [9].

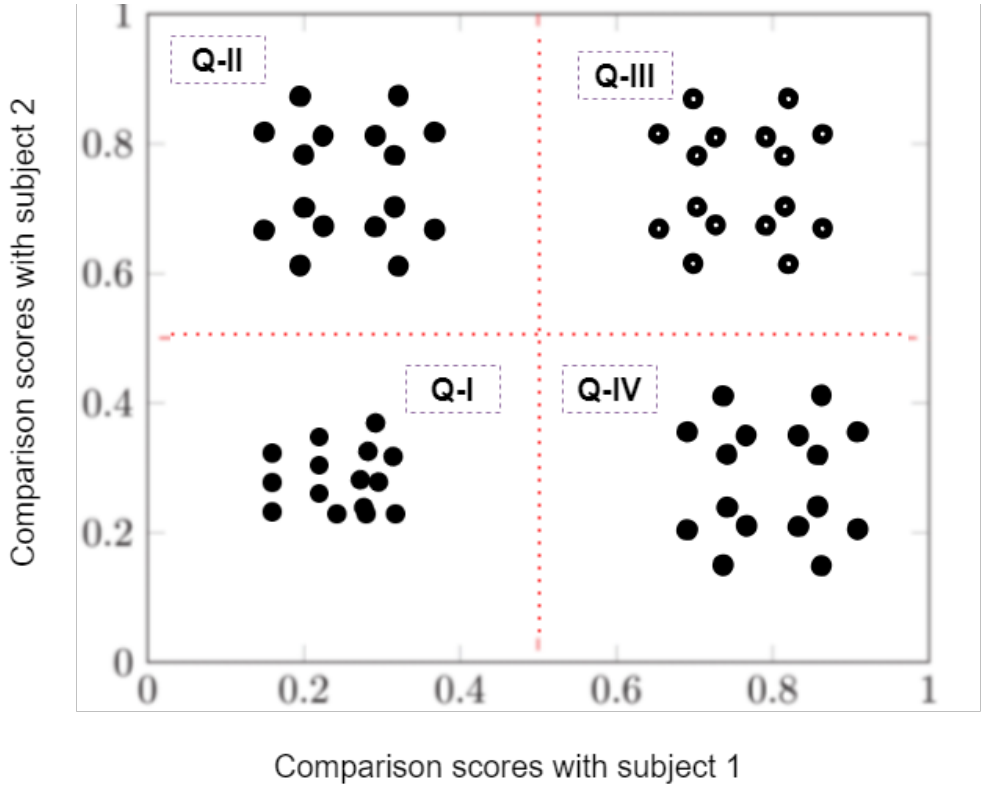


Figure 2.8: Vulnerability analysis plot

Chapter 3

State of the art in Morphing Attack Detection

Ferrara et al. [2] first proposed the possibility of generating a morphed face image attack utilizing two genuine images. They used two face recognition solutions to compare altered images with the original subject images, and came to the conclusion that face recognition is highly vulnerable to such attacks. Since then, many morph detection techniques for both single (no reference) and differential morph attack detection scenarios have been presented. The state-of-the-art in morphing attack detection is detailed in this chapter [1]. This chapter also covers some of the databases built to study the detection of morphing attacks, as well as experiments undertaken to investigate the human observer's ability to detect morphed images. As described in the section 2.3, single (no reference) morph attack detection systems rely solely on the potential morphed image to classify a potential morphed image. Differential morph attack detection methods, on the other hand, compare the potential morphed image to a second trusted image. As such, differential morph attack detection algorithms have more information at their disposal for categorization and, thus, perform better than single morph attack detection algorithms.

3.1 Single Image MAD

Single image MAD solutions can be classified into two types: those that use handcrafted features and those that use deep learning features. Binarized Statistical Image Features (BSIF) [17, 18], Local Binary Patterns (LBP) [10], Local Phase Quantization (LPQ) [16], and features established in image forensic analysis such as photo response non-uniformity (PRNU) [19] were among the handcrafted features. Since the advancement of deep learning in the last decades, some approaches have used convolutional neural networks (CNNs) to detect the morphing process [10, 20–22]. Pre-trained networks with or without fine-tuning, such as versions of

[1] Some contents from this chapter has been used by the author for Advane Project Work course

VGG [23], AlexNet [24], or networks trained for face recognition purposes, such as OpenFace [25], were often utilized in MAD solutions based on deep learning. The biggest drawback of these kinds of corpora is the number of samples required to train models. For this reason, some research works employed pretrained networks (networks with pre-calculated weights) such as FaceNet [26] or VGG-Face [27].

3.2 Differential Image-Based MAD (D-MAD)

Other studies looked into the possibilities of differential morph attack detection where morphing attacks are detected by running a live probing image alongside the reference image. The objective of D-MAD approaches is to decide whether a suspect image is morphed or bonafide when a corresponding image captured in a trusted environment is available. D-MAD approaches are further divided into two categories: 1) feature-based D-MAD and 2) demorphing.

3.2.1 Feature Difference-Based D-MAD

This method works by subtracting features computed on the suspicious morph image and a live probe image. The features are further categorized by calculating the difference in the feature vectors to detect a morphing attack. Classical feature extraction methods have been applied to the differential application by determining the difference of the feature vectors of the images being compared. This difference vector, together with the original feature vector of the potential morph, is then used to train a difference SVM and a feature SVM, respectively. Several feature extraction techniques, including texture information, 3-D information, gradient information, landmark points, and deep feature information, are explored.

Texture information includes the LBP and BSIF. The Local Binary Pattern (LBP) [28] is an image texture descriptor that thresholds surrounding pixels based on the current pixel's value. After comparing the gray level with nearby pixels, LBP assigns a binary number to each pixel in an image. A value of unity is assigned to neighbors in a preset patch with a gray level greater than the central pixel; otherwise, a zero value. After that, the central pixel is allocated a binary number. The original LBP operator evaluates a 3×3 patch, forming an 8-digit binary number from the surrounding pixels. LBP feature map and a histogram with 256 bins are obtained once all pixels in an image have been tagged. The LBP histogram is then used as a classification feature vector, with each bin representing one feature. On the other hand, binarized statistical image features (BSIFs) [29] utilizes specific filters learned from a set of images. By linearly projecting local picture patches into a subspace, the approach generates a binary code for each pixel. Local image basis vectors are learned from natural images using independent component analysis and thresholding to binarize the coordinates in this basis. The length of the binary code string is determined by the number of basis vectors. The features such

as Local Binary Patterns (LBP), Binarized Statistical Image Features (BSIF) are extracted and Obtained feature values are stored in a corresponding histograms.

Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF), in contract, extract sets of local keypoints. Because morphing images are expected to have fewer keypoint locations, which are defined as maxima and minima of the difference of Gaussian functions, than real images, keypoint extractors are used. The Histogram of Gradients (HOG) and sharpness features were also employed to compare the gradient of features between morphed and genuine images, since the morphing procedure reduces high frequency changes and so has a lower value of steepness of gradients. Scherhag et al. [30] has successfully performed the detection of morphed image in comparison with the live probe image captured in the ABC gate. Scherhag et al. [31] also investigated (LBP) features, BSIF, SIFT, SURF, and HOG descriptors with SVM.

Scherhag et al. [32] explored more in the differences between directed distances of landmarks with SVM in detecting the morphed images. The 68 facial landmarks determined utilizing the facial landmark predictor of dlib which returns the absolute position of 68 facial landmarks. Euclidean distance of the relative position of each landmark points between both images probe and bonafide is compared for detecting the morphed images. In addition, the angles of each landmark, to a predefined neighbor (in order to obtain the most discriminative dependencies) are computed for detecting the morphed images.

On the other hand, deep learning is fundamentally another approach defined by the development of algorithms that search for features to extract to solve a particular goal. These features are extracted using a deep Convolutional Neural Network (CNNs) due to its previous success in other computer vision tasks. To detect a morph attack, Scherhag et al. [33] use deep facial representations extracted from ArcFace feature embeddings. It is demonstrated that deep face representation methods may achieve very high detection performance (less than 3% D-EER) and robustness to various post-processing. The authors also highlighted the need of large variance, and their network was trained on a morph database created using a variety of morph generation approaches.

Furthermore, a Siamese disentangling network has also been proposed in [34], which separates the landmarks and the appearance of the two images being compared. Similarly, a Siamese network has also been explored by Soleymani et al. [35] in the image domain. A double Siamese network architecture has also been presented by Borghi et al. [36], which uses two Siamese networks and integrates their output to make a conclusion.

3.2.2 Demorphing

Face demorphing or reverting a face morph has yielded some promising results. Face demorphing techniques reverse the morphing process, revealing the component images utilized to create the morphed image. Ferrara et al. [37] made the initial approach in this field, which was designed to operate with landmark-based

morph generation. It utilized the idea of face demorphing by image subtraction to reveal the identity of the legitimate document owner, given a bonafide capture.

Recent work in face demorphing utilizing robust Deep CNNs has also achieved quality results [38, 39], when the image quality is good. However, one of the disadvantages of this approach is that the detection performance declines, when a face image is acquired in real-life conditions with pose and lighting variations that are relatively prevalent in real situations.

The Table 3.1 [2] summarizes the published differential methods and the approaches utilized to detect the morphing attack in D-MAD setting.

3.3 Databases for Morphing Attack Detection

The first face morph database was released by Ferrara et al. [2], who used landmark-based face morph generation. This small collection of the database was developed with 14 morphing photographs of both male and female participants from eight real images. This dataset was later expanded [45] to 80 morphing face pictures with 10 male and 9 female subjects.

Raghavendra et al. [16], on the other hand, created the first large database, including people of various ethnicities (Caucasian, Asian, European, American, Latin American, and Middle Eastern). It makes use of face landmarks as well as the GIMP/GAP morph generation approach using the GNU image manipulation tool. This dataset consisted of 450 altered facial pictures from 110 different individuals of various ethnicities.

To create high-quality morph images, Makrushin et al. [46] used automatic morph creation techniques. It uses a triangulation method based on 68 facial landmarks extracted using the dlib library [4]. Complete morph (consisting of the facial geometry of both facial photos) and splicing morph (the pixels representing the face are cropped out of the input faces) were utilized as morph creation approaches [9]. There are roughly 1326 complete morphs and 2614 splicing morphs in this database, which were generated from 52 data subjects, 17 females and 35 males. This database isn't available to the general public.

Scherhag et al. [18] presented the first print-scan face morph database. For morph generation, the authors used the landmark-based approach. There are 231 morphed images in this database, which were created from 462 real images. This is also a private database.

Thereafter, many databases, spanning from public [47] to sequestered datasets [17, 23, 48–50] with varied attack strengths, have been constructed using different attack generation mechanisms. The complete list of databases created so far using different techniques could be found here [9]. However, since the majority of these databases were private and were not widely accessible, the author developed new database for the implementation purpose.

[2] This table is inspired from a survey paper by S Venkatesh et al. [9]

Table 3.1: Overview of relevant differential MAD algorithms

Reference	D-MAD category	Approach
U Scherhag et al. [31]	Feature Comparison	Differences in the BSIF features
U Scherhag et al. [32]	Feature comparison	Differences in the angles of landmark pairs in SVM
N Damer et al. [40]	Feature comparison	Directed Distances with SVM
M Ferrara et al. [37]	Demorphing	Face demorphing by image substraction
M Ferrara et al. [41]	Demorphing	Face Verification
N Damer et al. [25]	Multi detector fusion	Transferable deep CNN
J M Sigh [35]	feature comparison	Euclidean distance, feature difference and a SVM classifier, and feature concatenation and a SVM classifier
N Damer et al. [40]	Landmark shift	facial landmarks shifting patterns between reference and probe images in a directed distances
F Peng et al. [42]	Face restoration by demorphing GAN	Symmetric dual-newtwork architecture
U Scherhag et al. [33]	Deep face representation	ArcFace, FaceNet algorithm
C Seibold et al. [43]	Deep Learning	Layer-wise Relevance Propagation (LRP)
D Ortego et al. [39]	Demorphing	Autoencoder (encoding and decoding process)
S Soleymani et al. [35]	Feature comparison	Euclidean distance, feature difference and feature concatenation using Siamese Network
S Soleymani et al. [34]	Feature Comparison	Landmark and appearance disentanglement
S Autherith et al. [44]	Geometric facial features comparison	Feature transformations of landmark locations

3.4 Human Perception and Morphed Face Detection

Matching unfamiliar faces is a challenging task even for an expert such as passport-issuing officers [51], who are required to have extensive training in face identification. Numerous studies [52–54] conducted over the last decade have also revealed that humans are prone to making mistakes when comparing unknown faces. White et al. [51] did a similar study with professionals who had received facial identification training (such as passport officers and ID card checkers) and

individuals who had not received any face identification training (such as student volunteers). The purpose of this study was to compare the performance of experts and non-experts in face verification tasks. While the average performance of passport officers was bad, certain officers did exceptionally well – and this was not connected to length of service or training.

Another study by Robertson et al. [53] looked at morph attack detection using human observers and found that while the accuracy of smartphone face recognition systems isn't perfect, the acceptance rate is much below the level at which two faces are indistinguishable. Although non-expert viewers were willing to accept morphing photos made with 50% of each contributing subject as true ID at alarmingly high rates, it is reasonably possible to lower this error rate significantly by following some basic guidelines. However, the rates are fairly low, and they are far from perfect—always substantially higher than acceptance of a false photo of another person thus on some occasions, be benefit to fraudsters in using this approach. This experiment was repeated by Kramer et al. [55] with a a high-quality morph database and the results show that people were highly error-prone when detecting morphs, and that training had very little effect. In a live matching task, morphs were accepted at levels that suggest they are a substantial security threat, and detection was error-prone once again. The same experiment was carried out with MAD algorithms, with the findings indicating that algorithm performance was higher than that of human observers.

Furthermore, Ferrara et al. [56] conducted an experiments with human observers in which they were provided two face images in each trial, bonafide or morphed face morph attack detection, and found that morphed images were also accepted as a bonafide image. Similarly, Phillips [57] investigated the performance of human observers in a differential morphing attack detection situation, in which static images and video imagery were used. The results showed that automated FRS systems function better with static facial images, however, human observers ability to detect morphed face is better in video contents. This experiment also highlighted that FRS systems had a greater morph detection rate than human observers. Similarly, separate experiment carried out by Marushin et al. [58] and Nightingale et al. [59] also concluded that automated face recognition comparatively has better accuracy in detecting morphed images. Moreover, Zhang et al. [14] investigated the same concept using a variety of morphing algorithms, including landmark-based morphs and GAN based morphs. The experiment was conducted with both expert and novice observers, and the results suggested that experienced observers outperform inexperienced observers, and also highlighted that landmark-based morphs is more challenging than detecting GAN based morphs.

Godage et al. [54] did a study that included both S-MAD and D-MAD settings. The first step in this research was to construct a new benchmark database of realistic morphing attacks from 48 different individuals, which results in 400 morphed images presented to 469 D-MAD observers and 410 S-MAD observers. Both experienced and inexperienced observers were included. The research concluded that even highly experienced professionals are likely to miss a lot of morphing attacks.

Furthermore, when compared to automated MAD systems, the study remarked that human observers have a lesser accuracy in detecting morphed images.

In recent decades, experiments in human observation to detect morphed images have been conducted frequently; nevertheless, all of the observations were limited to conventional colored images (RGB images). As no similar experiments using spectral images have been found, this work simulates human perception on morphing images by utilizing spectral images.

Chapter 4

Spectral Morph Attack Database

Almost all databases in the face morphing detection field are privately held, as noted in the subsection 3.3. Further, there are no databases with spectral images when considering morphing attack research. Consequently, developing a database for this research was an essential step and this chapter details the newly collected dataset during the thesis work.

4.1 Selection of Image Candidates

The initial step in creating the database was to analyze high-quality, high-resolution photographs from a sequence of images linked to a subject. Such images were provided by NTNU for the research purpose [60]. The database contains the spectral images for each bonafide image taken with the spectral camera. Spectral images are made up of images in eight narrow spectral bands throughout the Visible (VIS) and Near Infrared (NIR) spectrum: 530nm, 590nm, 650nm, 710nm, 770nm, 890nm, 950nm, and 1000nm. The photographs were organized into subject folders, with one subject per person. There are altogether 145 different subjects, with 86 male subjects and 67 female subjects. The images in each subject have plain background, with an evenly illuminated face, and upper body subsections, thus the subgroup of 145 unique individuals' face shots provided the best quality photographs for creating morph images. The number of subjects in each category in the database is represented in the Table 4.1.

Furthermore, each subject in each band has approximately 5-10 images, and we chose one regular (RGB, 3-channels) image from a series of 10-15 images to generate the morphing image, while the remaining images were used to analyze the vulnerability analysis and evaluation of the face recognition system (FRS).

4.1.1 Image Enhancement

As stated above, the database contains spectrum images ranging from visible to infrared. Without image enhancement, images from some spectral bands were not

Table 4.1: Number of subjects in the database

Category	Total
Total subjects	145
Male subjects	88
Female subjects	67

visible. Thus, image enhancement is utilized such that the face recognition system can detect images from all spectral bands. We enhanced the image contrast, brightness, and image sharpness. Various enhancement factors ranging from 1.5 to 16 have been utilized, where factors greater than 1.0 make the image stronger and factors fewer than 1.0 make it weaker. For example, brightness factors greater than 1.0 brighten the image, while factors less than 1.0 darken it, and a factor of 0.0 produces a completely black image. The factors for each category utilized for each spectral band are listed in the table 4.2.

