INTRODUCTION TO CYBERSECURITY (ECE6357)

TECHNICAL PAPER REVIEW

Morphing Attack Detection

-Database, Evaluation Platform, and Benchmarking.

Technical paper review by
Rahul Verma
PSID: 2251462, rverma6@uh.edu
Department of Electrical and Computer Engineering,
The University of Houston.

TABLE OF CONTENTS

Abstract

This study introduces a new dataset and evaluation platform for Morphing Attack Detection (MAD) algorithms, which are used to identify modified pictures in face recognition systems. The existing datasets lack diversity and do not correctly depict an actual Automated Border Control (ABC) operational condition. The new collection comprises facial photos from 150 people of various races, ages, and genders. The modified pictures are carefully created from the source photographs and treated to remove any morphing artifacts. Furthermore, the images are printed and scanned to provide MAD algorithms with a realistic challenge. The report gives a detailed examination of multiple dataset subsets and identifies the outstanding problems for future MAD research. The drawbacks of existing MAD strategies are studied, and a new secure database, evaluation platform, and benchmarking system for MAD algorithms are proposed. The SOTAMD database contains 5,748 morphing face images and 1,396 real-life face photographs of people of various ages, genders, and races. Furthermore, the study provides an unbiased and independent evaluation of five cutting-edge MAD algorithms against the SOTAMD database, as well as the development of a one-of-a-kind MAD algorithm evaluation platform. The post analyzes the limitations of current MAD procedures before outlining possible areas for future algorithm enhancement.

Keywords: *- Morphing attacks, Face Recognition Systems (FRS), Morphing Attack Detection (MAD), Automated Border Control (ABC), Visa management systems, Database, Evaluation platform, State Of The Art (SOTA) algorithms, Performance evaluation*

Introduction.

The study, "Morphing Attack Detection-Database Evaluation Platform and Benchmarking" focuses on the accuracy of Morphing Attack Detection (MAD) algorithms in detecting morphing attacks on Face Recognition Systems. Such attacks pose a substantial danger to biometric systems, particularly face recognition systems, because they combine two or more images of a person's face to create a new image that can overcome these systems. Unauthorized entry to secure facilities such as airports, government offices, and financial institutions can arise from this type of attack.

Although recent advances in MAD research, some issues remain unresolved including independent benchmarking, generalizability difficulties, and the effects of age, gender, and ethnicity. The present MAD datasets have limitations because they share the same ethnicity, morphing techniques, and post-processing procedures, and they do not provide a realistic operating environment for Automated Border Control (ABC) or allow testing MAD on unknown data.

To solve these issues, new databases for testing MAD algorithms are proposed, which utilize sequestered evidence that has been printed and scanned to eliminate all digital signs and offer a real challenge for MAD algorithms. They also provide a new online evaluation tool for testing algorithms using concealed data. This platform might be used to assess morph detection performance and investigate the generalization capabilities of MAD algorithms. The solutions proposed attempt to address outstanding issues in existing MAD research while also providing more realistic testing environments for the MAD algorithm. The selected databases will help researchers in developing more robust MAD algorithms by offering a diverse group of datasets on which to test their algorithms. Previous research has concentrated on developing a set of measures to evaluate the effectiveness of MAD practices. Other research has concentrated on evaluating the effectiveness of morphing attack detection methods. However, the absence of broad datasets for evaluating MAD algorithms often limits these evaluations.

Background of morphing attacks, and how do morphing attack detection algorithms address them?

