International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Generation and Detection of Face Morphing Attacks

A.Sravani[1], S.Rupa Lakshmi[2], S.L.S Vaishniavi[3], V.Yasaswi Sowmya[4], B.Ramesh[5], Y Lakshmi Narayana[6]

[1]Assistent Professor, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Dr.B.R.Ambhedkar Konaseema Dt, Andhra Pradesh - 533255
[2,3,4,5,6]Student, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Dr.B.R.Ambhedkar Konaseema Dt, Andhra Pradesh - 533255

Abstract
Failure of the facial recognition and authentication system can lead to some illegal activities. Current facial recognition systems are vulnerable to various biometric attacks. The detection of attacks is the main focus of this study. This study proposes a robust detection mechanism that can cope with changes in age, lighting, eyes and capillary. We implement a deep learning-based feature extractor and classifier. In addition, image enhancement and combination of functions are provided to improve detection results. Professional morphing software describes a more realistic morph attack scenario compared to morphs created by free software and coding scripts in previous works. Eight face databases are used to create morphs to cover the variation. These databases are Celebrity2000, Extended Yale, FEI, FGNET,GT-DB, MULTI-PIE, FERET and FRLL. The results are investigated with several experimental arrangements and it is concluded that the proposed method gives promising results.

Section I: Introduction
The world has become a global village.with present day innovation. Because of the accessibility of quick method for transport, for example, planes, trains, ships and transports, significant distances have now contracted. These plentiful transportation offices incredibly expanded the quantity of travelers. Physically checking travel records and perceiving faces is absurd when there are such countless individuals moving around. As a result, passports are authenticated and validated with the help of an automated border control system. Line control frameworks are presently utilized in excess of 180 air terminals around the world. This computerised framework utilises a facial acknowledgment framework to look at ongoing pictures of the explorer with the travel planner's data set framework or with the voyager's picture put away in a visa or other kind of machine- discernible travel report (MRTD). Assuming the facial acknowledgment framework acknowledges that both the traveler's facial photograph and the photograph in the visa are something very similar, the traveler gets an authorisation to travel. Along these lines, a programmed line control framework is executed to deal with the tremendous voyaging populace. The accessibility of picture handling innovation has likewise empowered hoodlums t o i n v o l v e t h i s i n n o v a t i o n f o r misrepresentation.
To acquire legitimate section abroad for criminal operations, numerous hoodlums utilize a procedure called facial transforming to trick the facial acknowledgment framework. Picture control has been

around since the 1980s, yet presently no sweat and availability of programming and equipment innovation to people in general, it is more straightforward than at any other time to make changed pictures for misrepresentation. In the face transforming procedure, the picture of at least two individuals can be joined or consolidated to look like the members in the changed picture, and the face acknowledgment framework acknowledges the changed picture as the first picture of the candidate. Likewise, the proportion of blends of various people in the changed picture is controlled so human control is additionally extremely challenging. An illustration of shapes is shown where two separate shapes are made from two items that are like one another. With a movement boycott, a needed crook can essentially change his facial picture to that of an assistant and effectively get an authorisation to travel to an unapproved country. A few techniques have been proposed in the past to moderate this weakness in facial acknowledgment frameworks. These strategies are grouped in light of their transform identification technique. Single picture transform assault location and differential transform discovery. This review presents a general transform assault location model that can order many kinds of pictures. Various sorts of pictures are utilised and various kinds of ID cards with various elements (age, demeanour, position, lighting, orientation, race, haircut, beard growth, headgear, glasses) have different foundation tones and determinations.

Section II: EXISTING SYSTEM

Deep learning approaches have recently been used in conjunction with conventional computer vision techniques to create face morphing assault detection systems. Numerous systems use classifiers to discern between real and altered photos, and facial feature extraction techniques to capture the distinctive features of real faces. These techniques frequently encounter difficulties due to differences in age, lighting, and the use of equipment like headgear or eyeglasses.
disrupted and not rapidly reinstated, the cardiac muscle starts to deteriorate. Untreated heart attacks can lead to significant health complications and, in some cases, even mortality. Heart attacks are a prevalent cause of mortality worldwide.

PROPOSED SYSTEM

The proposed framework plans to address the impediments recognized in existing face transforming assault recognition frameworks by presenting a vigorous philosophy that upgrades precision and versatility notwithstanding developing assault procedures. Our framework use progressed profound learning methods, consolidating a best in class highlight extractor explicitly intended to catch complex subtleties inborn to certifiable countenances while staying versatile to varieties in age, lighting, and the presence of frill. To conquer the difficulties presented by proficient grade transforming instruments with manual intercession, we present an original picture improvement technique and component blend approach, enlarging the discovery capacities. The proposed framework uses a flexible dataset, including both Transform 2 and the more difficult Transform 3 pictures, which have not been broadly investigated in the current writing. This dataset is carefully organized from eight different face data sets, guaranteeing a thorough portrayal of genuine situations. Our philosophy is approved through numerous exploratory arrangements, and the outcomes show promising progressions in face transforming assault location. It is a viable option for enhancing the security of facial recognition and authentication systems due to the system' s improved generalisation capabilities, improved resistance to adversarial manipulation, and adaptability to various datasets.