Table 4.2: Image enhancement in each band

Band	Contrast	Brightness	Sharpness
530	3	16	3
590	3	10	7
650	1.5	2.5	2
710	2	3	2.5
770	2	2	2
830	2	2.5	2
890	2	3	2
950	2	5	2
1000	5	6	3

The comparison of images in each spectral band before and after image enhancement is shown in the figure 4.1.

4.1.2 Face alignment and cropping face region

Face alignment is important because it can be an entry point in the face recognition process, and poor alignments can greatly affect recognition performance. We adjusted the alignment of the faces from each spectral band using appropriate scaling, rotation, and padding/cropping with respect to the eyes placement to ensure that the passport standards were met. Face landmarks are recognized using the Dlib algorithm [4], and alignment is accomplished using the detected eye coordinates, with a fixed intra-eye distance of 180 pixels. The facial alignment is done for all images from the database including spectral images, and regular RGB images. A sample of aligned images is shown in the Figure 4.2.

Furthermore, to focus on the image's region of interest, some non-essential

Figure 4.1: Comparison of images in each spectral band after image enhancement

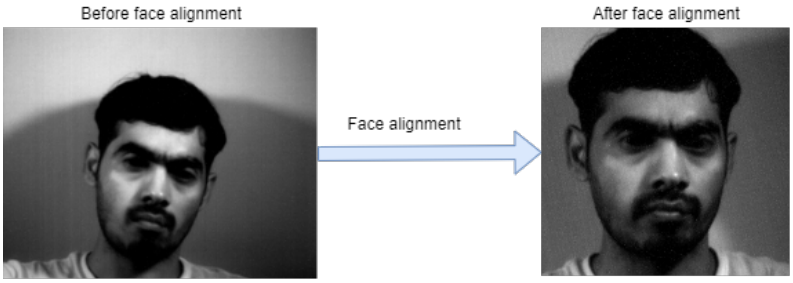


Figure 4.2: A sample of an aligned image

components can be deleted. This process is called cropping, which refers to removing the image's exterior elements to improve the frame, emphasize the subject matter, or adjust the aspect ratio. Cropping is necessary to remove the image background because the background effect affects the feature space discrimination power. The face is cropped from the whole image depending on the position of the left and right eyes as well as the mouth [61]. Finally, all of the new photos must have the same dimensions. Therefore, the new photos are normalized to a standard size of 112 x 112 pixels after cropping the face from the original image. A sample of cropped image is shown in the Figure 4.3

After image enhancement and cropping of the aligned face region, the data-

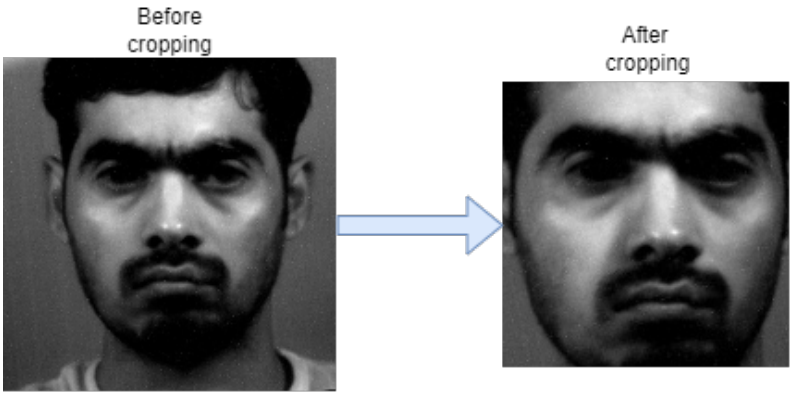


Figure 4.3: A sample of an cropped face image

base contains 16927 genuine images, including all spectral band images and standard RGB images. The Table 4.3 represents the number of images in the database in each spectrum after face alignment and cropping.

Table 4.3: Number of images in each spectrum

Band	Spectral bands									
	530	590	650	710	770	830	890	950	1000	RGB
Total	965	1536	1653	1713	1719	1704	1732	1647	1605	2626

4.2 Morphed image generation

In order to develop morphed images, one image from each subject from the database that exhibit uniform illumination, good focus, a neutral face expression with wide eyes and no visible teeth, neutral backdrop, and no reflections in glasses was chosen.

We separated the bonafide reference images from the morph input images as much as possible, avoiding the usage of the same image or image sections again throughout MAD training, which increases the variance of training data. The morph input images are lexicographically sorted for the creation of morphs, and then each input image is morphed with one of the next subsequent input images that meet the following criteria: both represented subjects are of the same gender; they look similar to each other; they are of the same age range; and they have the same color complexion. The input images for morphs are only utilized once, for the creation of a single morph. Since we aim to avoid a repeated use of the same image or same image parts in the training stage of MAD algorithms to prevent from over-fitting caused by over-represented image parts [33].

Furthermore, three different morph images generation tools are utilized to create the morphed images, which are listed below:

1. LMA [16]: Morphing Attack Generation Software provided by the Biometric Lab NTNU, Norway
   Generation of morphed images with Landmark based attacks (LMA) is performed by detecting 68 landmarks on the face using Dlib [4] model. The mean face points for each image are computed and each image is subsequently warped to sit on these coordinates after performing the Delaunay Triangulation on 68 facial points. Only the facial area is morphed, and transformed and merged into one of the original morphed images.

2. UBO: Automatic Morphed Face Generation Tools Version 1.1 [2, 41, 56], provided by the Biometric System Laboratory from University of Bologna, Italy

   In this technique, free GNU Image Manipulation Program v2.8 (GIMP) [62] and the GIMP Animation Package v2.6 (GAP) [63] were used to morph two facial images. Two faces are supplied as separate layers in the same image and aligned according to the position of the eyes. The GAP morph tool designates a series of essential facial points (e.g., eye corners, eyebrows, nose tip, chin, and forehead) on the two faces, as these points allow for better alignment and smoother morphing. After finding the feature points, the GAP morph function automatically generates a sequence of frames depicting the transition from one face to the other by interpolating these points. These frames are gradually shaded from subject 1 (applicant) to subject 2 (criminal). Finally, the frame selection is made by scanning the frames (beginning with the applicant photos) and continuing until the current frame has a matching score with the criminal subject greater than or equal to the matching criteria. Eventually, the selected frame is manually edited to improve its authenticity by removing ghost shadows and other minor flaws generated during the morphing process.

3. MIPGAN-I [14]
   The MIPGAN-I framework is designed based on the StyleGAN model [13]. In the first stage, corresponding latent vectors are predicted using facial photos from the accomplice (subject 1) and malicious (subject 2) data subjects. The predicted latent vectors thus provide the initialization for the morphed face generation obtained using a weighted linear average of two faces. The resultant weighted linear average vector is fed into the synthesis network, which produces a morphing image with a resolution of 1024×1024 pixels. The generated morphed face image is optimized using the perceptual loss function to generate the high-quality morphed face image.

The Figure 4.4 shows a sample of morphed images generated using all three approaches. Both landmark-based (as explained in the subsection 2.2.1) and deep learning-based approaches (as detailed in the subsection 2.2.2) were utilized to construct the morphed photos. As explained above, first two techniques are based

Figure 4.4: An example of morphed images generated using all three methods

on landmarks, while the third is based on deep learning based approach. A total of 484 morphed photos are generated using the tools mentioned above, including 322 morphed images using the landmark based approach and 162 using the deep learning based approach. The number of morphed images generated in each category is shown in Table 4.4.

Table 4.4: Number of morphed images

Category	UBO	LMA	MIPGAN-I
Female morphed images	71	77	74
Male morphed images	81	87	88
Total morphed images	152	164	162

4.2.1 Post-processing of morphed images

Since pixel positions were changed when generating the morphed images in the landmark-based approach, some pixel misalignment occurred, thus making the image appear unrealistic. Thus, image post-processing techniques such as image smoothing, image sharpening, edge correction, and hand retouching were performed on these images. Adobe Photoshop was used to post-process the landmark-based morphed images such that the morphing images look as natural as possible. Double background, unnatural artifacts, double iris, and so on are corrected in the post-processing task. Figure 4.5 depicts the face photo after and before the post-processing.

Figure 4.5: An example of morphed image post-processing

Chapter 5

Attack Potential of New Database and Vulnerability Analysis

5.1 Validation of Attack Potential

As mentioned in the chapter 4, the new database has been created which consists of morphed images generated from both landmark based and deep learning based techniques. The vulnerability study will help in determining the impact of the generated morphed images on the commercial face recognition system. Thus, this chapter presents the vulnerability analysis of morphed face generation techniques employed in this study to quantify the impact of attacks on different FRSs. It details the attack success by verifying the morphed images against six distinct face recognition systems, including two Commercial Off-The-Shelf (COTS) and four open-source deep-learning-based FRS. The COTS FRS includes the Cognitec (Version 9.6.0) [64] and Neurotechnology (Version 11.1) [65] and the set of open-source FRS includes ArcFace [66], ArcFacePlus [67], CosFace [68], and CosFacePlus [67].

The attack potential is demonstrated by computing the comparison score distributions of an imposter, genuine, and morphed and compared against original probe identities contained in the database. We presented the comparison scores between the morphing attacks and their two original identity images in the probe set to test the attacks' ability to match both original identities. As mentioned in the section 4.1, for the vulnerability analysis, one image from each subject was extracted from the database; these images were used as reference images. For the probe images, spectral images from the database were used to compute genuine and impostor scores, along with reference images. Since the database comprises 145 people, each with 10-15 sample images, the total number of comparisons would be huge for imposter, around 144 X 144 X (10-15). Therefore, only random 25 subjects and three images from each sample subject were considered to simplify the number of impostor scores. In addition, for morphed scores, images from both the reference (which includes the morphed images generated using three different techniques) and probe sets which includes the images from different spectral

bands are compared. The morphing attacks score distribution is based on comparing the 484 morphed images, each with their corresponding two identities in the probe set. Table 5.1 summarizes the number of bonafide and imposter comparisons (all potential cross-comparisons of reference and probe images of distinct subjects) used for this study.

Table 5.1: Number of comparisons per test set

Band	Bonafide	Morphed			Imposter
		UBO	LMA	MIPGAN-I	
530	874	1906	2046	2021	8861
590	1464	3157	3388	3349	10584
650	1650	3504	3762	3715	10466
710	1710	3620	3885	3837	10501
770	1715	3619	3883	3835	10694
830	1700	3591	3855	3807	10634
890	1727	3645	3910	3863	10874
950	1645	3487	3736	3699	10520
1000	1579	3435	3681	3633	10547

For the deep learning based face recognition systems, the embeddings from the pre-trained models are employed as face authentication features, and the cosine similarity [42] between the features from two face images is used as the face authentication similarity score S_{sim_f}, which is defined as follows:

$$S_{sim\_f} = 0.5 + 0.5\frac{f_1 f_2'}{\sqrt{\left(f_1 f_1'\right)\left(f_2 f_2'\right)}} \tag{5.1}$$

where f_1 and f_2 are two feature vectors of two face images. The threshold of the deep learning models is tuned by LFW [69] database. For bonafide face images, a threshold of FMR $= 0.1\%$ was utilized following the guideline of Frontex [70]. The graphs of distance (dissimilarity) score distributions for the selected morphed, genuine, and impostor pairs are shown in Appendix A. The graph shows that imposter and genuine scores overlap for all deep-learning-based face recognition systems in all spectral bands. Since we used the pre-trained deep learning networks, which were trained on the regular RGB images. Therefore, we fine-tuned the models using spectral images and computed the scores (the graphs in the figures are after fine-tuning). Although the models have been fine-tuned, the impostor and genuine scores were still overlapping. This overlap in genuine and imposter score indicates that the newly created database could not be used to identify a potential attack on these deep-learning based face recognition systems.

The distribution plots for COTS FRSs (Cognitec and Neurotechnology) for all three types of morphed images are shown in Figure 5.1, Figure 5.2, Figure 5.3, Figure 5.4, Figure 5.5, Figure 5.6. The graphs show that both COTS FRSs are vulnerable to the morphed attack using all three types of morphed generation techniques: UBO, LMA, and MIPGAN-I. The attack potential of these COTS FRSs are seen on all nine spectral bands.

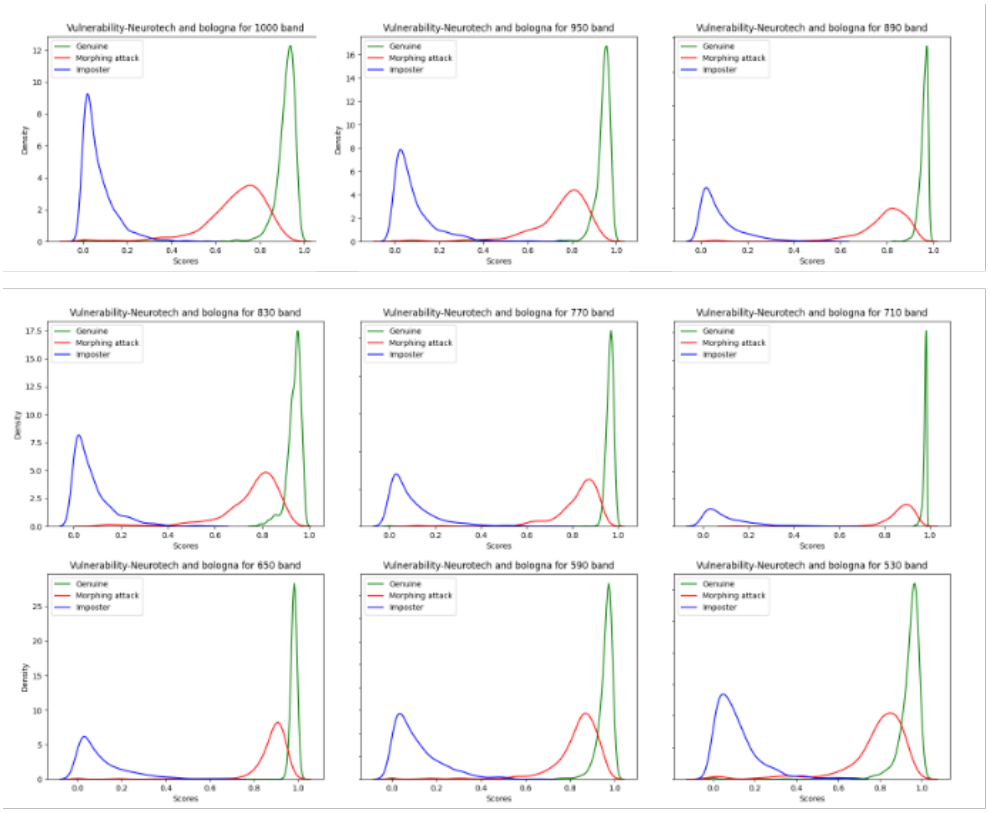


Figure 5.1: A vulnerability study of Cognitec with UBO morphed images in all spectral bands

5.2 Evaluation Metrics

The vulnerability for a particular morph image $MI_{1,2}$ acquired using two subjects by enrolling $MI_{1,2}$ and confirming it against probe images from the contributing subjects I_1 and I_2 were computed. If acquired comparison scores S_1 and S_2 for both probe images I_1 and I_2 against the morphing image $MI_{1,2}$ cross the verification threshold, then this morphed image is considered as a threat to FRS. The vulnerability is examined using different evaluation metrics: Mated Morphed Presentation Match Rate (MMPMR) [71], Fully Mated Presentation Match Rate (FMMPMR) [8] and Relative Morph Match Rate (RMMR) [71] using the validation threshold

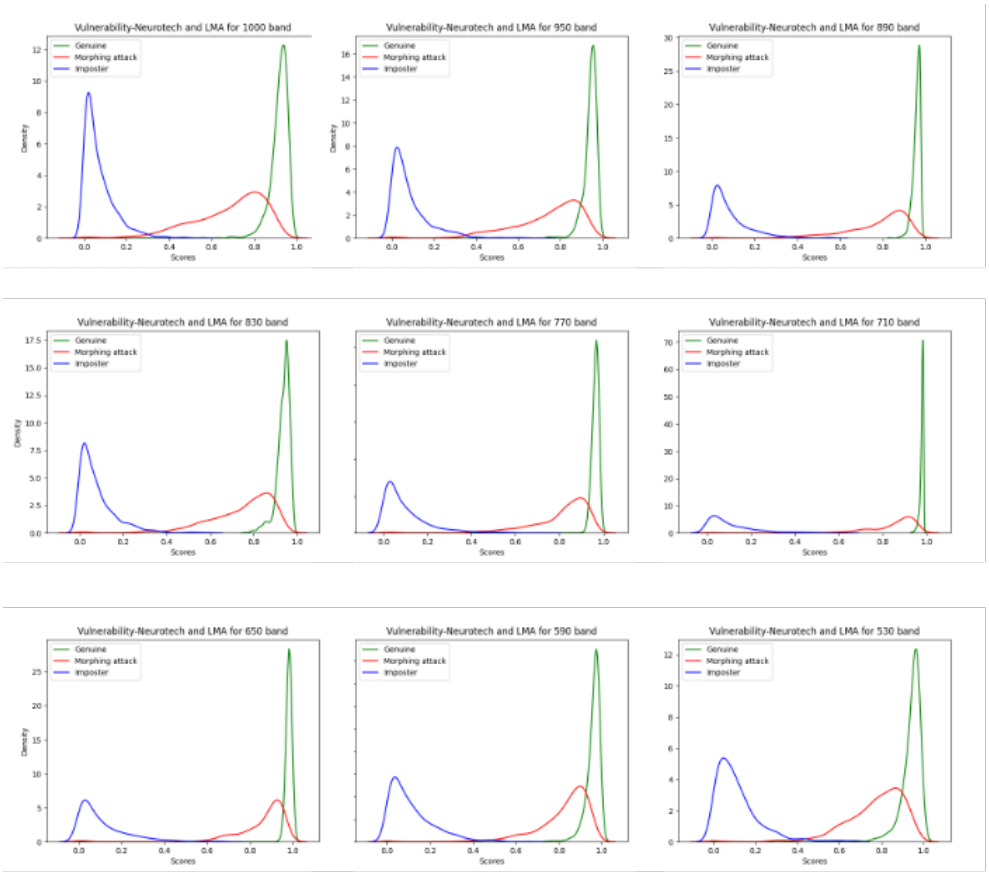


Figure 5.2: A vulnerability study of Cognitec with LMA morphed images in all spectral bands

for each FRS. The threshold utilized for Cognitec is 0.5 and 36 for Neurotechnology. If the score falls below the threshold, the morphed image is not considered a real threat as the comparison scores can't effectively verify the morphed image against both contributing subjects, rendering the morphing attack ineffective [8].