The background part looks at the threat posed by morphing attacks on Face Recognition Systems (FRS) and the ramifications for identity management, border control, and visa management. Morphing attacks include the creation of a modified image from two or more legitimate face photographs to get around FRS and gain unauthorized entry to protected locations or systems. MAD methods detect morphing attacks in FRS by

examining the texture and characteristics of facial images. These algorithms use machine learning techniques to distinguish between legitimate and edited images and provide a score for each image. If the score is less than a particular threshold, the picture is regarded as real; otherwise, the image is considered modified. It emphasizes the limitations of current MAD mechanisms based on texture analysis and machine learning methods. These processes are ineffective and susceptible to adversarial attacks. As a result, more robust MAD algorithms that can detect morphing attacks in a variety of contexts and settings are required. It proposes a new approach to existing algorithm flaws in recognizing modified images in face recognition systems. They provide a private database, a benchmarking system, and an evaluation platform for MAD algorithms. The proposed evaluation platform is based on a fresh dataset used to evaluate the efficacy of MAD algorithms. The researcher presents a new MAD algorithm evaluation platform as well as an unbiased evaluation of five complex MAD algorithms against the new benchmark dataset.

The vulnerability of FRS systems to morphing attacks.

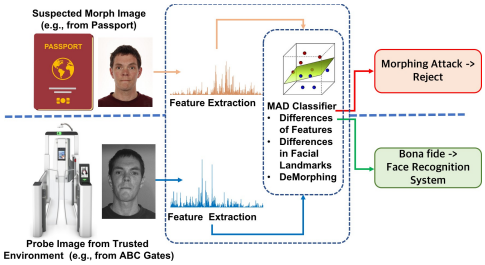
FRS systems are vulnerable to morphing attacks since they rely on facial characteristics to identify people. Because the morphed image contains facial features from multiple people, the FRS system may mistake it for a genuine image of a person even though it is not. This might confuse the FRS system and incorrect identification. Early research has looked into a variety of morphing attacks, such as FRS system defects, and MAD algorithms show potential in detecting these attacks. However, challenges must still be overcome in order for MAD research to progress. Finally, because FRS systems rely on facial features, they are vulnerable to morphing attacks, posing a significant security risk.

Work	Morphing Method	Re-digitized(R) (Print-and-Scan)	(# Morphed images)	Detection Approach	(see Section 2.3)
Ferrara et al. (2014) [1]*	GIMP GAP	D	12	-	-
Ferrara et al. (2016) [13]*	GIMP GAP	D	21	-	-
Raghavendra et al. (2016) [2]*	GIMP GAP	D	450	Texture + Classifier	S-MAD
Scherhag et al. (2017) [4]	GIMP GAP	D & R	231	Texture + Classifier	S-MAD
Raghavendra et al. (2017) [14]*	GIMP GAP	D & R	1423 (×2)	Texture + Classifier	S-MAD
Raghavendra et al.(2017) [3]*	GIMP GAP	D & R	362	Deep-CNN	S-MAD
Gomez-Barrero et al. (2017) [5]*	-	D	840	-	S-MAD
Ferrara et al. (2018) [15]	Sqirlz Morph 2.1	D & R	100	Demorphing	D-MAD
Damer et al. (2018) [7]	GAN	D	1000	GAN Based Detection	S-MAD
Raghavendra et al. (2018) [16]	GIMP-GAP	D & R	2518	Color Space Texture + Classifier	S-MAD
Scherhag et al. (2019) [11]*	OpenCV/dlib, FaceFusion and FaceMorpher	D & R	964 (×3)	PRNU + Classifier	S-MAD
Ferrara et al. (2019) [17]	Sqirlz Morph 2.1	D & R	100	Deep Neural Networks	D-MAD
Ferrara et al. (2019) [18]*	Triangulation with Dlib-landmarks	D	560 (×36)	-	-
Scherhag et al. (2020) [19]	OpenCV/dlib, FaceFusion,u FaceMorpher and UBO Morpher	D & R	791+3246 (×3)	Deep Features	D-MAD
Venkatesh et al. (2020) [20]*	StyleGAN	D	2500	-	S-MAD

State-of-the-art in morphing attack databases and vulnerability reporting

Modernity (state of the art) in Morphing Attack Detection (MAD) algorithms.

The current state of Morphing Attack Detection (MAD) algorithms says that current efforts are limited by the quantity, diversity, and quality of datasets used to train and test the algorithms. To overcome these limitations, the State-of-the-Art Morphing Detection (SOTAMD) dataset, which is a large-scale isolated collection of morphed and real face pictures collected from three different sources.



