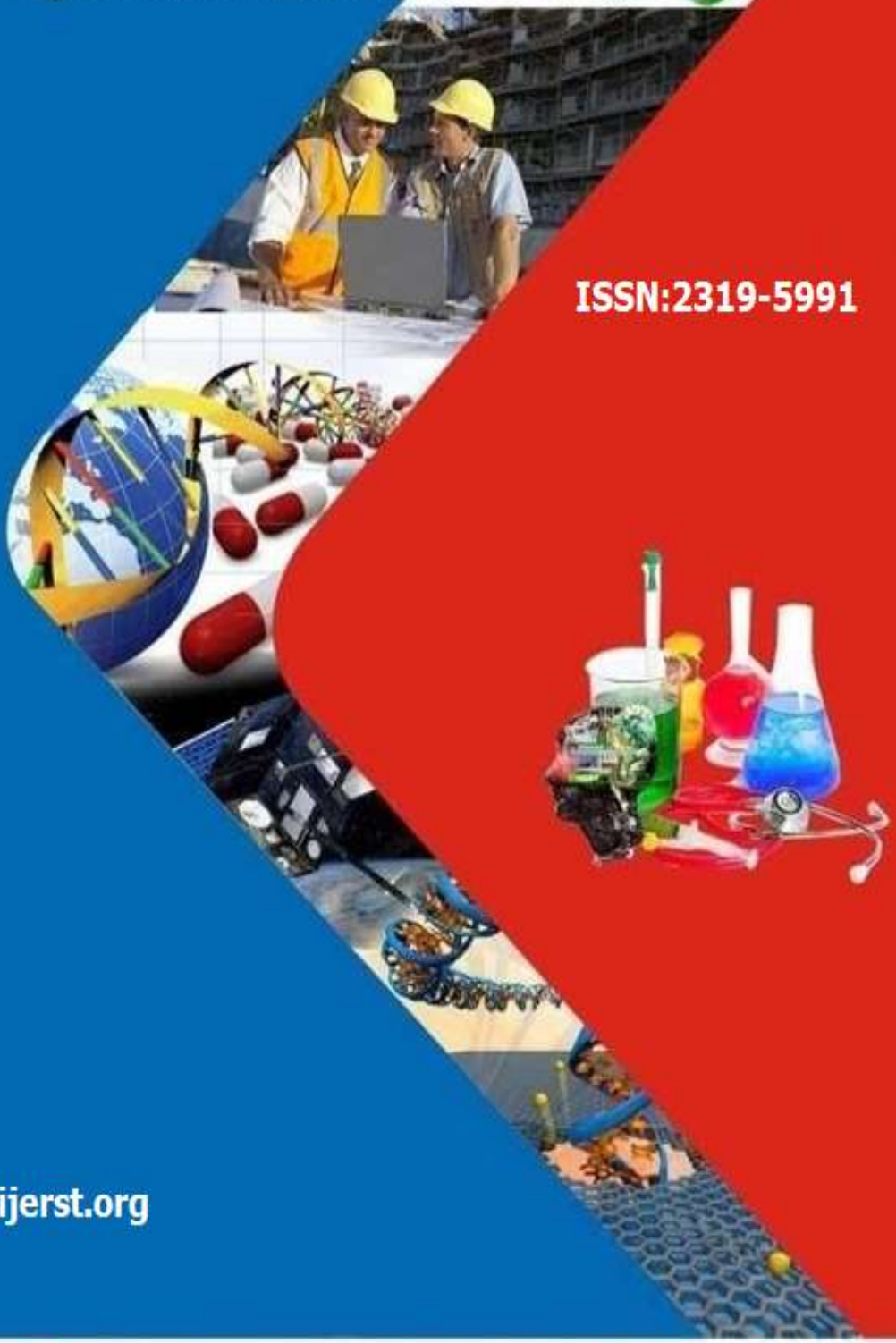
International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