5.2.1 MMPMR: Mated Morphed Presentation Match Rate

Mated morph comparison compares a morphing sample to another independent sample from the same contributing individual. Thus, only one mated morph comparison per subject is possible. Only the minimum (for similarity scores) or maximum (for dissimilarity scores) of all mated morph comparisons of one morphed sample is of interest, since the morphing attack works if all contributing subjects are correctly validated. The MMPMR for similarity scores is defined as:

$$MMPMR(\tau) = \frac{1}{M} \cdot \sum_{m=1}^{M} \left\{ \left[\min_{n=1,\ldots,N_m} S_m^n \right] > \tau \right\} \tag{5.2}$$

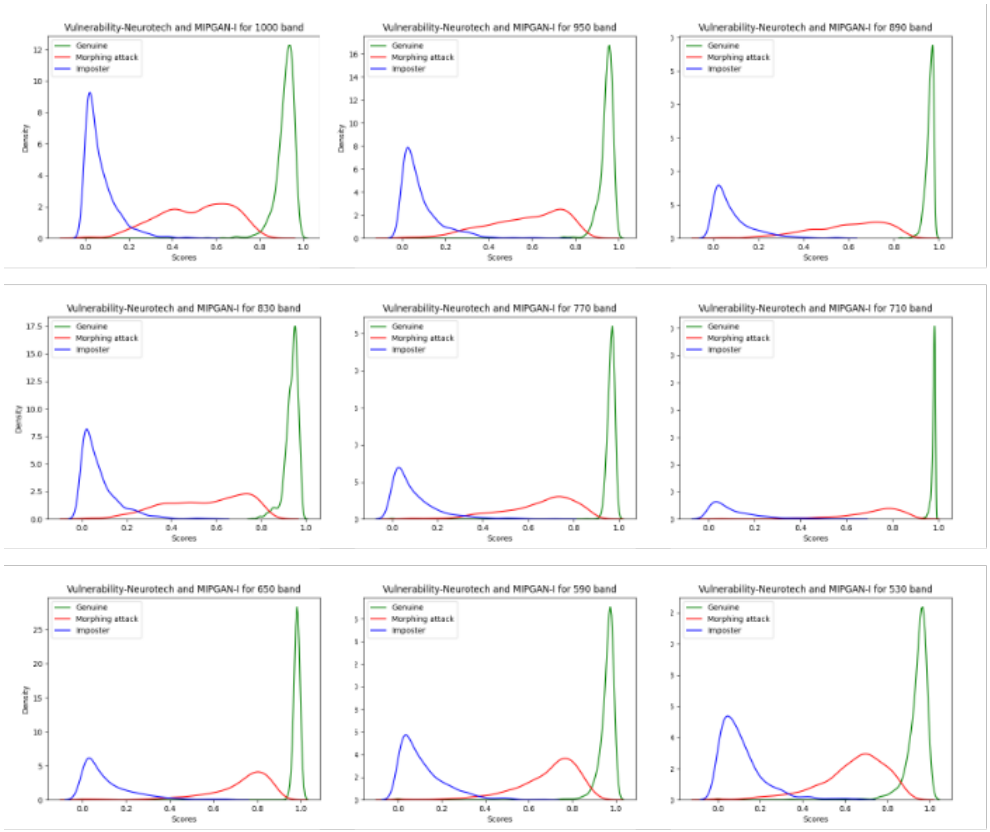


Figure 5.3: A vulnerability study of Cognitec with MIPGAN-I morphed images in all spectral bands

where τis the verification threshold, S_n^m is the mated morph comparison score of the n-th subject of morph m, and M is the total number of morphed images, and N_m is the total number of contributing subjects contributing to morph m.

5.2.2 FMMPMR: Fully Mated Morphed Presentation Match Rate

When comparing the FMMPMR to the MMPMR, the FMMPMR will take into account both pair-wise comparisons of contributory subjects and the number of attempts. The corresponding metric FMMPMR [8], is calculated as follows:

$$FMMPMR = \frac{1}{P}\sum_{M,P}\left(S1_M^P > \tau\right) AND \left(S2_M^P > \tau\right) \ldots AND \left(Sk_M^P > \tau\right) \tag{5.3}$$

where P=1,2,...,p represents the number of attempts made by presenting all probe images of the contributing subjects against the Mth morphed image, K = 1,2,...k represents the number of composite images used to generate the morphed image, Sk_M^P represents the comparison score of the Kth contributing subject obtained with the Pth attempt corresponding to the Mth morphed image.

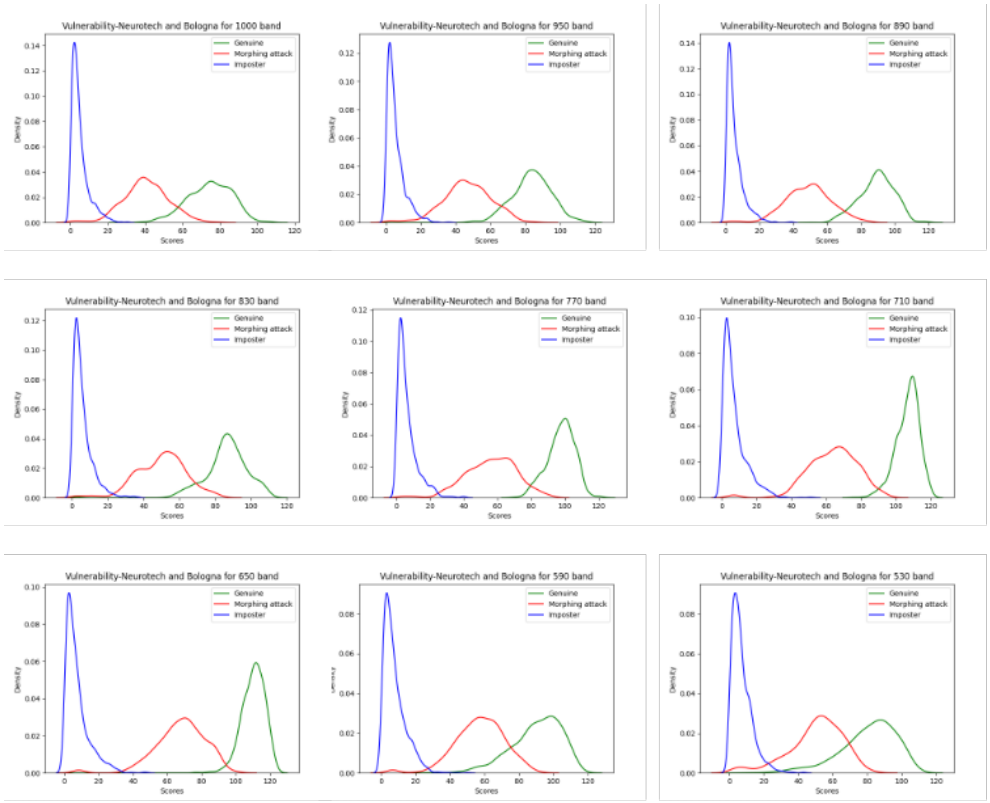


Figure 5.4: A vulnerability study of Neurotechology with UBO morphed images in all spectral bands

5.2.3 RMMR: Relative Morph Match Rate

Another vulnerability metric is the Relative Morph Match Rate (RMMR(%) [71], which combines the recognition accuracy with vulnerability measures. Specifically, when $\tau$is used to calculating either the MMPMR or the FMMPMR, the RMMR can be defined as follows.

$$\text{RMMR}(\tau)_{\text{MMPMR}} = 1 + (\text{MMPMR}(\tau)) - [1 - \text{FNMR}(\tau)] \quad (5.4)$$

$$\text{RMMR}(\tau)_{\text{FMMPMR}} = 1 + (\text{FMMPMR}(\tau)) - [1 - \text{FNMR}(\tau)] \quad (5.5)$$

where FNMR indicates the false rejection rate of the FRS under consideration obtained at the threshold τ.

5.3 Results from Vulnerability analysis

Table 5.2 presents the quantitative values of MMPMR, and FMMPMR computed from all COTS FRS techniques [1] for all three types of morphed images (UBO,

[1]Scores obtained for Nuerotechology are normalized in range o to 1

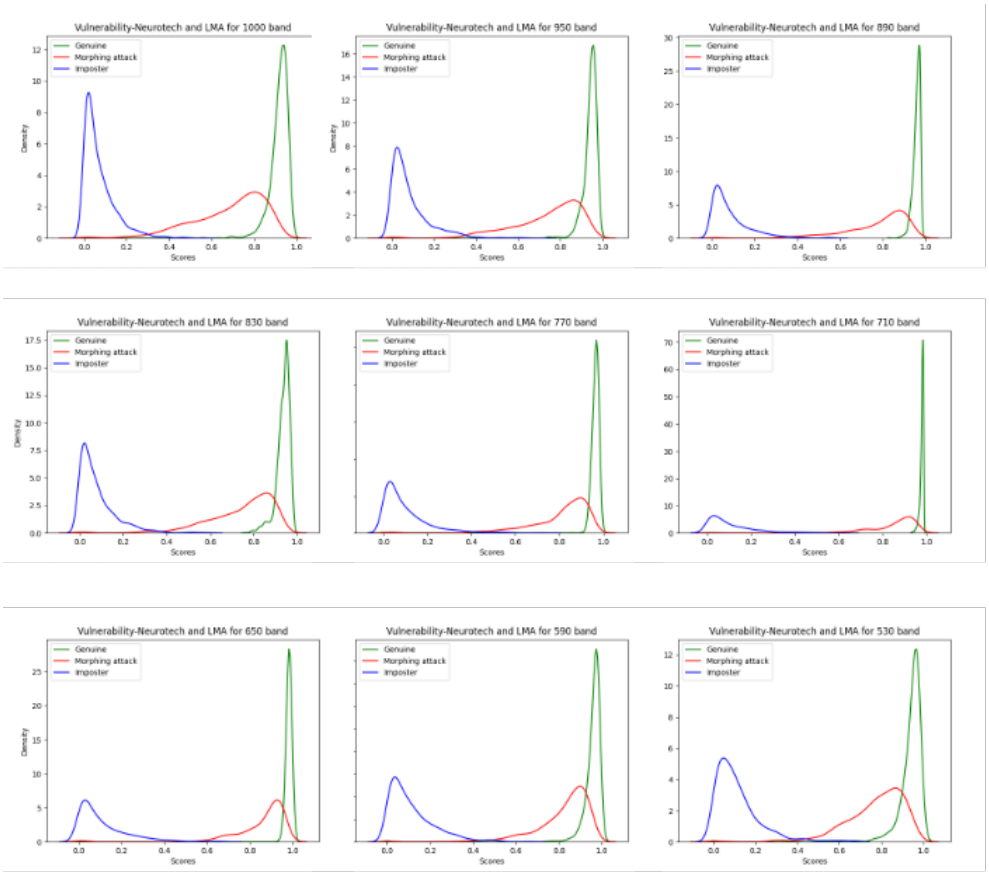


Figure 5.5: A vulnerability study of Neurotechology with LMA morphed images in all spectral bands

LMA and MIPGAN-I) in each spectral band. It is noted that, higher the value of the FMMPMR the higher the threat from morphed images and correspondingly a higher vulnerability of FRS towards morphed images. Based on the obtained results, the key observations are listed below:

- Among the COTS FRS, the highest vulnerability is noted in Cognitec FRS, which is comparatively more vulnerable to all three kinds of face morphing attack methods.
- Among three different morph generation methods, UBO-Morpher indicates a higher vulnerability than all other FRSs.
- The vulnerability of landmark-based morph generation methods is higher than that of deep learning-based morph generation methods. This is observation is made in all spectral bands for both COTS FRSs.
- When UBO morphed images were used for Cognitec FRS, the MMPMR is higher in 710nm spectral band with value 98.16% , which indicates that the Cognitec FRS more vulnerable to the morphed attack using UBO-morpher in this band. This case is also similar with LMA, MIPGAN-I morphed images,

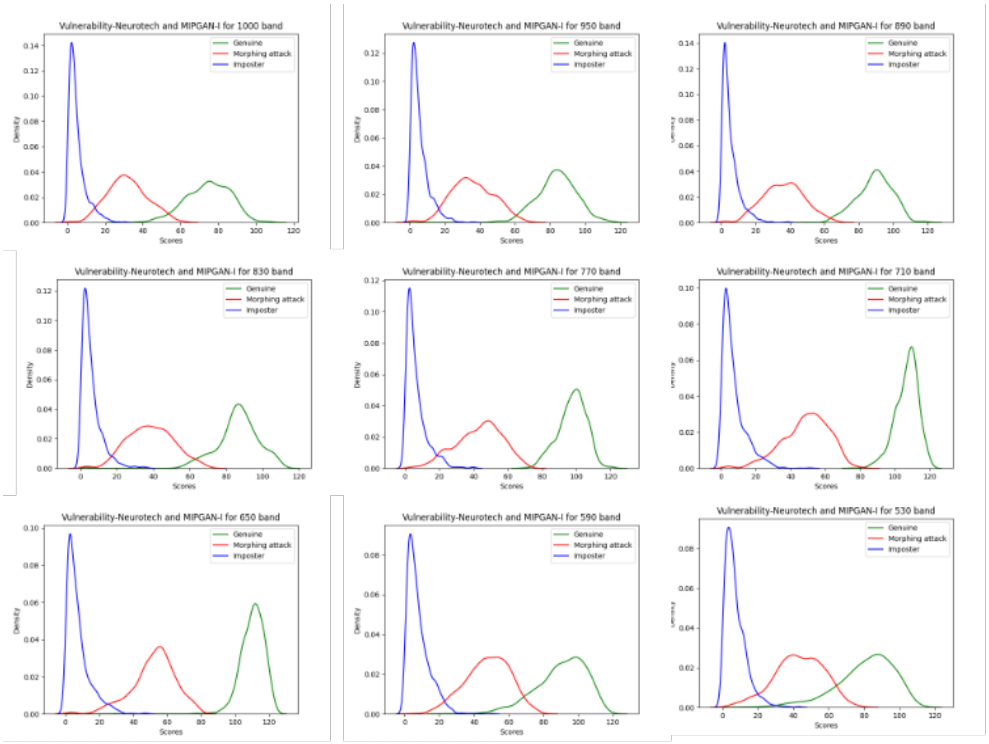


Figure 5.6: A vulnerability study of Neurotechology with MIPGAN-I morphed images in all spectral bands

which have the MMPMR scores of 98.3%, 90.03% in this spectral band.

- For the Neurotechnology FRS, the spectral band 650nm is found comparatively more prone to the attack with MMPMR score of 98.01%, 96.75%, 86.5% repectively for UBO, LMA and MIPGAN-I morphed images.