An illustration of the D-MAD pipeline

Furthermore, an independent assessment platform for MAD algorithms is being developed to promote reproducible research and benchmarking. Deep-S-MAD, a new deep learning-based MAD approach that leverages pre-trained deep networks to extract texture information and recognize morphing attacks in both the digital and re-digitized domains, is also introduced in the study. The accuracy of the current MAD algorithms is considered insufficient for operational demands, underlining the need for continued research and development to improve their accuracy and efficacy in spotting morphing attacks. Finally, the SOTAMD dataset and evaluation platform will help in the development of more robust and effective MAD mechanisms.

Different morphing attacks on Face Recognition Systems (FRS) and databases.

In more general, morphing attacks on Face Recognition Systems (FRS) and databases can be classified into two distinct types. The first kind uses digital photos for morphing assaults, whereas the second utilizes re-digitized images (also known as printed-and-scanned images) for morphing attacks.

Morphing attacks in digital pictures include the production of an image that is combined two people who bear an uncanny similarity, such as people of the same race and age. In a security-related situation, this composite image, known as a "morphed image," is utilized to authenticate two people. The morphing image must be of sufficient quality to exceed the score level provided by a Face Recognition System (FRS) in an automated face comparison system and trick a trained border guard during human examination in order to carry out the attacks or get access effectively. Several studies have been out to assess FRS's vulnerability to morphing attacks using digital images. Ferrara and peers began their investigation in 2014 by compiling a set of modified images from the AR Face Database. The investigation found that two commercial FRS, the Neurotechnology VeriLook SDK 5.4 and the Luxand SDK 4.0, were vulnerable to morphing attacks. Raghavendra and peers went even further, testing the susceptibility to such attacks on a broader range of grayscale images, including 450 morphing examples from 110 distinct individuals, using the Neurotechnology Verilook SDK. The researchers provided a method for detecting modified photos that have just been digitally manipulated. In contrast, other research has used other approaches to generate modified photos, such as face image averaging or Generative Adversarial Networks (GAN). Raghavendra and peers described face image averaging and established FRS's digital domain sensitivity to changing and averaged images. Damer and peers also utilized GAN to generate morphing pictures, trained on 1500 photos, and generated 1000 different images. The MAD process was compared to typical Landmark Aligned (LMA) morphing procedures by the researchers. They evaluated the security of the created database using two open-source face SDKs, VGG Network and Open Face.

Digital morphed face

Morphing attacks on print and scanned images may also be carried out by printing and scanning a digitally morphed image. Printing and scanning methods, which use distinct vendor equipment, result in pixel-level information loss, reducing MAD capacity. The same methods used to create morphs are employed to print and scan re-digitized images. Several studies have been performed to evaluate FRS's susceptibility to morphing attacks using print and scanned photographs. Raghavendra and peers used pixel averaging and morphing to create a print and scanned collection of 1423 changed photographs. Genuine, converted, and averaged photos were printed on 300 g/m2 high-quality photo paper with a RICOH MPC 6003 SP and scanned at 300 dpi with a RICOH MPC 6003 SP.

Image
Printer, scanned and compressed morphed face image

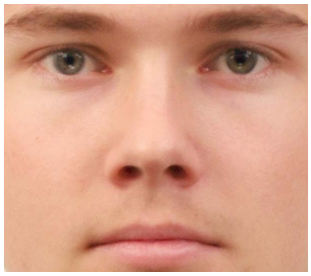
According to the study, while MAD performance decreased, COTS FRS remained as sensitive to re-digitized images as digital domain images. The same analysis was expanded to include a database of 2518 manipulated pictures. Ferrara and peers also created a printed-scanned MAD database to study the de-morphing method, in which the authors remove re-digitized pictures to detect a face-morphing attack. On a professional-quality photo printer, the altered pictures were printed and scanned at 600 dpi. Scherhag and peers used the FRGCv2 face dataset to develop a printed-scanned morphing face picture database. The printed and scanned changed

pictures were made with three distinct morphing technologies, namely OpenCV/dlib, Face Fusion, and Face Morpher, using the Epson DS-50000 Scanner at 300 dpi.