GENERATION AND DETECTION OF FACT MORPHING ATTACKS

1 Mrs. M. SHARADA, 2 J. DEEPTHI SREE, 3 K. KIRTHI, 4 P. KOTIBABU

5 K. BALA VENKATA SWAMI

1Assistant Professor, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

ABSTRACT

Failure of facial recognition and authentication system may lead to several unlawful activities. The current facial recognition systems are vulnerable to different biometric attacks. This research focuses on morphing attack detection. This research proposes a robust detection mechanism that can deal with variation in age, illumination, eye and head gears. A deep learning-based feature extractor along with a classifier is adopted. Additionally, image enhancement and feature combination are proposed to augment the detection results. A versatile dataset is also developed that contains Morph-2 and Morph-3 images, created by sophisticated tools with manual intervention. Morph-3 images can give more realistic appearance and hence difficult to detect. Moreover, Morph-3 images are not considered in the literature before. Professional morphing software depicts more realistic morph attack scenario as compared to the morphs generated in the previous work from free programs and code scripts. Eight face databases are used for creation of morphs to encompass the variation. These databases are Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET and FRLL. Results are investigated using multiple experimental setups and it is concluded that the proposed methodology gives promising results.

Keywords: **Cloud Computing, Data Security**

I. INTRODUCTION

The world has become a global village with the introduction of modern technologies. Vast distances have now shrunk due to the availability of fast means of conveyance like airplanes, trains, ships and buses. These abundant conveyance options have given rise to a significant increase in the travelling population. With such a large number of mobile population, manual verification of travelling documents and facial authentication is not possible. This automatic system uses face recognition system to compare the live captured images of the traveller with the image of traveller that is stored in the travel agency‘s database system or in the form of passport or any other type of machine readable travel documents (MRTD).

After face recognition system approves that both the live captured image of the traveller and the image on the passport are same, the traveller is granted travelling authorization. In this way an automatic border control system is implemented to deal with enormous travelling population. Availability of image manipulation

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

technology has also enabled the culprits to use this technology for fraudulent activities. In order to gain legal entry permission into foreign countries for unlawful activities many criminals are utilizing a technology called face morphing to trick the face recognition system. Image morphing has been around since 1980s but now with the ease and abundance in availability of software and hardware technology to the general public, creating morphed images for fraudulent activities is easier than ever. In face morphing technology the image of two or more persons can be combined or merged together in such a way that it resembles the participants of the morphed image and the facial recognition system approves the morphed image as the original image of the applicant. By using image morphing a wanted criminal who is barred from travelling can easily morph his facial image with the facial image of an accomplice and successfully acquire travel permission in an unauthorized country.

In order to alleviate this vulnerability of the face recognition systems several methods have been proposed in the past. These methods are categorized based on their methodology of morph detection. Single image morph attack detection and differential morph detection. This study introduces a general morph attack detection model that would be able to classify a wide variety of images. Images of different types and varying features (age, expression, posture, illumination, gender, race, hair style, facial hair, head gear, eye wear) are used as different type of ID cards have different back ground colours and specifications.

II. LITERATURE SURVEY

Face morphing attack is proved to be a serious threat to the existing face recognition systems. Although a few face morphing detection methods have been put forward, the face morphing accomplice‘s facial restoration remains a challenging problem. In this paper, a face de- morphing generative adversarial network (FD-GAN) is proposed to restore the accomplice‘s facial image. It utilizes a symmetric dual network architecture and two levels of restoration losses to separate the identity feature of the morphing accomplice. By exploiting the captured facial image (containing the criminal‘s identity) from the face recognition system and the morphed image stored in the e-passport system (containing both criminal and accomplice‘s identities), the FD-GAN can effectively restore the accomplice‘s facial image. Experimental results and analysis demonstrate the effectiveness of the proposed scheme. It has great potential to be applied for tracing the identity of face morphing attack‘s accomplice in criminal investigation and judicial forensics.

One of the key challenges in face perception lies in determining how different facial attributes contribute to judgments of identity. In this study, we focus on the role of color cues. Although color appears to be a salient attribute of faces, past research has suggested that it confers little recognition advantage for identifying people. Here we report experimental results suggesting that color cues do play a role in face recognition and their contribution becomes evident when shape cues are degraded. Under such conditions, recognition performance with color images is significantly better than that with gray-scale images. Our