Table 5.2: MMPMR-FMMPMR result for COTS FRSs

Band	UBO				LMA				MIPGAN-I			
	Cognitec		Neurotec		Cognitec		Neurotec		Cognitec		Neurotec	
	MMPMR	FMMPMR	MMPMR	FMMPMR	MMPMR	FMMPMR	MMPMR	FMMPMR	MMPMR	FMMPMR	MMPMR	FMMPMR
530	93.64	95.02	81.74	85.32	92.75	94.82	77.93	81.68	80.32	84.32	65.49	68.05
590	97.86	97.88	92.84	93.35	96.96	97.11	89.67	90.17	88.81	89.01	77.32	77.67
650	97.29	97.6	98.01	98.03	97.81	98.11	96.75	96.7	90.37	90.85	86.5	86.44
710	98.16	98.18	97.67	97.68	98.3	98.25	95.25	95.14	90.03	89.92	80.56	80.33
770	97.97	97.96	92.83	92.73	96.37	96.34	88.12	87.98	82.92	82.87	71.24	71.04
830	95.14	95.07	85.97	85.97	92.99	92.87	82.69	82.6	66.52	66.31	57.04	56.93
890	96.99	97.04	83.58	83.74	93.11	93.1	80.61	80.72	74.51	74.4	51.39	51.55
950	94.22	94.32	81.15	80.71	90.97	90.98	75.39	75.01	70.68	70.3	48.62	47.78
1000	90.07	90.19	66.58	66.59	85.36	85.5	61.83	61.71	58.76	58.72	36.53	36.43

Chapter 6

Human Observers in Morphing Attack Detection

6.1 Database creation

As noted in section 3.4, there are lack of experiments on human observer analysis of morphing attack detection that utilizes spectral images, thus, we performed a human experiment on how well human can detect morphed images in comparison with spectral images. We began with generating a new database for spectral images and morphed images which included a combination of both regular face images (RGB images) and spectral images. The morphed images used here are created using both landmark-based approaches (LMA, and UBO) and deep learning-based approach (MIPGAN-I), as explained in the section 4.2. Since the morphed attacked detection using spectral imaging can only be utilized in the D-MAD environment, where both bonafide and probe images are included for comparison, the database only corresponds to the D-MAD setting. To make the testing more reliable, we made sure that each image corresponded to a different data subject, and avoided repeating data subjects. Also, to avoid gender bias by participants, a near equal distribution of male and female data subjects were selected in each group.

Furthermore, the database was then divided into three primary subsets for individual analysis of spectral and regular color images with morphed images. The first subset consists of 38 pairs of bonafide images and probed (bonafide images or morphed) images. All images in this subset are regular RGB images. A sample image from the first subset is presented in the Figure 6.1.

Similarly, the second subset is presented with 36 pairs of one spectral band image with probe (bonafide or morphed) images. The images from the spectral band 650nm are included here. A sample image from the second subset in the human observation database is presented in the Figure 6.2. In contrast, the last subset includes 26 pairs of one probe (bonafide or morphed) image with all nine spectral band images. The included probe image is the regular (RGB, 3-channel) image. A sample image from the third subset in the human observation database

Figure 6.1: A sample image from first subset in the Human observation database

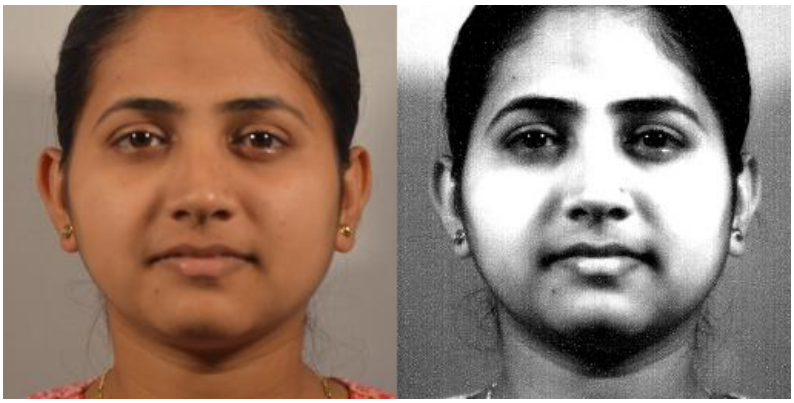


Figure 6.2: A sample image from second subset in the Human observation database

is presented in the Figure 6.3.

Figure 6.3: A sample image from third subset in the Human observation database

A total of 100 images were selected where morphed images generated from all three techniques are incorporated. The experiment was confined to 100 photos due to the time restrictions involved in assessing these images for human observ-

ers. As it was crucial to keep in mind that the detection experiments should not cause the observers to lose attention, 100 images was determined a preferred number of images in initial experiment done on three participants which is further discussed below. The Table 6.1 shows the statistics of images used in each subset.

Table 6.1: Statistics of number of images used for human observation experiment

Category	Experiment-1	Experiment-2	Experiment-3	Total
Female subjects	18	16	11	45
Male subjects	20	20	15	55
Bona fide images	19	18	13	50
Morphed images	19	18	13	50
MIPGAN-I morphed images	7	7	5	19
Bologna morphed images	6	6	5	17
LMA morphed images	6	5	3	14
Total	38	36	26	100

6.2 Human Observer Platform for Evaluation

In order to facilitate the experiment while taking consideration of confidentiality of the data being used, a platform hosted by NTNU server QuickEval was used. In addition, the human observer platform is designed by incorporating the guidelines of the General Data Protection Regulation (GDPR) to protect and preserve participants' privacy with full considerations of the anonymity of participants.

Furthermore, the new evaluation platform simulates a real-world scenario in which photographs are shown to observers to determine whether they are genuine or morphed. It consists of three different experiments, each of which incorporates subsets of data in the database (as explained in the section 6.1).

The platform is designed to be operated in a desktop environment. Before inviting participants to the experiment, we took an initial experiment with three observers. In this experiment, 144 images were included for detection. However, this number was reduced to 100 in the final observation by considering the feedback received from the initial observer: as participants might lose interest in detecting the images if a high number of images are included for comparison. Thus, a total of 100 images were finalized for the final experiment.

A brief introduction to the experiment and its objectives was presented to each participant on the home page, where users were directed to enter their information, including their age range (such as 21-25, 26-30) and gender. The portal then takes the user to the first experiment, in which they are shown two images side-by-side and asked to detect if they are of the same person.

In experiment 1, images from the first subset of the database were presented, where each image consists of regular RBG images. After reviewing 38 pairs of images in the first experiment, participants were presented with images from

(a) Experiment-1 **(b)** Experiment-2 **(c)** Experiment-3

Figure 6.4: Graphics user interface of each experiment

a second subset of the database in the second experiment. In the second experiment, regular RGB images and one spectral band image were presented. The images from the spectral band 650 nm are utilized for this comparison. At last, the third experiment was shown, where images from the third subset of the database were presented. Here, we presented a regular RGB probe with nine spectral band images and asked to detect the RGB images by comparing them with all spectral band images. The idea is to identify how effectively the user can detect the morphed images by analyzing the spectral images. The third experiment The Figure 6.4 shows the graphical user interface for the human observers' experimental setup in each experiment used in this work.

6.3 Observer Evaluation

Three alternative configurations related to Differential Morphing Attack Detection (D-MAD) in respect to spectral images make up the online evaluation platform for benchmarking the human observer ability to detect morphed images. Participants from both inside and outside NTNU who indicated no prior knowledge on morphing process were invited via the link https://quickval.no/observer/883. Each participant was given a brief introduction and instructions to the goals of the study and were further asked for consent under GDPR. In addition, each participant was instructed to participate anonymously in order to protect their personal information. Furthermore, in the set of questionnaire, the participants were asked to provide information regarding age range such as 21-25, 26-30 and their gender.

The Table 6.2 shows the different information of 51 human observers participated in the experiment. All these participants noted not having any prior knowledge, training or experiment on detecting morphed images.

6.4 Findings, Analysis, and Discussion

The experiment results and analysis the findings are presented in this section, along with a complete analysis of the trends in human observer evaluation.

Table 6.2: Classification of participants in gender and age range

Age range	Female	Male	Total
16-20	0	1	1
21-25	4	12	16
26-30	8	16	24
31-35	3	5	8
36-40	0	1	1
41-45	0	1	1
Total	15	36	51

6.4.1 Metrics for Evaluations

To illustrate the findings, we use an accuracy metric, defined as the total number of correct classifications of morph as morph and bonafide as bonafide, aligning the results to the NIST FRVT MORPH challenge. The accuracy of automated MAD algorithms is provided as the Attack Presentation Classification Error Rate (APCER) and Bonafide Classification Error Rate (BPCER). The accuracy is defined as follows:

$$Accuracy = \frac{(1-APCER)+(1-BPCER)}{2} \tag{6.1}$$

6.4.2 Accuracy of detection: Experiment Type

The Table 6.3 shows the quantitative results of each experiment obtained from 51 observers, including 15 female and 36 male participants. It also includes the accuracy of each gender in each experiment. The main observation are presented below:

- The overall accuracy of recognizing morphed photos compared to the spectrum images presented in this experiment is 69.39%, which suggests that human observers are more likely to overlook the morphed images when spectral images are used as a reference. Similarly, in each experiment, detecting morphing photos is 80.49%, 68.57%, and 64.80%, respectively, for experiment-1, experiment-2, and experiment-3.
- Human observers show higher accuracy (80.49%) in spotting morphed images when both images in a comparison pair are conventional RGB images.
- In all three experiments, female observers exhibited higher detection accuracy than male observers, with 82.34%, 71.43%, and 66.92% accuracy in each experiment, respectively. It implies that female observers are more likely to notice morphed images; nevertheless, it is worth noting that only 15 female observers participated in the study, compared to 36 male observers.
- Among all three different types of the experimental setup, the combination of probe images with all nine spectral images is challenging compared to

other experiment types. The accuracy of detection observed for this setting (Experiment-3) is 64.80%.

Table 6.3: Human observers' accuracy on detecting morphed images in each experiment

Gender	Experiment-1	Experiment-2	Experiment-3	Overall Accuracy
Female	82.34	71.43	66.92	71.06
Male	79.69	67.35	63.90	68.68
Overall Accuracy	80.49	68.57	64.80	69.39

6.4.3 Accuracy of detection: Gender of observers

The Table 6.4 shows the quantitative results of Experiment obtained from 51 observers on detecting the different types of morphed images. The Table 6.4 also presents the how well the observers can detect different types of morphed images. As noted from the Table 6.4 following are the main observations:

- The findings from 51 human observers show that detecting morphed facial images is challenging.It aligns with the results obtained on other similar studies as also discussed in chapter 3.
- The ability of a human observer to detect deep-learning-based morphed images is higher than that of landmark-based morphed images.
- From the observation, it is observed that the human observer's ability to detect the bonafide images is comparatively higher than detecting morphed images. The detection accuracy of 89.43% for bonafide images; on the other hand, for UBO, LMA, and MIPGAN-I morphed images is 62.22%, 32.30%, and 62.96% respectively.
- The detect percent of LMA morphed images is deficient (32.30%), indicating that when LMA morphed pictures are presented to cross the border, the human inspector is more likely to miss them.

Table 6.4: Gender wise observers' accuracy on detecting morphed images

Gender	Bonafide image	UBO morphed	Mipgan morphed	LMA morphed
Female	95.36	60.74	64.82	26.0
Male	86.88	62.86	62.17	35.0
Overall Accuracy	89.43	62.22	62.96	32.30

An analysis has also done on accuracy of male and female to differentiate the images with their own and opposite gender. The Table 6.5 shows the result of the experiment and following are the main observations:

- Female observers, on average, show a more remarkable ability to recognize either gender than male observers. It suggests that female observers are

more likely than male observers to recognize morphing images; nevertheless, it is essential to note that the number of female observers is 15, while male observers are 36.

- Furthermore, female observer demonstrated higher accuracy in recognizing morphed images in each experiment.

Table 6.5: Classification of accuracy on same or different gender data

Gender	Experiment-1		Experiment-2		Experiment-3	
	Male	Female	Male	Female	Male	Female
Female	83.14	81.63	64.74	78.94	65.33	69.09
Male	80.46	78.82	62.80	72.44	63.32	64.69

Chapter 7

Morphing Attack Detection

7.1 Morphing Attack Detection using spectral images

Using the workflow of a generic biometric system as an example, this idea is feasible in detection at the time of authentication, where a live capture from an authentication attempt serves as an additional source of information for the morph detector in addition to reference images from the passport. The spectral camera would be utilized to capture live images, which creates multiple spectral band images. Along with the images from the passport, these spectral images would then be employed in the face morphing attack detection algorithm. The morphing attack detection algorithms extract features from comparing images and thus decide whether the image is genuine or morphed based on the extracted features.

7.1.1 Morphing attack detection using feature differentiation

Focusing on morph detection, image morphing is expected to cause changes in textual features between bonafide and morphed face images. Local Binary Patterns (LBP) and Binarized Statistical Image Features (BSIF) are well-known general-purpose texture descriptors that have proven effective in various texture classification problems. Thus, LBP features and BSIF features are extracted from the aligned cropped face images. Obtained feature values are stored in corresponding histograms. The LBP feature descriptors are extracted according to patches of 3×3. The values of the LBP binary code are represented by the feature vectors, which are normalized histograms of size 256. Similarly, 12-bit filters are used to create 8-bit BSIF feature vectors. The feature vectors are then loaded into an Radial Basis Function (RBF) kernel-based SVM. Since the linear SVM was first utilized but failed to provide adequate training accuracy, we switched to the Grid-Search SVC. Grid search is a hyperparameter tuning technique that may facilitate building and evaluating a model for every combination of algorithm parameters per grid.

Furthermore, since a morphed face image contains the attacker's biometric

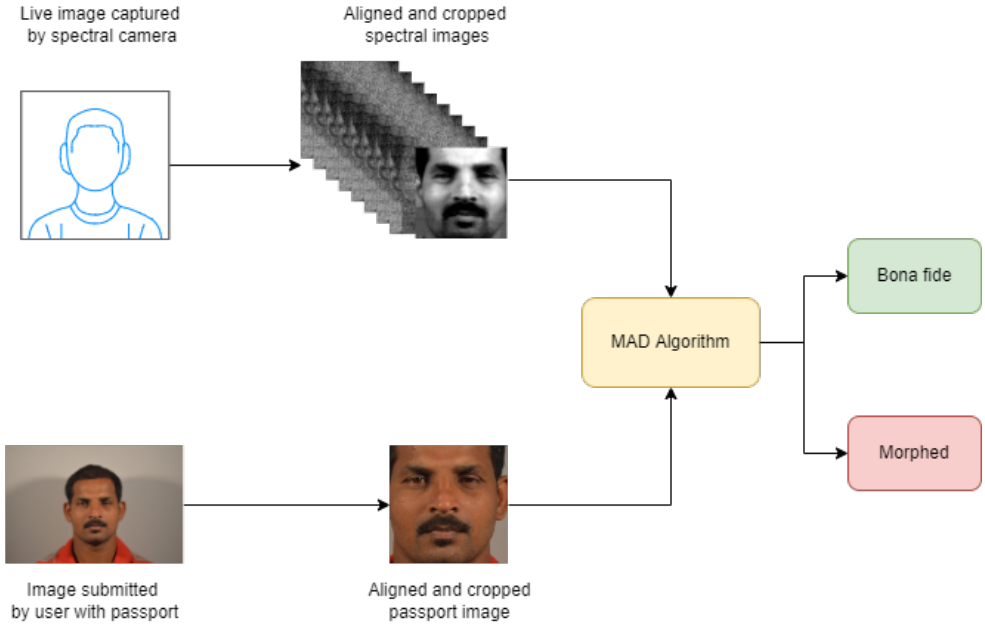


Figure 7.1: Proposed model of morphing attack detection technique

information and that of the accomplice, thus its deep face representation is likely to differ considerably from that detected in the probe image, at least in some aspects. By incorporating this idea, we also employed in the ArcFace to get the embedding vectors. Therefore, we examined two MAD techniques based on texture descriptors: LBP [72] and BSIF [29] with 12-bits filter and one MAD based on deep face representations (feature vectors) retrieved using ArcFace [66].

The feature vectors are then loaded into an RBF kernel-based SVM. For all classical baseline models, the feature representation of the image to be tested is subtracted from the feature representation of the RGB images before feeding it to the SVM classifier as proposed in [30]. Using a disjoint training set, feature vectors for each technique are retrieved, and support vector machines (SVM) with RBF kernels are trained to distinguish between genuine and morphed face images. For the training and testing purpose, we divided the dataset created in the chapter 4 into train and test segments in a 60/40 ratio to analyze the morphing attack detection. The split is done in such a way that none of the trains set participants have images in the test set, neither in the genuine nor in the morphed set of test class. Table 7.1 shows the number of images used in each set. All three MAD techniques are trained in three different approaches, employing three different sets of morphed images developed in this work.

Table 7.1: The number of images in train and test set for experimental evaluations

Category	Training Set	Testing Set
Morph	98	55
Bonafide	7206	4741

7.2 Evaluation metrics

This subsection includes the evaluation of the accuracy of different MAD approaches using spectral images on different morphed images generated in this study. We used the standard measures such as APCER, BPCER, and EER rates for morph attack detection to evaluate network performance. APCER stands for Attack Presentation Classification Error Rate and is defined as the proportion of attack images incorrectly classified as bonafide images. APCER is the rate at which morphs pass undetected. In contrast, BPCER stands for Bonafide Presentation Classification Error Rate and is defined as the proportion of bonafide images incorrectly classified as attack images. The APCER and BPCER rates represent the Type 1 and Type 2 error, or the false positive and negative rates. The point when BPCER and APCER are equal is called as Equal Error Rate (EER). Furthermore, BPCER is also called a false alarm rate, and highly recommended to restrict it to fixed thresholds. The rates at a defined threshold are also reported for morph detection, often to control the false alarm rate. APCER5 is the APCER rate, where BPCER is 5%. Similarly, APCER10 is the rate when BPCER is 10%. These rates are plotted in a Detection Error Tradeoff (DET) curve.