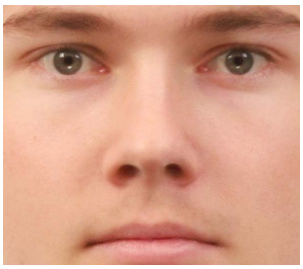
Different approaches to detecting morphing attacks.

There are several kinds of morphing attack detection methods: feature-based, texture-based, and deep learning-based.

- Feature-based techniques extract and compare certain elements of face pictures, such as eye distance or nose shape, to a reference image. These tactics are useless against morphing attacks because the morphed images may retain characteristics of both original faces, making detection difficult.
- Texture-based techniques detect morphing by evaluating the texture of facial pictures, such as pixel distribution or pattern frequency. These approaches are stronger than feature-based methods, but they need a considerable quantity of training data and are computationally costly.
- Deep learning approaches use neural networks to learn the characteristics and patterns of modified pictures. Although these systems have demonstrated promising results in identifying morphing assaults, they need a significant quantity of training data and are subject to adversarial attempts. The report acknowledges the shortcomings of the current approach and emphasizes the need for more research to build more efficient and robust ways for detecting morphing attacks.



Before



After

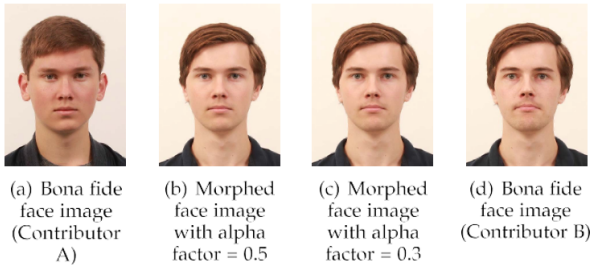
The need for more diverse and realistic databases for testing MAD algorithms on different types of morphed images.

Morphing Attack Detection (MAD) algorithms must be evaluated on a larger and more realistic database of morphed photographs. Existing MAD attempts are mostly based on internally created datasets that are limited in size, picture-collecting equipment diversity, image quality, and morphing algorithm variability. As a result, evaluating MAD algorithms and evaluating their efficacy for actual application is difficult. To overcome these shortcomings, the researchers developed the State-of-the-Art Morphing Detection (SOTAMD) dataset. The SOTAMD dataset is a large-scale isolated collection of morphed and actual photos acquired from three distinct sources, containing 5,748 modified face shots created by six different morphing algorithms. The collection contains morphing photos that have been post-processed to eliminate digital imperfections, as well as printed and scanned copies of ICAO standard passport images made using various combinations of printers and scanners, including those used in European government ID management offices. The researchers believe that the SOTAMD dataset can provide a more diversified and realistic database for MAD algorithm testing and development, as well as for generating more effective MAD algorithms for practical application.

Technical details on the proposed database of morphed images used to create the sequestered dataset.

Data collection process: The researcher collected a big collection of modified and genuine photos by visiting three distinct places and taking pictures of 150 people, 1800 times. These people were picked from a list of university personnel and students, as well as an internet casting agency. To simulate the process of obtaining a passport photo in real life, each of the 150 participants had two enrollment images taken in a high-quality studio setting. The photos were taken with a Canon EOS 5D Mark III camera and a Canon EF 85mm f/1.2L II USM lens. The photographs were saved in RAW format and then converted to JPEG using Adobe Photoshop.

Morphing methods: To morph the images, six different morphing algorithms were applied, each with a different approach. The alpha factors, or contributing factors, for each of the two faces contributing to the morphing picture were set at 0.3 and 0.5. The collection comprises both raw and fully processed image collections. Additionally, to give more realistic data, post-processed images were printed and scanned using a variety of methods, increasing the dataset's complexity.