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

experimental results also indicate that the contribution of color may lie not so much in providing diagnostic cues to identity as in aiding low- level image-analysis processes such as segmentation. Cross-modality face recognition is an emerging topic due to the wide-spread usage of different sensors in day-to-day life applications. The development of face recognition systems relies greatly on existing databases for evaluation and obtaining training examples for data-hungry machine learning algorithms. However, currently, there is no publicly available face database that includes more than two modalities for the same subject. In this work, we introduce the Tufts Face Database that includes images acquired in various modalities: photograph images, thermal images, near infrared images, a recorded video, a computerized facial sketch, and 3D images of each volunteer's face. An Institutional Research Board protocol was obtained and images were collected from students, staff, faculty, and their family members at Tufts University. The database includes over 10,000 images from 113 individuals from more than 15 different countries, various gender identities, ages, and ethnic backgrounds. The contributions of this work are: 1) Detailed description of the content and acquisition procedure for images in the Tufts Face Database; 2) The Tufts Face Database is publicly available to researchers worldwide, which will allow assessment and creation of more robust, consistent, and adaptable recognition algorithms; 3) A comprehensive, up-to-date review on face recognition systems and face datasets.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

The matter of morph attack detection has enticed a significant amount of attention from the research community in the recent years. Different studies have been conducted in this field and different approaches have been applied to effectively detect morph attacks. Variety of face databases are utilized for creation of morph image databases as sufficient morph images are not easily available for research purposes.

Existing morph detection datasets have another very major problem. These datasets have considered the morph of two persons only (morph-2 images), leading to easy morph detection. Furthermore, low quality programming script based morphing tools like FaceMorpher, OpenCV, FaceFusion are used that generate morphed images automatically and majority of created morphed images are easily detectable through visual inspection by a human. Therefore, these techniques are rarely used by criminals, hence not depicting the real world scenarios. Methods tested on the datasets with the discussed limitations, can give very high detection rates but will not be very successful in real scenarios. Morphs of high quality and high variance are still very difficult to classify properly. Previous work has succeeded in achieving high accuracy but the results were achieved on databases having limited features.

DISADVANTAGES

The technology required to generate morphing attacks is becoming increasingly accessible, which could

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

potentially lead to more widespread misuse if the knowledge and tools fall into the wrong hands. Moreover, while detection algorithms are improving, they often struggle with achieving perfect accuracy, especially in real-time applications where the consequences of false positives or negatives can be significant. Implementing such detection systems also requires considerable computational resources and infrastructure, which can be costly and time-consuming for organizations to adopt. Furthermore, the rapid pace of technological advancement means that detection systems need continual updates and refinements, posing ongoing challenges for developers and security professionals. Overall, while the study of face morphing attacks is essential for safeguarding biometric systems, it also necessitates careful consideration of the associated risks and challenges.

PROPOSED SYSTEM

The security vulnerabilities posed by morphing techniques, which blend facial features from multiple individuals to create a single image that can deceive facial recognition systems. The system comprises two primary components: morph generation and morph detection. In the morph generation phase, advanced algorithms utilize deep learning techniques to create highly realistic morphed faces by seamlessly blending features from multiple source images. This involves leveraging Generative Adversarial Networks (GANs) to produce high-quality morphs that can bypass existing facial recognition systems. The detection phase employs a robust approach to identify morphed images. It uses machine learning models trained on a diverse dataset of authentic and morphed images to recognize subtle inconsistencies and artifacts introduced during the morphing process. The detection algorithms analyze spatial and frequency domain features, along with leveraging deep neural networks, to effectively distinguish between genuine and morphed images. Additionally, the system incorporates a continuous learning mechanism that adapts to new morphing techniques and countermeasures, ensuring its effectiveness against evolving threats. By integrating morph generation and detection, the system not only tests the resilience of facial recognition systems but also enhances their security by providing a reliable method to identify and counter morphing attacks.

IV. IMPLEMENTATION

MODULE DESCRIPTION

IMAGE MORPHING

In the late 1980s and 1990s, face image morphing was used for introducing visual effects in movies and animations. In image morphing, features of two face images were compared and spatial relationship between the features was determined for combination. After the alignment of both images through warping, color interpolation is applied to generate a new image. The new image is a mix of both input images. The varying of warping and color interpolation was referred to as transition control. Different techniques of morphing like mesh warping [8], field morphing [9] and radial basis

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

morphing have been used for creation of morphed faces. In mesh warping, meshes are used to link different landmarks or control points on the images of two subjects. The source image is morphed into the target image by freezing some parts of the image while warping others through control points. In field morphing, a pair of lines were used to map corresponding features between two images. Different points on the images were mapped based on their distance from the respective line. In radial basis functions, the features on the image were considered to be represented by a set of points. Different lines and curves that formulated a mesh on an image were considered as a set of points. Mapping was done from the two surfaces that were considered on both images.

METHODS OF MORPH ATTACT DETECTION

There are two basic types of morph attack detection (MAD) methods that are prevalent in the literature.