The accuracy of different MAD approaches obtained utilizing the LBP, BSIF, and ArcFace feature embedding, respectively, is shown in the Table 7.3, Table 7.2 and Table 7.4. The main observations from the DET curve for the feature differentiation using ArcFace embedding are as following:

- The deep face differentiation technique has a good detection accuracy compared to other approaches. The performance is even better in detecting morphed images created using the deep-learning-based method (MIPGAN-I). In all spectral bands, the error rate for this combination is 0.0 as shown in Table 7.2.
- In terms of landmark-based morphed images, the detection performance of the deep face differentiation technique (ArcFace embedding) compares favorably to LMA based morphed images, with an error rate of 0.0 for all bands except 650nm, which has a 1.82 percent error rate.
- The performance of the deep face differentiation technique (ArcFace embedding) in terms of spectral bands is best at 1000nm, with an error rate of 0.0 in all three types of morphed images.

Similarly, observations for the texture feature differentiation (LBP and BSIF) from Table 7.3, Table 7.4 are as follows:

- Good detection rates are obtained for texture descriptors, with BSIF obtain-

Table 7.2: APCER/BPCER result for ArcFace-SVM MAD approach

Band	UBO			LMA			MIPGAN-I		
	EER	APCER[%]		EER	APCER[%]		EER	APCER[%]	
		5	10		5	10		5	10
530	1.82	0	0.00	0	0	0.00	0	0	0.00
590	1.82	0	0.00	0	0	0.00	0	0	0.00
650	1.82	0	0.00	1.82	0.36	0.18	0	0	0.00
710	1.82	0	0.00	0	0	0.00	0	0	0.00
770	1.82	0	0.00	0	0	0.00	0	0	0.00
830	1.82	0	0.00	1.82	0	0.00	0	0	0.00
890	1.82	0	0.00	0	0	0.00	0	0	0.00
950	1.82	0	0.00	1.82	0	0.00	0	0	0.00
1000	0	0	0.00	0	0	0.00	0	0	0.00

ing the greatest performance of D-EER=0.0 %.

- Using the BSIF texture descriptors, good performance is achieved in the spectral bands in the intermediate range, such as 650, 710, 770, and 830, when LMA based morphing images are employed. However, for the MIPGAN-I and UBO morphing images, detection accuracy is good in the higher and lower frequency ranges such as 530 and 1000nm with D-EER = 0.0%.
- On the other hand, when LPB feature differentiation is used for detection, better results are obtained in the higher frequency ranges, such as 530 and 590nm. The D-EER of 0.0 is observed for these bands.

The DET curve is shown in the Figure 7.2, Figure 7.3 and Figure 7.4. The following observation are made DET curve results:

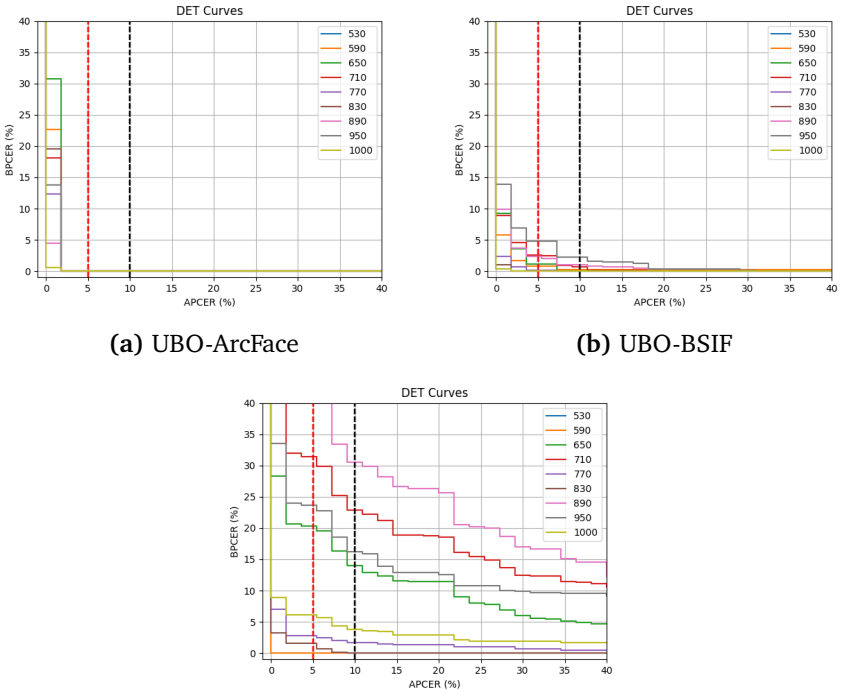
- ArcFace embedding performs better in detecting UBO morphed images with error rate of D-ERR = 0.0, as shown in Figure 7.2. Furthermore, the LBP-SVM MAD method has a lower performance rate, implying that when the LBP-SVM MAD algorithm is applied, it is more likely to overlook the UBO morphing images.
- Similarly, when MIPGAN-I morphing images are presented to three MAD techniques, the same result is observed, as illustrated in Figure 7.3. When using a deep feature differentiation MAD strategy, the MIPGAN-I morphed images are more likely to be recognized, however using an LBP-based MAD

Table 7.3: APCER/BPCER result for BSIF-SVM MAD approach

Band	UBO			LMA			MIPGAN-I		
	EER	APCER[%]		EER	APCER[%]		EER	APCER[%]	
		5	10		5	10		5	10
530	0	0	0.00	1.82	0.37	0.37	0	0	0.00
590	1.82	0.83	0.21	1.82	0.21	0.21	0	0.41	0.00
650	3.64	1.09	0.00	1.82	0	0.00	3.64	0	0.00
710	3.64	2.44	0.17	3.64	0	0.00	3.64	2.79	0.17
770	1.82	0.17	0.00	3.64	0	0.00	3.64	0.17	0.00
830	1.82	0	0.00	0	0	0.00	3.64	0.87	0.00
890	3.64	2.04	0.85	3.64	3.07	2.73	3.64	1.36	0.00
950	3.64	4.78	1.59	5.45	3.36	1.42	3.64	1.24	0.00
1000	0	0	0.00	0	0.19	0.00	0	0	0.00

Table 7.4: APCER/BPCER result for LBP-SVM MAD approach

Band	UBO			LMA			MIPGAN-I		
	EER	APCER[%]		EER	APCER[%]		EER	APCER[%]	
		5	10		5	10		5	10
530	0	0	0.00	0	0	0.00	0	0	0.00
590	0	0	0.00	0	0	0.00	0	0	0.00
650	12.73	19.64	12.91	16.36	27.09	22.18	7.27	8.73	4.73
710	18.18	29.97	22.30	18.18	41.29	31.01	12.73	22.3	15.16
770	1.82	2.51	1.67	5.45	4.52	2.84	5.45	3.18	2.34
830	1.82	0.7	0.00	5.45	4.52	2.43	1.82	0.52	0.35
890	21.82	40.55	29.64	25.45	55.03	46.34	16.36	35.26	24.19
950	14.55	22.65	15.93	25.45	55.58	47.96	9.09	15.93	9.56
1000	5.45	5.73	3.63	14.55	23.47	18.70	7.27	6.68	4.58



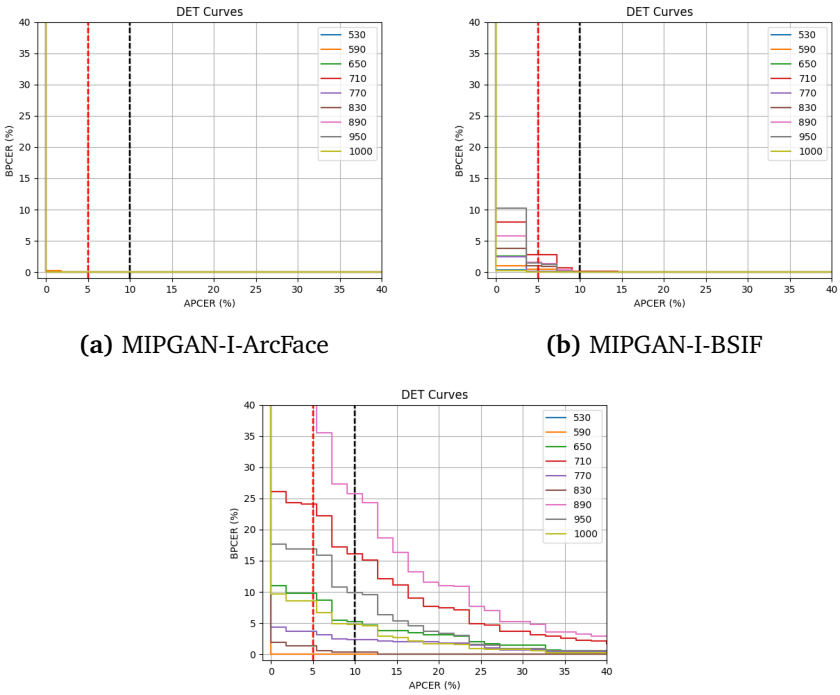
(a) UBO-ArcFace **(b)** UBO-BSIF

(c) UBO-LBP

Figure 7.2: DET curve for UBO-Morpher with three different MAD techniques

approach has the possibility to miss the detection.

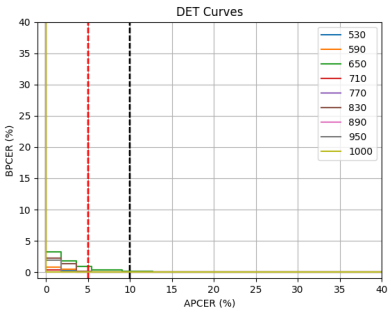
- Likewise, similar result is found when LMA morphed images are provided, as depicted in Figure 7.4.



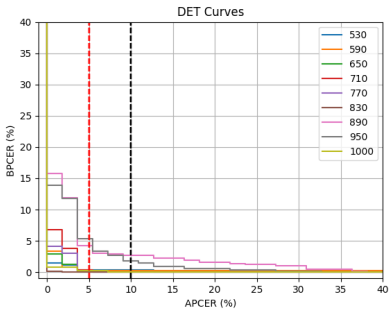
(a) MIPGAN-I-ArcFace **(b)** MIPGAN-I-BSIF

(c) MIPGAN-I-LBP

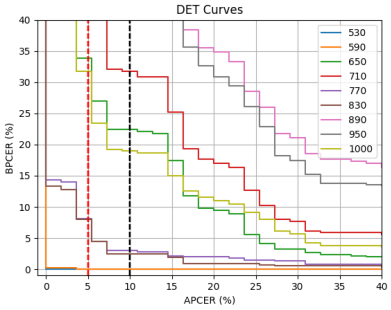
Figure 7.3: DET curve for MIPGAN-I with three different MAD techniques



(a) LMA-ArcFace



(b) LMA-BSIF



(c) LMAI-LBP

Figure 7.4: DET curve for LMA with three different MAD techniques

Chapter 8

Discussion

Border control and other security applications requiring identification, such as official identity cards, surveillance, and law enforcement have increasingly incorporated biometric facial recognition technology. These systems provide high accuracy at a low operational cost, with an automated fail-safe that allows a human expert on-site to verify the scenario if the algorithm generates a false alarm. In particular, face recognition systems have a significant edge over other biometric systems because of these factors as a result, the International Civil Aviation Organization (ICAO) has recommended that all electronic documents include a facial reference image. The face is thus the only biometric identifier included in important documents like passports worldwide.

However, despite their widespread success, facial recognition systems still are not impervious to attack. The widespread use of automatic biometric systems in border control has highlighted critical vulnerabilities in the border security system, especially the systems' inability to recognize a fraudulent image. Moreover, some countries require that applicants give a face reference image either digitally or as a physical print instead of a live photo during the registration process which exacerbate the issue allowing criminals to alter the picture and use a morphed photograph instead of a real image. As face morphing attacks create face images that multiple people may use to authenticate themselves, morph attack is one type of deceptions that has lately been identified as a serious threat.

8.1 Vulnerability analysis of different FRS using spectral images

When automated face morphing technologies, such as landmark manipulation and GAN generation create artifacts, some distinguishing features can suggest that the image was morphed even though they are not always apparent to the human eye. These morphing anomalies can be observed in very high or low-frequency spectra. The spectrum imaging technique obtains complementary image information (i.e., reflectance or emittance) across discontinuous spectral bands to produce

typical discriminating features.

This study explored the attack success of images against the contributing subjects using six different FRSs, including two commercial Off-The-Shelf (COTS) and four open-source deep-learning-based FRSs. COTS FRS includes Cognitec FRS and Neurotec, whereas open-source FRS includes ArcFace, ArcFacePlus, CosFace, and CosFacePlus. The attack potential is depicted via a distribution plot of the impostor, genuine, and morphing attack comparison scores. While analyzing the distribution plot in the deep-learning-based FRSs, the imposter and genuine scores overlapped. The attack potential of the created morphed images are challenging to detect using the spectral images for the deep learning-based face recognition system. One of the possible reasons for this could be because these face recognition systems are designed to operate on conventional colored (RGB) images. Thus, we fine-tuned the FRS models to deal with spectral images, however, the distribution plot was still found to be overlapping. When the plots are overlapping, evaluating these deep-learning algorithms' attack potential using the morphed images created in this study and spectral images becomes a challenging task.

In contrast, the distribution of imposter and genuine comparison scores shows a clear distinction between them for the COTS FRSs. In addition, the scores of all types of morphed images lie between genuine and imposter scores. Thus, it indicates that morphed images created in this study have potential to attack these COTS FRSs. This shows that the spectral images could be utilized for determining the attack potential of the COTS FRSs (Cognitec and Neurotechnology).

8.2 Human observation in detecting morphed images

As the morphed image seems identical to both contributing subjects, it presents a greater challenge for human viewers to detect morph images. While an amateur attacker may create a morphed image with ghost artifacts that are easy to spot, a professional attacker could create a high-quality image by removing unnatural artifacts introduced during the morphing process. Such images are especially more challenging for a human observer to spot the morphs. Several studies also concluded that human observers often fail to detect the morphed images. An exception could be granted for experts who have been specially educated to identify morphing and can accurately detect the facial morph.

In this study, an experiment was also carried out to determine the human observer's capacity to detect morphed images using spectral images. Observers were provided with the morphed images in three distinct ways: ordinary color images, one spectral band image, and all spectral band images. This study, like others that looked at human error in detecting morphed photos, showed that humans are prone to making mistakes when it comes to detecting morphed images. If the reference photos are spectral images, the rate was observed to be significantly higher. In a preliminary experiment performed with three participants to get feedback before making the experiment available to everyone, participants were asked on factors that makes it challenging to them to detect morphed images when

presented with spectral images. The observer noted that they usually use texture features, shades, lighting, and so on as a reference while detecting the morphed images in regular RGB images; however, these features were absent in spectral images making it hard to detect morphs. Furthermore, they stated that they are accustomed to looking at conventional images, but since they were provided with spectral images for the experiment, they did not feel very confident and were rather indecisive.

8.3 Spectral images in detecting morphed images

Three different MAD approaches have been evaluated, including the texture feature descriptors (LBP, BSIF) and deep feature descriptor (ArcFace embeddings) methods using the SVM classifier. The results reveal that when several MAD approaches are trained and tested with spectral images, they perform well in detecting morphed images. This performance is significantly higher in the higher and lower frequency bands (such as 1000nm and 530nm). It indicates that there is a high possibility of detecting morphed images when high or lower frequency band reference images are used. This statement is also supported by the study performed by Chaudhary et al. [73]. This states that most morphing artifacts reside in the high-frequency spectrum, and they are discernible when we examine the low frequency and high-frequency data separately. However, it is worth mentioning that we employed a small set of morphed images in the training and testing set (98, 55, respectively) for this experiment, and the results may vary if a more extensive morphed dataset is used.

Overall, although some challenges regarding limited data set and inexperienced observer may have affected the result to some extent, the study could still set as a stepping stone in future research to detect morphing attacks using spectral images.

Chapter 9

Conclusion

The main purpose of this study was to identify the attack potential of efficient FRSs using the morphed images created when spectral images are presented as a reference. This research project also aims to assess the efficiency of various MAD techniques for detecting morphed images with respect to spectral images.

A new database was created which consist of the 484 morphed images created using three different morphing techniques: UBO, LMA and MIPGAN-I. The database also included spectral images in nine different spectral bands: 530nm, 590nm, 650nm, 710nm, 770nm, 830nm, 890nm, 950nm, 1000nm. It could serve as a referenced database for future research for similar projects and studies. The possibility of attack by newly created database is determined with six different FRSs including two COTS (Cognitec, and Neurotechnology) and four different deep learning based FRSs (ArcFace, ArcFacePlus, CosFace, CosFacePlus). The attack potential was demonstrated by computing the comparison score distributions of an imposter, genuine, and morphed and was compared against original probe identities contained in the database. Cosine distance between two face feature embedding was used to compute the comparison score. For the deep learning based approach, it was observed that imposter and genuine score are in the same range indicating that the determination of the vulnerability study of these methods are challenging when spectral images are used as a reference.