(a) Bona fide face image (Contributor A) | (b) Morphed face image with alpha factor = 0.5 | (c) Morphed face image with alpha factor = 0.3 | (d) Bona fide face image (Contributor B)

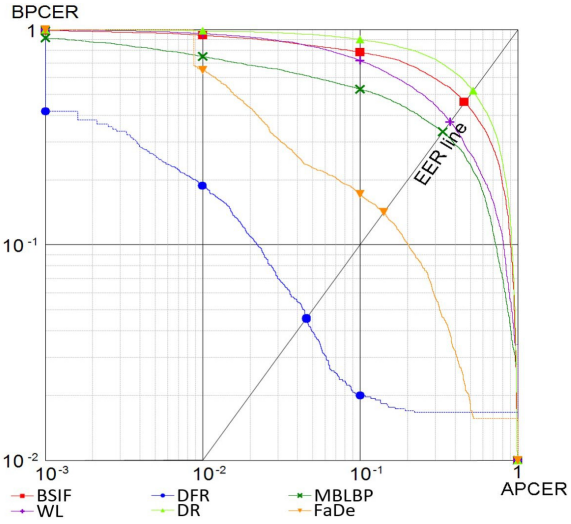
Impact of morphing factors (α) on morphing.

Print-Scan Pipeline: The researchers wanted to widen the dataset by printing and scanning each photo pair using various printer and scanner combinations, including those used in European government ID management offices. To increase the variety of the dataset, several printers and scanners were used during the print and scan procedures. The authors printed and scanned the morphed images created with three separate morphing approaches (OpenCV/dlib, FaceFusion, and FaceMorpher) using the Epson DS-50000 Scanner at 300 dpi.

Compression Techniques: The researchers compressed the photographs in the dataset using JPEG compression with a quality factor of 90, which is typically used for high-quality JPEG compression. Furthermore, the authors employed a sequestered dataset to ensure confidentiality and prevent unauthorized access to the photographs. The proposed morphing picture collection provides a diverse and realistic dataset for testing MAD algorithms, including high-quality images captured in realistic settings. The dataset has persons of various ages.

<u>Technical details on the evaluation framework for MAD and comparing their performance with other state-of-the-art algorithms.</u>

Technical details on the evaluation system used to test Morphing Attack Detection (MAD) algorithms include the framework of an independent and objective evaluation of five state-of-the-art MAD algorithms against 5,748 morphed face photographs and 1,396 actual face images. For MAD algorithms, the system delivers DET curves, Attack Presentation Classification Error Rate (APCER), and Bona Fide Presentation Classification Error Rate (BPCER) metrics. In order to encourage reproducible research, the researchers create a unique and unbiased evaluation platform that allows any researcher, government agency, or commercial enterprise to submit SDKs and analyze the effectiveness of their MAD algorithm. The site compares MAD performance to all previously submitted techniques and provides data for various age, gender, and ethnicity categories.



DET plots for the D-MAD-SOTAMD_D-1.0.

The evaluation process is completely automated and consists of participant registration, algorithm submission, performance evaluation, and results display. To preserve security and minimize external intrusions, the assessment framework is divided into two servers: the Front-End server, which houses the website and algorithm repository, and the Test Engine server, which contains the test engine and benchmark datasets.

The evaluation processes such as D-MAD and S-MAD protocols, as well as a detailed explanation of the algorithms tested on the new database and assessment platform.

The performance evaluation of Morphing Attack Detection (MAD) algorithms using a new independent evaluation platform.

The evaluation platform is designed to give a number of performance measures for MAD algorithms, including the Bona fide Presentation Classification Error Rate (BPCER) and the Attack Presentation Classification Error Rate (APCER). The BPCER is the fraction of genuine presentations identified mistakenly as morphing presentation attacks, whereas the APCER is the proportion of morphing presentation assaults classified incorrectly as genuine presentations. The platform enables an independent and objective evaluation of cutting-edge MAD algorithms on a large-scale isolated library of morphed and real face pictures. The evaluation platform evaluates a total of 500,200 trials with real (69,800) and morphed (430,400) face photographs to explain the detection performance of existing SOTA MAD approaches. MAD's accuracy does not meet the operational standards, and independent testing using manipulated photographs unbeknownst to the developers is necessary. In addition, the book underlines the importance of cross-database training and testing to improve detection algorithm robustness. Overall, the study emphasizes the importance of continuous MAD algorithm research and development to improve their accuracy and usefulness in detecting morphing attacks.