1. SINGLE IMAGE MAD METHOD

In these types of methods only the morphed image is analysed for presence of morphing attempt. Morphing an image leaves some artifacts in the image that are traced for detection of morph. Texture descriptors like binary statistical image features (BSIF) are utilized for texture classification. Furthermore, ghosting or shading artifacts are also detected in such images. Similarly, deep neural network can also be trained to detect such artifacts as long as the training data contain variety of images.

2. DIFFERENTIAL MAD METHOD

In these types of methods both the potential morph and the live captured images are analysed, compared and processed to detect morphing attempt, Feature vectors from both images are extracted for comparison. Demorphing process is also done in some of these techniques to extract the identity of the accomplice by subtracting the live captured image from the morphed image**.**

3. STATE OF THE ART RESEARCH WORK

Significant amount of work has been done in the field of morph attack detection. Different tools, preprocessing methods and databases are used for morph image creation. Overview of related literature work is shown in Table 1. Several research studies in the area of morph attack detection have reported good detection results but these studies are tested on the datasets with limited variations and lack real world scenarios. Features like variation in age, race, facial hair, head gear, eye wear, illumination, expression and posture are underutilized or not utilized at all in many studies. Similarly limited number of databases are utilized for morph attack detection. Furthermore, fixed contribution weights (attacker and accomplice) are used in creation of morphed images instead of random contribution weights from attacker‘s and accomplice‘s images. Images in which head gear and eye wear are present, resulted in incorrect classification of original images as morph images. The quality of live

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

captured images is very high in previous studies that is not applicable for all checkpoints due to variation of available resources.

V. RESULTS

PROTECTING CLOUD DATA

MORPHED IMAGE

FINAL RESULT

VI. CONCLUSION

In this study, a robust and generalized morph attack detection model and a very diverse morphed database is introduced to better deal with morph attacks in a practical scenario. Different feature combination techniques are analyzed and feature concatenation proved to be the best technique for morph detection. Some of the methods like feature concatenation provided better morph attack detection performance but with the increase of computational cost. Similarly, it was observed that manually created morphed images with high quality morphing tools were difficult to detect by the models that were trained on morphed databases that had low variation and were made automatically from low quality morphing tools like OpenCV and Face Morpher using programming scripts.

The training of model on manually created morphed databases with high quality tools proved to be helpful in achieving good results and the results achieved by the model on testing data improved significantly. Proposed model gives very encouraging and improved results in case of age, illumination, posture and expression variations. Testing of morphed images was also done using different machine learning based classifiers and SVM produced the best results. Different image enhancement techniques were also applied on image databases and it was observed that databases with low variation in illumination and colour benefited from image enhancement. Manually created morph-3 images were very difficult to detect when the model was only trained on morph-2 images created from low quality tools. After training the model on morph-3 images created from high quality tools, the performance of morph-3 detection increased significantly.

REFERENCES

1. 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. 75122–75131, 2019.
2. M. Ferrara, A. Franco, and D. Maltoni, __Face demorphing,“ IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 1008–1017, Apr. 2018.
3. U. Scherhag, C. Rathgeb, J. Merkle,

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

R. Breithaupt, and C. Busch, Face recognition systems under morphing attacks: A survey,‟ IEEE Access, vol. 7, pp. 23012–23026, 2019.

4. U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, Deep face representations for differential morphing attack detection,‟ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3625– 3639, 2020.
5. K. Panetta, Q. Wan, S. Agaian, S. Rajeev, S. Kamath, R. Rajendran, S. P. Rao, A. Kaszowska, H. A. Taylor, A. Samani, and X. Yuan, A comprehensive database for benchmarking imaging systems,‟ IEEE Trans. Pattern Anal. Mach. Intell., vol. 42, no. 3,pp. 509–520, Mar. 2020.
6. J. Kannala and E. Rahtu, Bsif: Binarized statistical image features,‟ in Proc. 21st Int. Conf. pattern Recognit. (ICPR2012), pp. 1363–1366, IEEE, 2012.
7. D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello, Border control morphing attack detection with a convolutional neural network de-morphing approach,‟ IEEE Access, vol. 8, pp. 92301–92313, 2020.
8. D. B. Smythe, A two-pass mesh warping algorithm for object transformation and image interpolation,‟ Rapport Technique, vol. 1030, p. 31, Mar. 1990.