In contrast, COTS FRSs were found to be vulnerable to the potential attack. This attack rate is highest for Cognitec than the Neurotechnology. The UBO morphed images have the highest potential of attack in 710nm spectral band with value MMPMR 98.16% and 98.18% FMMPMR in Cognitec while 650nm spectral band has highest threat to attack for Neurotechnology with 98.01% and 98.03% score in MMPMR and FMMPMR, respectively. However, the MIPGAN-I generated morphed images are comparatively less threatening to both FRSs.

At the end of the thesis work, we succeeded in answering the following research question:

1. Can spectral imaging help in detecting morphing attacks?
   Evaluating different MAD approaches such as LBP and BSIF texture feature differentiation and ArcFace deep feature differentiation with Support Vector

Machine shows that even though the attack potential is high, the highest detection accuracy is achieved. These approaches offer good performance in detecting all three types of morphed images, and the best detection is achieved at higher and lower frequency ranges (530nm and 1000nm) with EER = 0.0. The findings also reveal that deep face differentiation has a higher detection accuracy than texture feature differentiation techniques. The performance is even better in detecting morphed images created using the deep-learning-based method (MIPGAN-I). Therefore, from the analysis, we can conclude that the spectral images could be useful in detecting the morphed attacks.

2. What proficiency does a novice Human observer have in spotting morphed images from spectral images?
   An experiment was conducted to determine the human observer's capacity to detect the morphed images when spectral images are presented as a reference. It was observed that humans are more prone to miss morphed images. When morphed images are given with standard color images, the observers achieved an accuracy of 80.49%; however, when presented with all spectral bands, the accuracy dropped to 64.80%. Therefore, according to experiment results, an inexperienced human observer's capacity to recognize morphed images while examining spectral images is relatively poor. However, it should be noted that the experiment consisted of inexperienced human observers, and the result could be different when experts with experience and training on detecting frauds in identity documents were taken for the experiment.

9.1 Limitation and Future Work

Although this paper presents different reference image for detecting morphing attacks tested empirically using COTS FRS, it has few limitations. In the current scope of work, we evaluated the impact of only digital images. However, the MAD mechanism used in this study has not been tested with different image configurations, such as print and scan (re-digitizing) images, which needs to be addressed in future research.

Because the dataset we used in this investigation was captured in an experimental context rather than a real-world scenario, the performance measured in this study lacks critical information on how well it adjusts in real-world scenarios. Furthermore, the number of morphed images in the training and testing sets from each morphing generating approach is relatively low (98 and 55, respectively). This small collection may not necessarily represent the performance of detecting morphed attacks. Thus, better study could have been made if MAD techniques were performed on bigger morphed dataset.

Furthermore, the current scope of study only examined morphing attack detection using feature differentiation for individual spectral bands; nevertheless, it is critical to investigate how MAD approaches work when feature differentiation

of all bands is performed together. Thus, this aspect needs to be investigated in future studies.

Bibliography

[1] D. ICAO, '9303-machine readable travel documents-part 9: Deployment of biometric identification and electronic storage of data in emrtds,' *International Civil Aviation Organization (ICAO)*, 2015.

[2] M. Ferrara, A. Franco and D. Maltoni, 'The magic passport,' in *IEEE International Joint Conference on Biometrics*, 2014, pp. 1–7. DOI: 10.1109/BTAS.2014.6996240.

[3] L. D. Jacob, 'Real vs fake faces: Deepfakes and face morphing,' in *Graduate Theses, Dissertations, and Problem Reports.8059*, 2021. DOI: 10.33915/etd.8059.

[4] D. E. King, 'Dlib-ml: A machine learning toolkit,' *The Journal of Machine Learning Research*, vol. 10, pp. 1755–1758, 2009.

[5] M. Hildebrandt, T. Neubert, A. Makrushin and J. Dittmann, 'Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps,' in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, IEEE, 2017, pp. 1–6.

[6] A. Makrushin, T. Neubert and J. Dittmann, 'Automatic generation and detection of visually faultless facial morphs,' in *International conference on computer vision theory and applications*, SciTePress, vol. 7, 2017, pp. 39–50.

[7] T. Neubert, A. Makrushin, M. Hildebrandt, C. Kraetzer and J. Dittmann, 'Extended stirtrace benchmarking of biometric and forensic qualities of morphed face images,' *IET Biometrics*, vol. 7, no. 4, pp. 325–332, 2018.

[8] S. Venkatesh, H. Zhang, R. Raghavendra, K. Raja, N. Damer and C. Busch, 'Can gan generated morphs threaten face recognition systems equally as landmark based morphs? -vulnerability and detection,' Apr. 2020. DOI: 10.1109/IWBF49977.2020.9107970.

[9] S. Venkatesh, R. Ramachandra, K. Raja and C. Busch, 'Face morphing attack generation and detection: A comprehensive survey,' *IEEE Transactions on Technology and Society*, vol. 2, no. 3, pp. 128–145, 2021. DOI: 10.1109/TTS.2021.3066254.

[10] N. Damer, A. M. Saladie, A. Braun and A. Kuijper, 'Morgan: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network,' in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE, 2018, pp. 1–10.

[11] M. Ferrara, A. Franco and D. Maltoni, 'Decoupling texture blending and shape warping in face morphing,' in *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, IEEE, 2019, pp. 1–5.

[12] E. Sarkar, P. Korshunov, L. Colbois and S. Marcel, 'Vulnerability analysis of face morphing attacks from landmarks and generative adversarial networks,' *arXiv preprint arXiv:2012.05344*, 2020.

[13] T. Karras, S. Laine and T. Aila, 'A style-based generator architecture for generative adversarial networks,' in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 4401–4410.

[14] H. Zhang, S. Venkatesh, R. Ramachandra, K. Raja, N. Damer and C. Busch, 'Mipgan—generating strong and high quality morphing attacks using identity prior driven gan,' *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 3, pp. 365–383, 2021. DOI: 10.1109/TBIOM.2021.3072349.

[15] N. Damer, K. Raja, M. Süßmilch, S. Venkatesh, F. Boutros, M. Fang, F. Kirchbuchner, R. Ramachandra and A. Kuijper, 'Regenmorph: Visibly realistic gan generated face morphing attacks by attack re-generation,' *arXiv preprint arXiv:2108.09130*, 2021.

[16] 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)*, 2017, pp. 555–563. DOI: 10.1109/BTAS.2017.8272742.

[17] R. Ramachandra, S. Venkatesh, K. Raja and C. Busch, 'Detecting face morphing attacks with collaborative representation of steerable features,' in *Proceedings of 3rd International Conference on Computer Vision and Image Processing*, Springer, 2020, pp. 255–265.

[18] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-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)*, IEEE, 2017, pp. 1–6.

[19] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl and C. Busch, 'Prnu-based detection of morphed face images,' in *2018 International Workshop on Biometrics and Forensics (IWBF)*, 2018, pp. 1–7. DOI: 10.1109/IWBF.2018.8401555.

[20] C. Seibold, W. Samek, A. Hilsmann and P. Eisert, 'Accurate and robust neural networks for security related applications exampled by face morphing attacks,' *arXiv preprint arXiv:1806.04265*, 2018.

[21] L. Wandzik, G. Kaeding and R. V. Garcia, 'Morphing detection using a general-purpose face recognition system,' in *2018 26th European Signal Processing Conference (EUSIPCO)*, IEEE, 2018, pp. 1012–1016.

[22] C. Seibold, W. Samek, A. Hilsmann and P. Eisert, 'Detection of face morphing attacks by deep learning,' in *International Workshop on Digital Watermarking*, Springer, 2017, pp. 107–120.

[23] M. Ferrara, A. Franco and D. Maltoni, 'Face morphing detection in the presence of printing/scanning and heterogeneous image sources,' *arXiv preprint arXiv:1901.08811*, 2019.

[24] K. Raja, S. Venkatesh, R. Christoph Busch *et al.*, 'Transferable deep-cnn features for detecting digital and print-scanned morphed face images,' in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2017, pp. 10–18.

[25] N. Damer, S. Zienert, Y. Wainakh, A. M. Saladié, F. Kirchbuchner and A. Kuijper, 'A multi-detector solution towards an accurate and generalized detection of face morphing attacks,' in *2019 22th International Conference on Information Fusion (FUSION)*, IEEE, 2019, pp. 1–8.

[26] 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*, 2015, pp. 815–823.

[27] O. M. Parkhi, A. Vedaldi and A. Zisserman, 'Deep face recognition,' 2015.

[28] T. Ahonen, A. Hadid and M. Pietikäinen, 'Face recognition with local binary patterns,' in *European conference on computer vision*, Springer, 2004, pp. 469–481.

[29] J. Kannala and E. Rahtu, 'Bsif: Binarized statistical image features,' in *Proceedings of the 21st international conference on pattern recognition (ICPR2012)*, IEEE, 2012, pp. 1363–1366.

[30] U. Scherhag, C. Rathgeb and C. Busch, 'Towards detection of morphed face images in electronic travel documents,' in *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*, IEEE, 2018, pp. 187–192.

[31] U. Scherhag, C. Rathgeb and C. Busch, 'Towards detection of morphed face images in electronic travel documents,' in *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*, 2018, pp. 187–192. DOI: 10.1109/DAS.2018.11.

[32] U. Scherhag, D. Budhrani, M. Gomez-Barrero and C. Busch, 'Detecting morphed face images using facial landmarks,' in *International Conference on Image and Signal Processing*, Springer, 2018, pp. 444–452.

[33] U. Scherhag, C. Rathgeb, J. Merkle and C. Busch, 'Deep face representations for differential morphing attack detection,' *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3625–3639, 2020.

[34] S. Soleymani, A. Dabouei, F. Taherkhani, J. Dawson and N. M. Nasrabadi, 'Mutual information maximization on disentangled representations for differential morph detection,' in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2021, pp. 1731–1741.

[35] S. Soleymani, B. Chaudhary, A. Dabouei, J. Dawson and N. M. Nasrabadi, 'Differential morphed face detection using deep siamese networks,' in *International Conference on Pattern Recognition*, Springer, 2021, pp. 560–572.

[36] G. Borghi, E. Pancisi, M. Ferrara and D. Maltoni, 'A double siamese framework for differential morphing attack detection,' *Sensors*, vol. 21, no. 10, p. 3466, 2021.

[37] M. Ferrara, A. Franco and D. Maltoni, 'Face demorphing,' *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008–1017, 2017.

[38] F. Peng, L.-B. Zhang and M. Long, 'Fd-gan: Face de-morphing generative adversarial network for restoring accomplice's facial image,' *IEEE Access*, vol. 7, pp. 75 122–75 131, 2019.

[39] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso and E. Cabello, 'Border control morphing attack detection with a convolutional neural network demorphing approach,' *IEEE Access*, vol. 8, pp. 92 301–92 313, 2020.

[40] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhörst, A. Braun and A. Kuijper, 'Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts,' in *German Conference on Pattern Recognition*, Springer, 2018, pp. 518–534.

[41] M. Ferrara, A. Franco and D. Maltoni, 'Face demorphing in the presence of facial appearance variations,' in *2018 26th European Signal Processing Conference (EUSIPCO)*, IEEE, 2018, pp. 2365–2369.

[42] L. Qin, F. Peng, S. Venkatesh, R. Ramachandra, M. Long and C. Busch, 'Low visual distortion and robust morphing attacks based on partial face image manipulation,' *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 1, pp. 72–88, 2020.

[43] C. Seibold, W. Samek, A. Hilsmann and P. Eisert, 'Accurate and robust neural networks for face morphing attack detection,' *Journal of Information Security and Applications*, vol. 53, p. 102 526, 2020.

[44] S. Autherith and C. Pasquini, 'Detecting morphing attacks through face geometry features,' *Journal of Imaging*, vol. 6, no. 11, p. 115, 2020.

[45] M. Ferrara, A. Franco and D. Maltoni, 'On the effects of image alterations on face recognition accuracy,' in Feb. 2016, pp. 195–222, ISBN: 978-3-319-28499-6. DOI: 10.1007/978-3-319-28501-6_9.

[46] A. Makrushin, T. Neubert and J. Dittmann, 'Automatic generation and detection of visually faultless facial morphs,' in *International conference on computer vision theory and applications*, SciTePress, vol. 7, 2017, pp. 39–50.

[47] P. J. Phillips, *Color feret database*. [Online]. Available: https://www.nist.gov/itl/iad/image-group/color-feret-database (visited on 21/11/2021).

[48] S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis and C. Busch, 'Morphed face detection based on deep color residual noise,' in *2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 2019, pp. 1–6. DOI: 10.1109/IPTA.2019.8936088.

[49] C. Seibold, A. Hilsmann and P. Eisert, 'Style your face morph and improve your face morphing attack detector,' in *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2019, pp. 1–6.

[50] L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl and C. Busch, 'Prnu variance analysis for morphed face image detection,' in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018, pp. 1–9. DOI: 10.1109/BTAS.2018.8698576.

[51] D. White, R. I. Kemp, R. Jenkins, M. Matheson and A. M. Burton, 'Passport officers' errors in face matching,' *PLOS ONE*, vol. 9, pp. 1–6, Aug. 2014. DOI: 10.1371/journal.pone.0103510. [Online]. Available: https://doi.org/10.1371/journal.pone.0103510.

[52] V. Bruce, Z. Henderson, C. Newman and A. M. Burton, 'Matching identities of familiar and unfamiliar faces caught on cctv images.,' *Journal of Experimental Psychology: Applied*, vol. 7, no. 3, p. 207, 2001.

[53] 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, pp. 1–12, Mar. 2017. DOI: 10.1371/journal.pone.0173319. [Online]. Available: https://doi.org/10.1371/journal.pone.0173319.

[54] S. R. Godage, F. Løvåsda, S. Venkatesh, K. Raja, R. Ramachandra and C. Busch, 'Analyzing human observer ability in morphing attack detection–where do we stand?' *arXiv preprint arXiv:2202.12426*, 2022.

[55] R. S. Kramer, M. O. Mireku, T. R. Flack and K. L. Ritchie, 'Face morphing attacks: Investigating detection with humans and computers,' *Cognitive research: principles and implications*, vol. 4, no. 1, pp. 1–15, 2019.

[56] M. Ferrara, A. Franco and D. Maltoni, 'On the effects of image alterations on face recognition accuracy,' in *Face Recognition Across the Imaging Spectrum*, T. Bourlai, Ed. Cham: Springer International Publishing, 2016, pp. 195–222.

[57] P. J. Phillips, A. N. Yates, Y. Hu, C. A. Hahn, E. Noyes, K. Jackson, J. G. Cavazos, G. Jeckeln, R. Ranjan, S. Sankaranarayanan, J.-C. Chen, C. D. Castillo, R. Chellappa, D. White and A. J. O'Toole, 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms,' *Proceedings of the National Academy of Sciences*, vol. 115, no. 24, pp. 6171–6176, 2018. DOI: 10.1073/pnas.1721355115. eprint: https:

//www.pnas.org/doi/pdf/10.1073/pnas.1721355115. [Online]. Available: https://www.pnas.org/doi/abs/10.1073/pnas.1721355115.

[58] A. Makrushin, D. Siegel and J. Dittmann, 'Simulation of border control in an ongoing web-based experiment for estimating morphing detection performance of humans,' in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, 2020, pp. 91–96.

[59] S. J. Nightingale, S. Agarwal and H. Farid, 'Perceptual and computational detection of face morphing,' *Journal of Vision*, vol. 21, no. 3, pp. 4–4, 2021.

[60] N. Vetrekar, R. Raghavendra, K. B. Raja, R. S. Gad and C. Busch, 'Disguise face recognition based on spectral imaging,' in *Proceedings of the 11th Indian Conference on Computer Vision, Graphics and Image Processing*, 2018, pp. 1–9.

[61] K. Dharavath, F. A. Talukdar and R. H. Laskar, 'Improving face recognition rate with image preprocessing,' *Indian Journal of Science and Technology*, vol. 7, no. 8, pp. 1170–1175, 2014.

[62] *Gimp: Gnu image manipulation program*. [Online]. Available: http://www.gimp.org/.

[63] *Gimp: Gimp animation package*. [Online]. Available: http://registry.gimp.org/node/18398.

[64] *Facevacs technology version 9.4.2, 2020*. [Online]. Available: https://www.cognitec.com/facevacs-technology.html.

[65] *Verilook cots*. [Online]. Available: http://www.neurotechnology.com/verilook.html.

[66] J. Deng, J. Guo, N. Xue and S. Zafeiriou, 'Arcface: Additive angular margin loss for deep face recognition,' in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 4690–4699.

[67] F. Boutros, N. Damer, F. Kirchbuchner and A. Kuijper, *Elasticface: Elastic margin loss for deep face recognition*, 2021. arXiv: 2109.09416 [cs.CV].

[68] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li and W. Liu, 'Cosface: Large margin cosine loss for deep face recognition,' in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 5265–5274.

[69] G. B. Huang, M. Mattar, T. Berg and E. Learned-Miller, 'Labeled faces in the wild: A database forstudying face recognition in unconstrained environments,' in *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, 2008.