Limitations in existing MAD algorithms and the need for addressing generalization challenges in MAD research.

The limitations of existing MAD algorithms can be further divided into four main categories:

Need for cross-dataset evaluation: Because much research used in-house datasets produced using various methods, the suggested MAD methodology was confined to these specific datasets. Despite the fact that the suggested MAD techniques performed well on these in-house datasets, there has been little examination into the generalizability of their detection skills, with the exception of recent articles that seek to test the algorithms across several datasets.

Limited diversity of morphing attacks: The current MAD algorithms were developed to detect particular types of morphing attacks and may be incapable of detecting previously unknown attacks. The basic reason for this is the scarcity of morphing attacks in present datasets.

Lack of standardization: Comparing and evaluating the effectiveness of different techniques is difficult due to the lack of a standardized assessment approach for MAD algorithms.

Computational complexity: Certain MAD algorithms may need a significant amount of computer resources for training and testing, limiting their practical utility.

In order to get beyond the constraints of MAD research, the problem of generalization must be addressed. This includes developing more diversified datasets that span a wider range of evolving tactics and scenarios, standardizing assessment metrics and methods, and developing more powerful algorithms that can identify previously undiscovered sorts of assaults. Additionally, there is a need to focus on designing computationally efficient algorithms that may be employed on resource-constrained devices such as smartphones or embedded systems.

Contributions in the field of Morphing Attack Detection (MAD).

Sequestered dataset: The researchers provide a new dataset of modified pictures that may be seen publicly and used to evaluate MAD techniques. This dataset has a wide range of ages, genders, and ethnicities, and it is designed to imitate real-world events such as Automated Border Control (ABC). The dataset includes both single-image and differential-image morphing attacks, allowing researchers to test the MAD mechanism in a

variety of scenarios. The researchers offer dataset specifics such as the number of photos, the types of morphing assaults, and the distribution of ethnicity, age, and gender.

Evaluation metrics: The researchers give a number of evaluation indicators for determining the effectiveness of MAD algorithms. The false positive rate (FPR), false negative rate (FNR), detection accuracy, precision, recall, and F1 score are among the metrics. Using these measurements, researchers may analyze many aspects of the MAD algorithm's performance and compare its results to those of more complex algorithms.

Online evaluation platform: The researchers propose an online platform for evaluating MAD algorithm SDKs. Researchers can submit their SDKs and test them on the publicly accessible isolated dataset. The site analyzes the performance of the MAD algorithms against all previously submitted algorithms and presents data for various age, gender, and ethnicity groups. Researchers may use this platform to test their algorithms against a consistent dataset and standard assessment measures.

Potential areas for improvement.

One area for improvement is the creation of more diversified datasets for MAD algorithm training and testing. Existing datasets are frequently restricted to the public and lack variety in terms of race, age, gender, and morphing processes. While sequestered datasets have been proposed as a solution, more diverse datasets capable of recording a wider range of morphing processes and settings are still needed. One option, in my opinion, is to gather data in real-world situations such as airports or border crossings. This would result in a more realistic dataset that depicts the obstacles that MAD algorithms confront in real-world circumstances more precisely.

Another area for improvement is the creation of more robust MAD algorithms capable of dealing with real-world situations. While deep learning-based methods have shown promise in detecting morphed images with high accuracy, they may be susceptible to changes in lighting, pose, and image quality. Incorporating domain adaptation techniques into the training process, in my opinion, is one approach to increasing the resilience of MAD algorithms. By reacting to differences in data distribution, domain adaptation approaches can assist the algorithm in learning to generalize across domains or scenarios.

Aside from enhancing the robustness of the MAD algorithm, another potential area of improvement is the incorporation of multimodal biometric data for improved detection accuracy. The majority of MAD research today focuses on detecting altered photos solely on the basis of facial characteristics. However, MAD accuracy may be improved by incorporating other biometric modalities such as fingerprints or iris scans. This, in my opinion, may give extra information that might help in distinguishing between legitimate and fake identities, hence increasing overall detection accuracy.

Possible areas for future algorithm enhancement.

MAD research can be improved in a variety of ways in the future. One of the biggest challenges is the lack of variance in the current MAD algorithm datasets. As a result, it may be challenging to generalize and reflect a realistic operating environment for Automated Border Control (ABC). As a result, while analyzing MAD algorithms, researchers should aim on generating more varied databases that take age, gender, and ethnicity into consideration.

When evaluating MAD algorithms, another important area for future algorithm development is the addition of post-processing pipelines and different morphing techniques. This strategy can improve the generalization power and efficacy of MAD algorithms in identifying morphing attacks.

MAD algorithms that are impervious to various types of morphing attacks must also be developed. Most MAD algorithms are currently designed to identify particular morphing assaults, limiting their use in real-world circumstances where attackers may employ a variety of morphing tactics. Finally, MAD algorithms that can

detect morphing attacks in real time are critical. This is especially important for applications that need rapid and precise identification

Conclusion.

A new database with an extensive data set description, a separate evaluation platform, and a collection of State of The Art (SOTA) algorithms that have been evaluated on a sequestered dataset are all part of the proposed solution. This evaluation platform allows researchers to measure their MAD algorithm's performance and examine their generalization potential on isolated data. The database will include face photos of 150 people of various ethnicities, ages, and genders. The modified photos are carefully built from the originals before being treated to remove any morphing artifacts. The images are also printed and scanned in order to put MAD algorithms to the test. The study thoroughly investigates a number of dataset subsets as well as the performance of the MAD algorithms on the new dataset. There are still challenges in MAD research that must be addressed for future advancements, such as increasing the diversity of current databases for MAD algorithms and evaluating MAD algorithms while taking additional factors into account, such as post-processing pipelines and various morphing processes. It is critical to specifically spot morphing threats in order to keep identity management systems secure such as Automated Border Control (ABC) and visa management systems. Morphing attacks are dangerous because they can result in misidentification and impersonation. As a result, developing effective MAD algorithms capable of reliably spotting changing threats is critical. While there are still open challenges for future advancements in MAD research, the proposed approach has the potential to detect morphing attacks in FRS using MAD algorithms and improve MAD algorithm performance, which is critical for ensuring the security of identity management applications.

Acknowledgment

I would like to express my sincere gratitude to Professor Dr. Miao PAN and teaching assistants for their valuable guidance and support throughout this project. Their expertise in the field of introduction to cybersecurity has been instrumental in shaping the direction and outcomes of this technical paper review. Thank you for your unwavering commitment and dedication to our academic pursuits.

References.

1. *Raja, K., Ferrara, M., Franco, A., Spreeuwers, L., Batskos, I., De Wit, F., Gomez-Barrero, M., Scherhag, U., Fischer, D. A., Venkatesh, S., Singh, J. J., Li, G., Bergeron, L., Isadskiy, S., Raghavendra, R., Rathgeb, C., Frings, D., Seidel, U. M., Knopjes, F., . . . Busch, C. (2021). Morphing Attack Detection-Database, Evaluation Platform, and Benchmarking. IEEE Transactions on Information Forensics and Security, 21, 4336–4351.* https://doi.org/10.1109/tifs.2020.3035252
2. M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep. 2014, pp. 1–7.
3. R. Raghavendra, K. B. Raja, and C. Busch, "Detecting morphed face images," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2016, pp. 1–7.
4. R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Transferable deep-CNN features for detecting digital and print-scanned morphed face images," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 1822–1830.
5. 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 *Proc. 5th Int. Workshop Biometrics Forensics (IWBF)*, Apr. 2017, pp. 1–6.
6. M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, "Is your biometric system robust to morphing attacks?" in *Proc. 5th Int. Work- shop Biometrics Forensics (IWBF)*, Apr. 2017, pp. 1–6.