[70] Frontex, *Best practice technical guidelines for automated border control (abc) systems*, 2015.

[71] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel *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)*, IEEE, 2017, pp. 1–7.

[72] M. Pietikäinen, 'Local binary patterns,' *Scholarpedia*, vol. 5, no. 3, p. 9775, 2010.

[73] B. Chaudhary, P. Aghdaie, S. Soleymani, J. Dawson and N. M. Nasrabadi, 'Differential morph face detection using discriminative wavelet sub-bands,' in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 1425–1434.

Appendix A

Additional Material

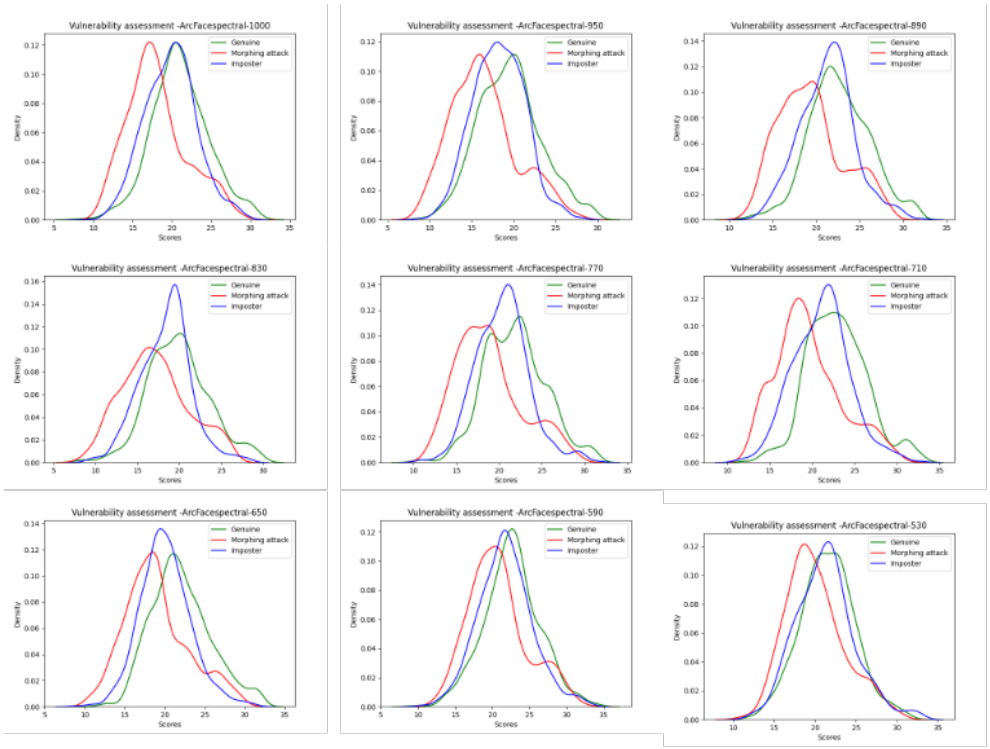


Figure A.1: A vulnerability study of ArcFace with UBO morphed images in all spectral bands

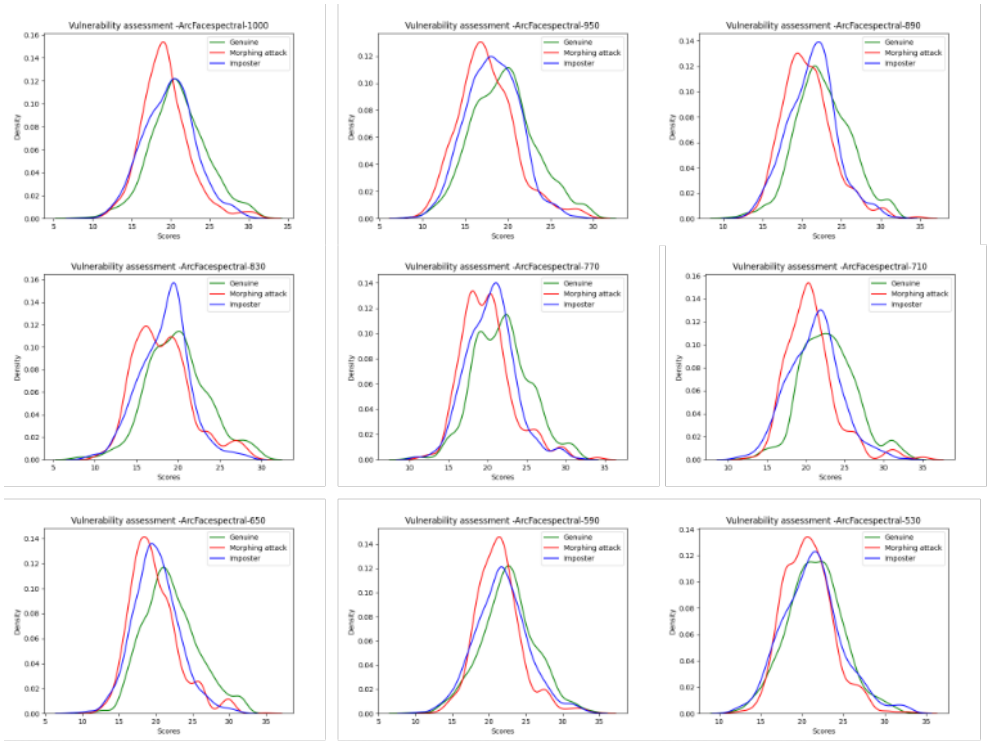


Figure A.2: A vulnerability study of ArcFace with LMA morphed images in all spectral bands

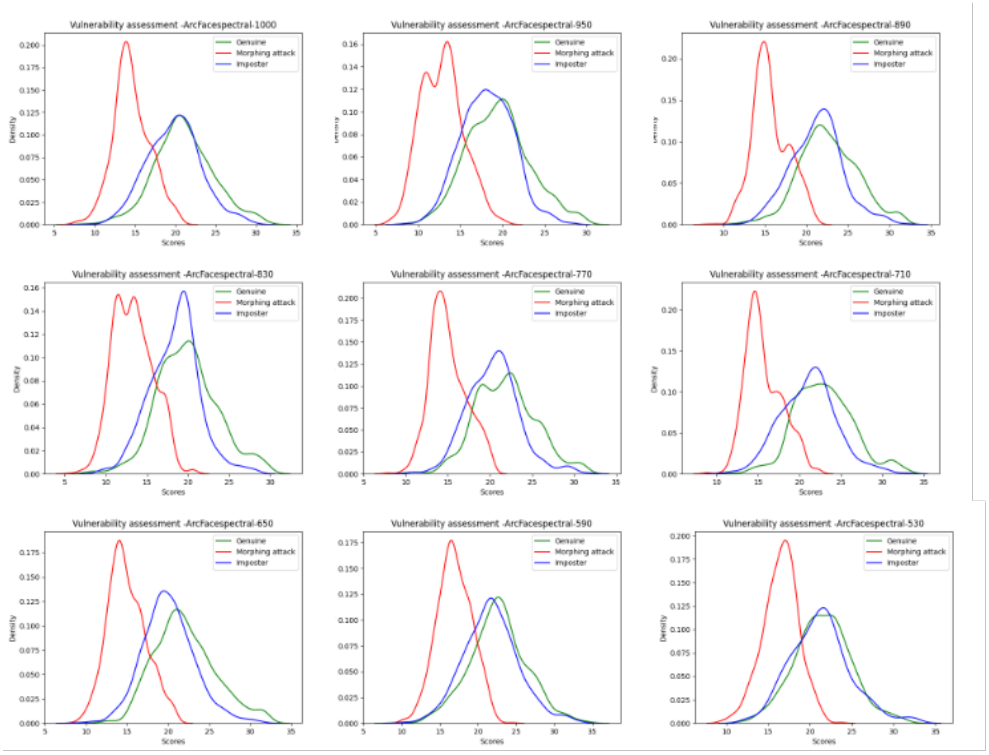


Figure A.3: A vulnerability study of ArcFace with MIPGAN-I morphed images in all spectral bands

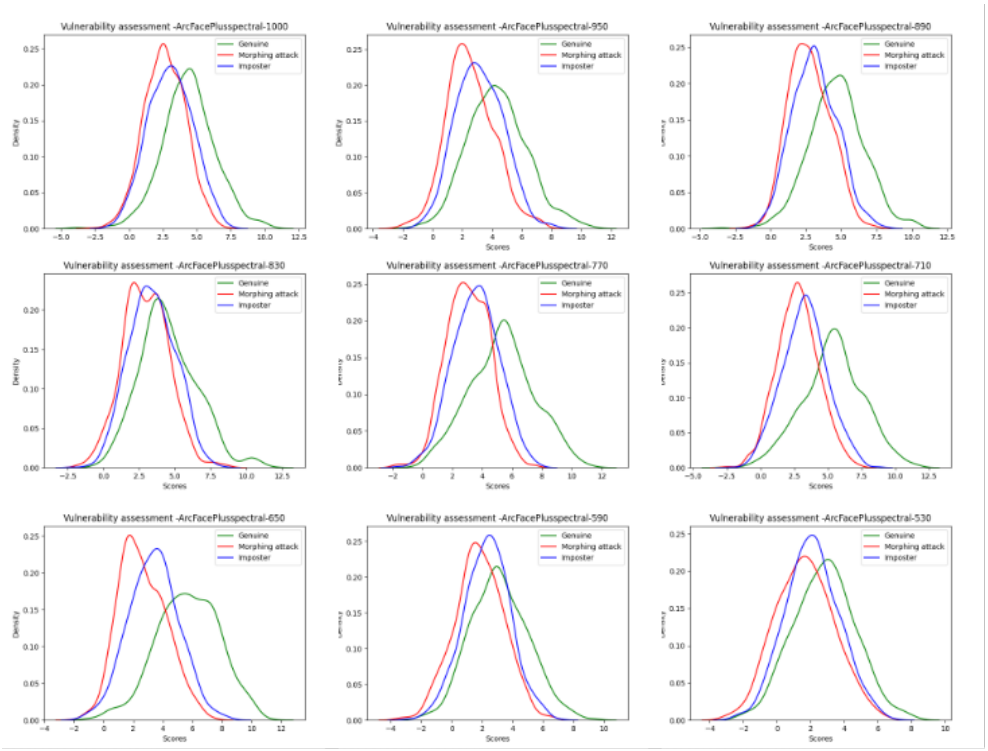


Figure A.4: A vulnerability study of ArcFacePlus with UBO morphed images in all spectral bands

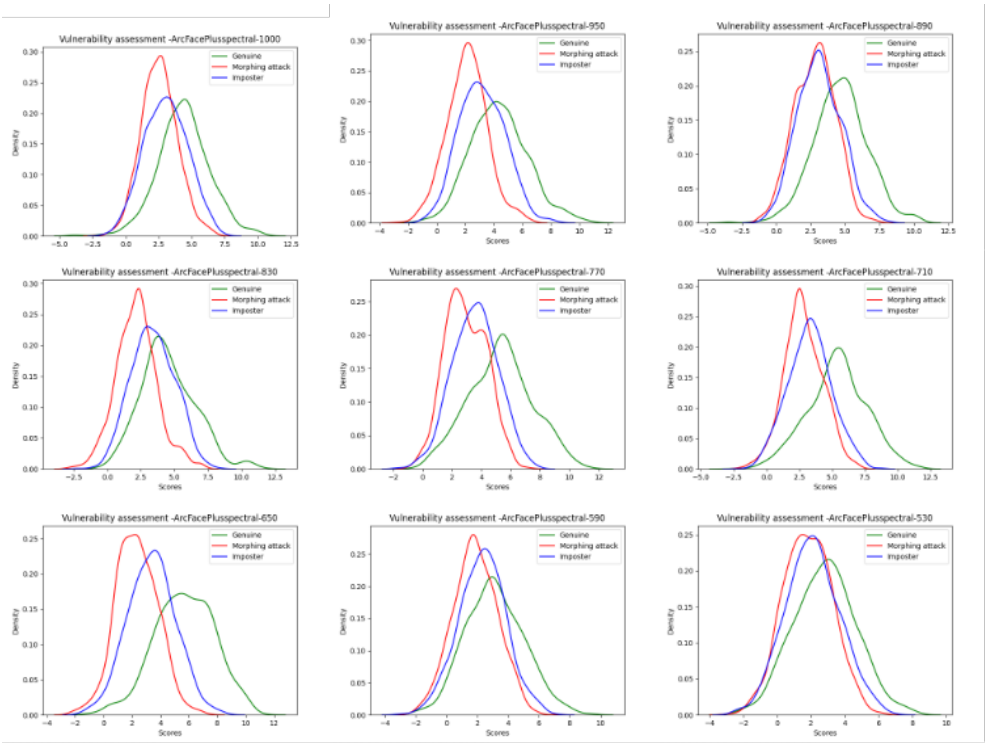


Figure A.5: A vulnerability study of ArcFacePlus with LMA morphed images in all spectral bands

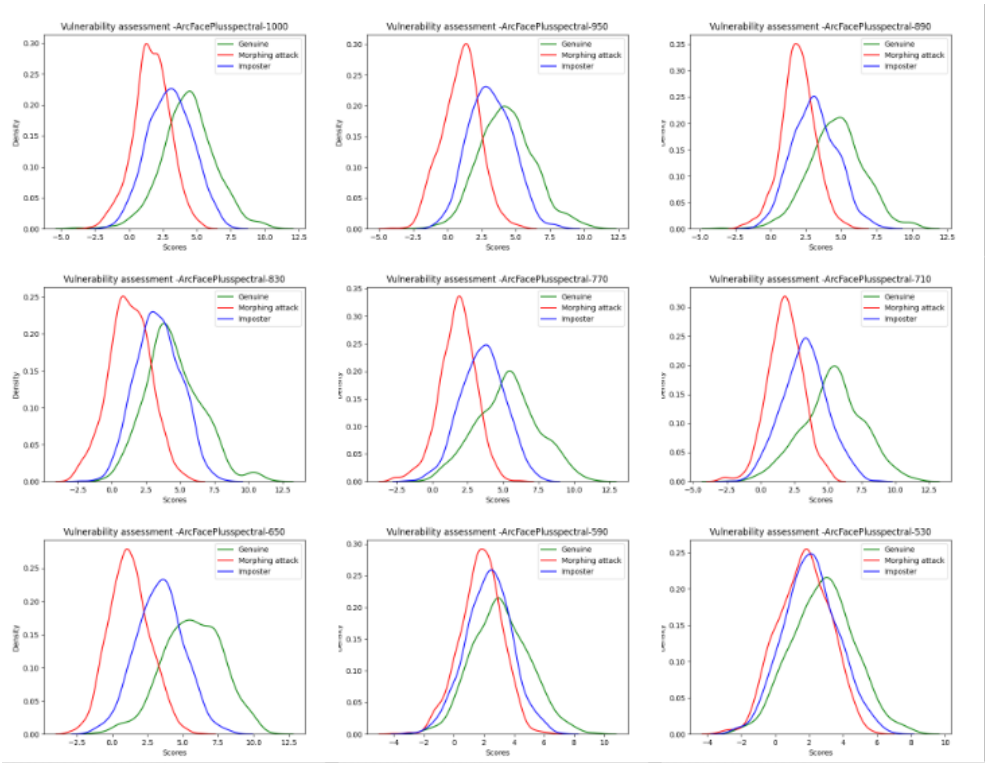


Figure A.6: A vulnerability study of ArcFacePlus with MIPGAN-I morphed images in all spectral bands

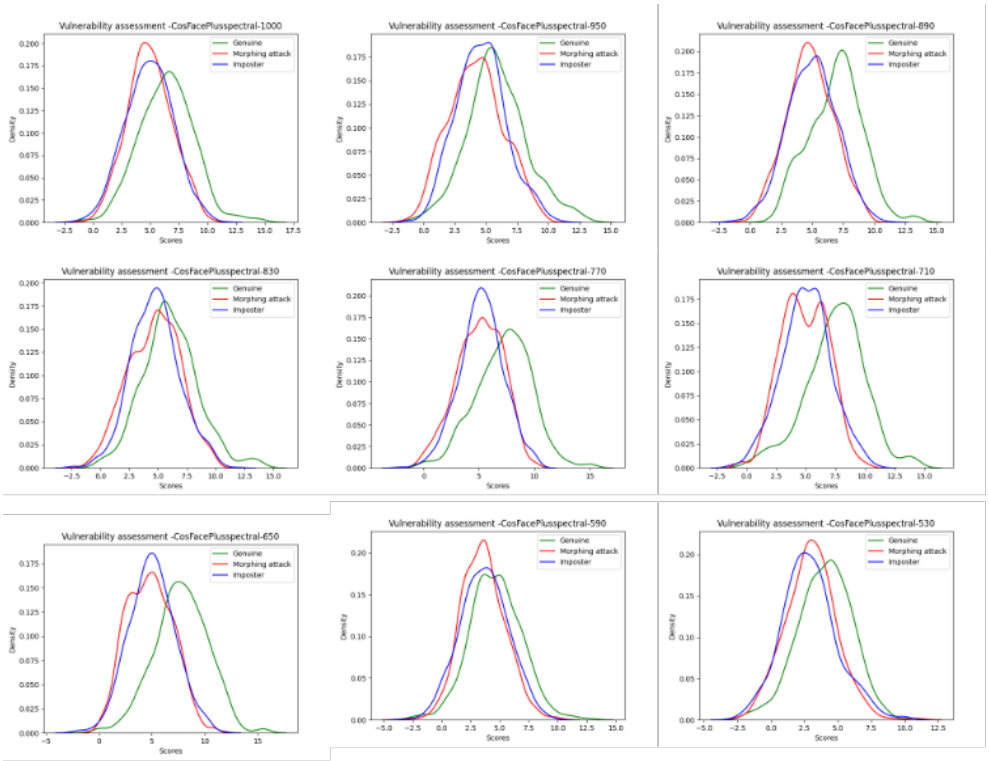


Figure A.7: A vulnerability study of CosFace with UBO morphed images in all spectral bands

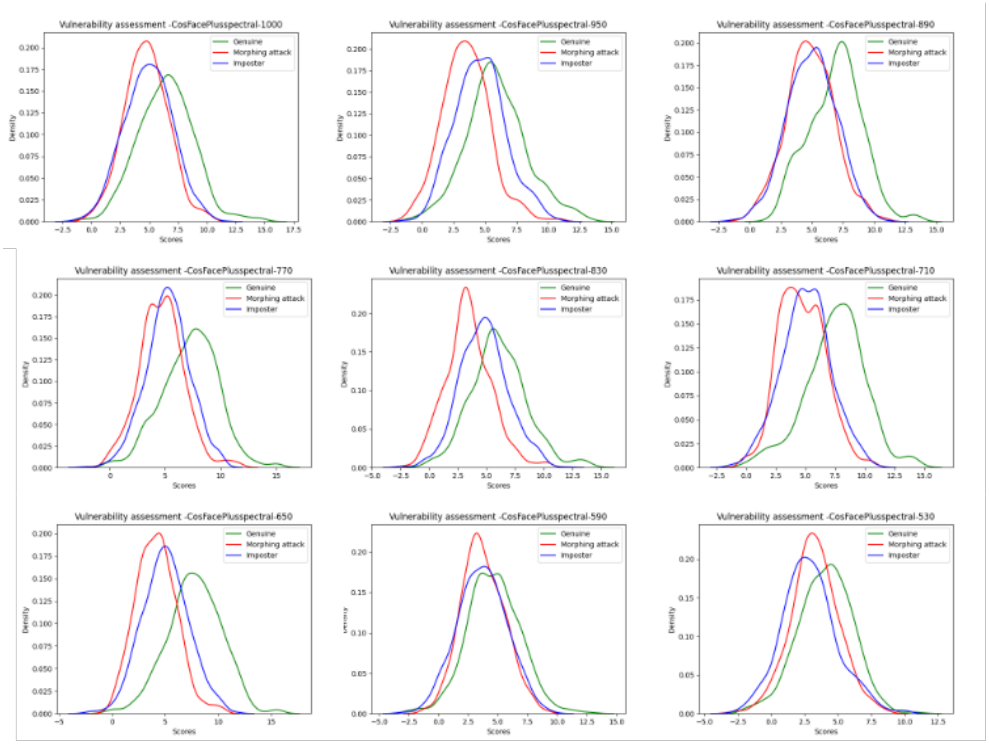


Figure A.8: A vulnerability study of CosFace with LMA morphed images in all spectral bands

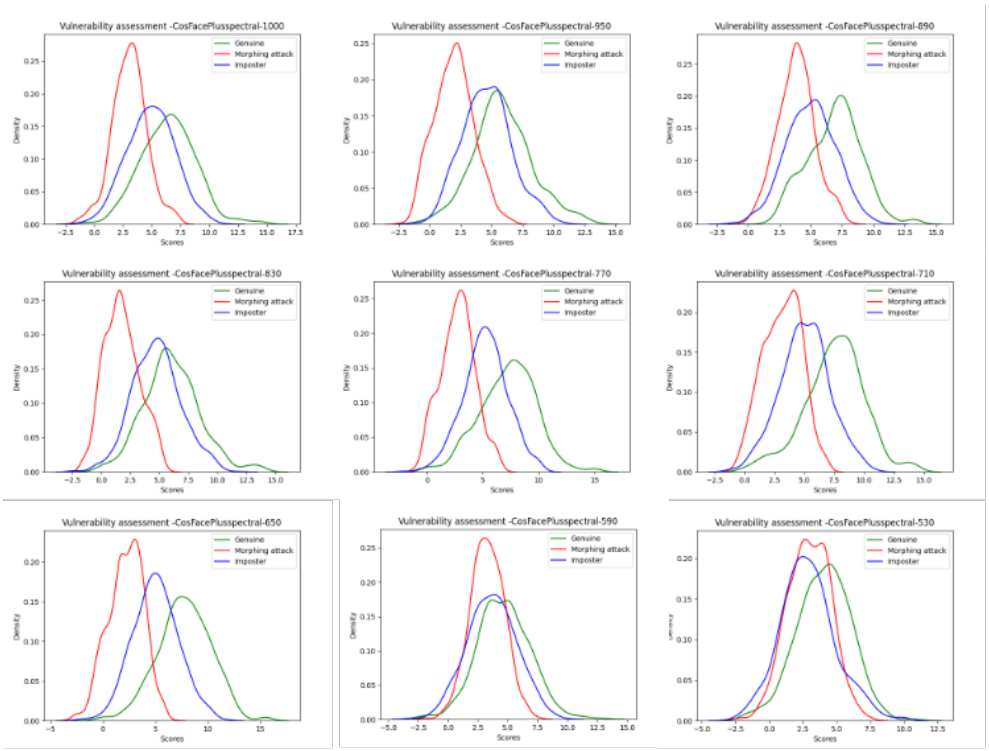


Figure A.9: A vulnerability study of CosFace with MIPGAN-I morphed images in all spectral bands

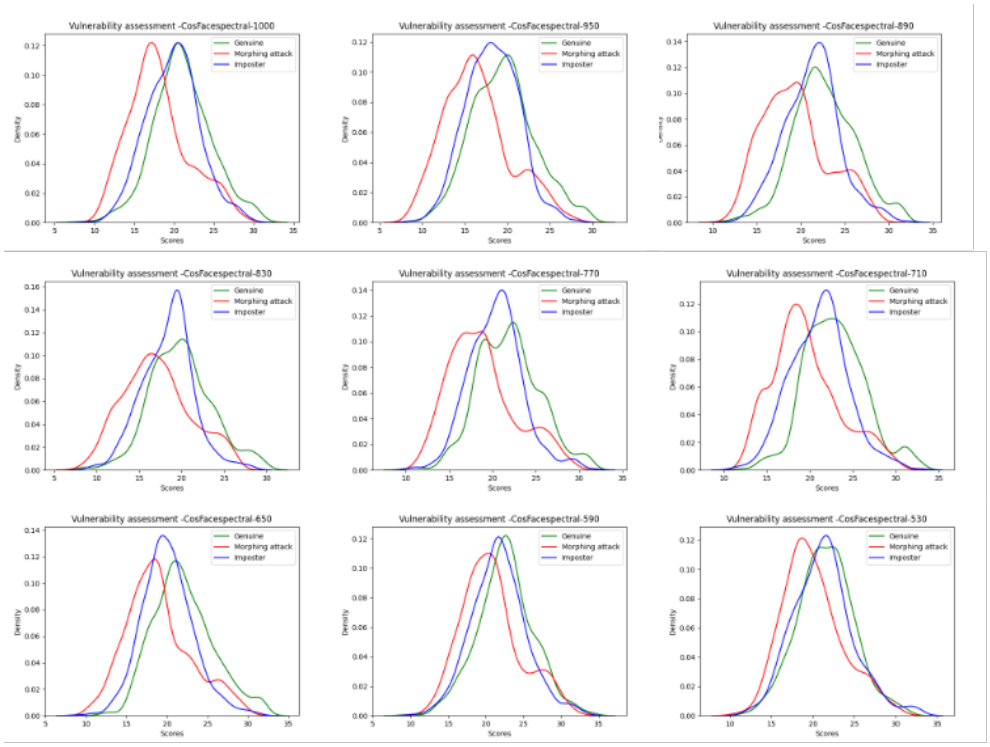


Figure A.10: A vulnerability study of CosFacePlus with UBO morphed images in all spectral bands

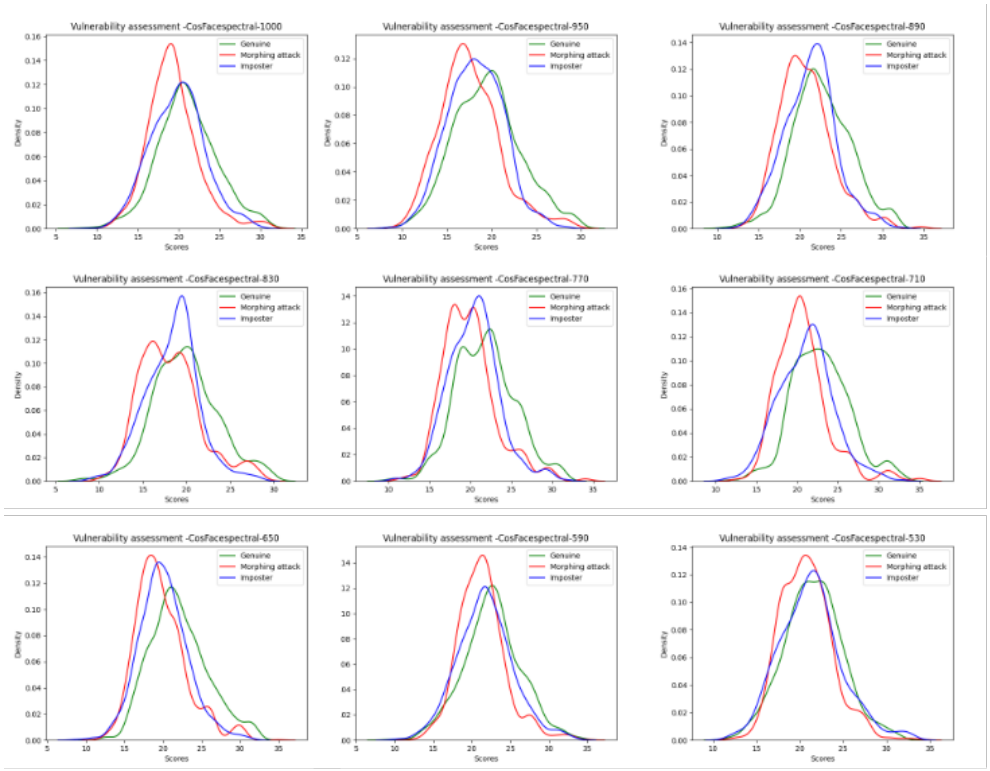


Figure A.11: A vulnerability study of CosFacePlus with LMA morphed images in all spectral bands

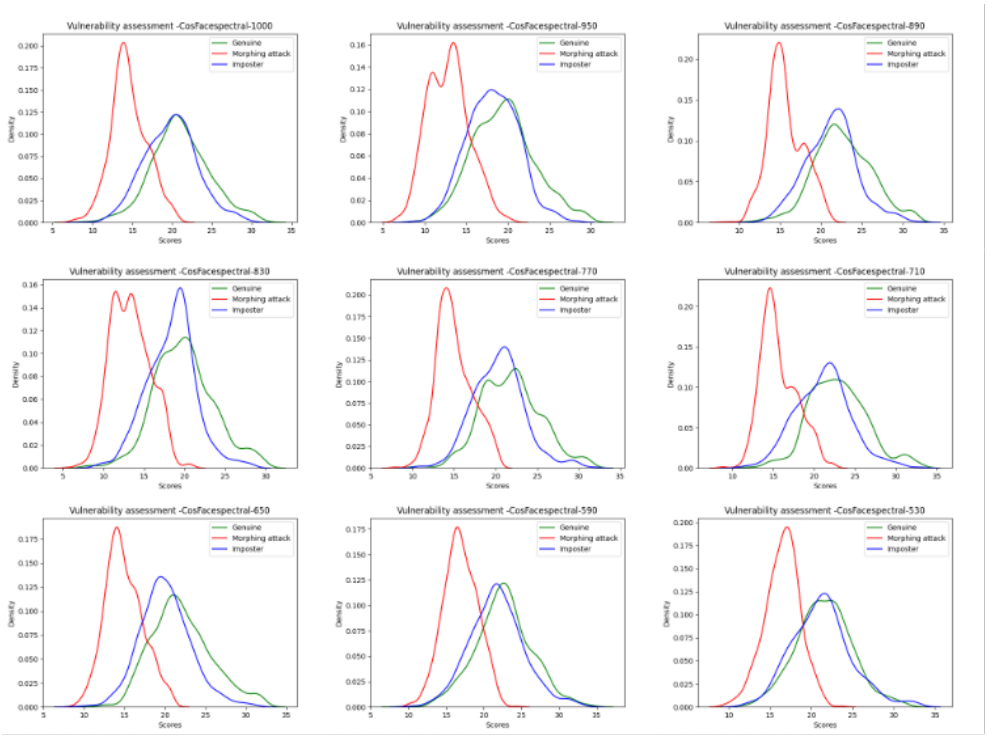
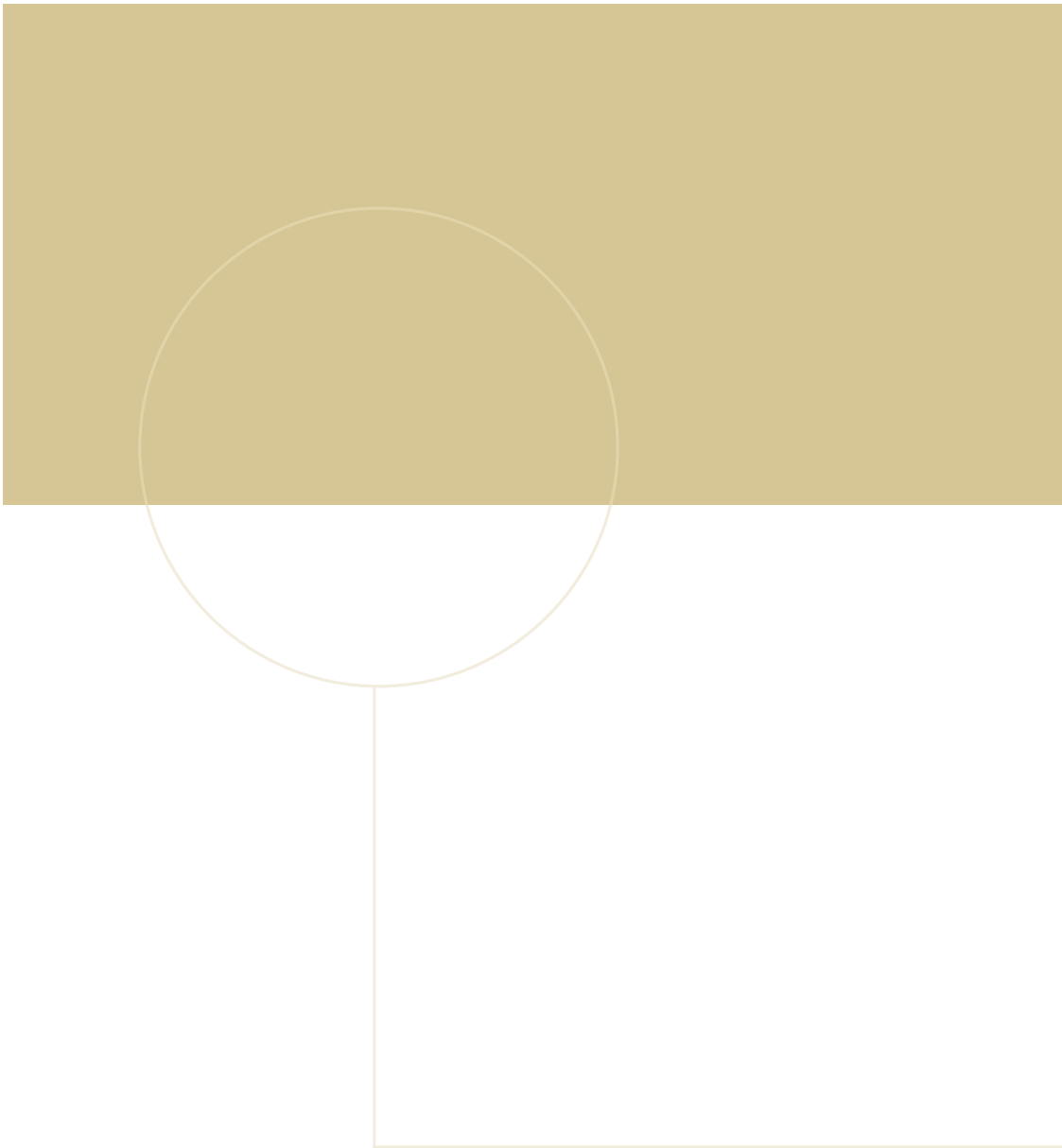


Figure A.12: A vulnerability study of CosFacePlus with MIPGAN-I morphed images in all spectral bands



NTNU

Kunnskap for en bedre verden