FEATURE COMBINATION

In order to, the following steps are taken merge the characteristics of potentially altered photos with live acquired photographs:

1. The SSIM score and cosine distance between the corresponding live collected photos and the possible morph are computed.
2. To calculate similarity score, Cosine Distance uses the extracted feature vectors from the input photos, whereas SSIM uses the extracted input face images.
3. An average is used to integrate the SSIM scores and the cosine distance.
4. Based on the lowest combined cosine and SSIM similarity score, the features of the possible morphing picture are blended with the live acquired image.

LITERATURE SURVEY

The literature survey encompasses a range of innovative approaches and technologies aimed at addressing the complex challenges posed by face morphing attacks in various contexts. One notable contribution is the development of FD- GAN, a Face De-morphing Generative Adversarial Network designed to restore accomplice's facial images, thereby aiding in criminal investigations and judicial forensics. Additionally, advancements in understanding the role of colour cues in face recognition, as highlighted in the study on the Contribution of Colour to Face Recognition, shed light on how colour information can enhance recognition performance under certain conditions. Furthermore, the creation of comprehensive databases such as the Tufts Face Database provides researchers with valuable resources for benchmarking imaging systems and developing robust face recognition algorithms across different modalities. Techniques like deep face representations and convolutional neural networks (CNNs) demonstrate promising results in detecting morphed face attacks, emphasising the importance of robust and accurate neural network training schemes for security-related applications. These advancements collectively contribute to the ongoing efforts in enhancing face recognition systems' resilience against sophisticated attacks, ultimately aiming to ensure reliable and secure identity verification in various real- world scenarios.

PRE PROCESSING AND DATA CREATION

A. CREATION OF MORPHED DATABASE

A specialised database for morphed images has been developed. for this concentrate by following the recommendation of a famous from an interview with the researcher Andrew Ng [42]. Ng, Andrew suggested that a data- centric strategy be used to work on the exhibition of profound learning based models as the design of the models is adequately changed and improved to get the most out of the results. Thusly, in this In research, quality is prioritised above all else. database to help the model learn and perform more effectively. TABLE 3. Subtleties and elements of pictures in the transformed data set. This data set has been made physically utilising unique transforming programming. In this data set, transformed pictures are made by using the pictures from the initial eight information bases that are referenced in Table 2. Transforms made from FERET, FRGC and FRLL data sets are acquired from other exploration work and those pictures were made utilising programming calculations of OpenCV and Face Morphed. In this study, two types of morphed images are produced: 1. Transform 3, Pictures that are made by blending facial pictures of three distinct people. 2. Transform 2, Pictures that are made by blending facial pictures of two people as it were. The point by point data about the transformed information base is shown in Table 3. All out 1045 transform 3 pictures are made physically utilising software of high quality [3] FantaMorph and 269 morph-2 FotoMorph is used to create photographs. While the database FRLL was used to create 570 borrowed morph2 images, also, 1058 transform 2 pictures (acquired) were made from FERET utilising programming calculations of OpenCV and FaceMorpher. FERET and FRGC data sets were additionally utilised in the preparation and testing of model in the past work [5]. Typical pictures in the transformed data set contain the source pictures that were utilised to make transformed pictures and ordinary images include live-capturing images as well. A part of ordinary pictures is utilised as unique pictures and the second part as live images taken during testing and training. Number of live caught pictures change for various subjects. Maximum measure of live caught pictures is utilised for each dependent upon present variety in the preparation and testing to bring this concentrate as near a sensible situation as could really be expected. Different qualities and types of databases exist. includes consequently pictures from a similar information base were utilized for making transformed pictures. Every information base has been divided into sets for testing and training. Source unique pictures VOLUME 10, 2022 72561 M. Hamza et al.: Age and Discovery of Face Transforming Assaults also, made transformed pictures from those source pictures are put in their separate preparation and testing segments. Around 20% pictures from every information base are utilised for testing while 80% pictures are utilised for preparing of model. In certain data sets 20% source pictures are utilised for making of in excess of 20% transformed pictures so all things considered every one of the transformed pictures made from source pictures are put in separate test set to stay away from the presence of preparing pictures in testing set. Blending of pictures from various information bases for making transforms has not been finished as various elements like variety in light causes relics in transforms and diminishes the nature of transforms. Pictures of subjects having comparable facial construction and highlights yield improved coming about transforms, so comparative facial pictures are transformed. The definite data about the pictures utilised in preparing and testing is shown in Table 1.

TABLE 1. An overview of the related morph-related research attack detection.

TABLE 2. Details and features of images in all the source databases.

Databases	Total images	Number of subjects	Images per subject	Variation in features
Celebrity2000 [18]	163,446	2000	Variable	Age (16 – 62), illumination, expression, posture, eye wear, head gear, hair style, race, gender, facial hair.
Extended Yale B [19], [6]	16,128	28	585	64 Illumination conditions with grayscale, posture, expression, race, gender.
FEI (Faculty of industrial engineering) [20], [21]	2800	200	14	Posture, expression, illumination, eye wear, race, gender.
FGNET (Face and gesture recognition working group) [22]	1002	82	Variable	Age (0-69), illumination, colour / grayscale, expression, posture, hair style, eye wear, facial hair, gender.
GT-DB (Georgia tech face database) [6]	750	50	15	Expression, illumination, posture, eye wear, gender.
CMU MULTI-PIE (Carnegie mellon university pose, illumination and expression) [23], [24]	130,000	250	520	19 illumination conditions, gender, race, eye wear, expression, posture.
FERET (Face recognition technology) [25], [26]	14,126	1199	Variable	Colour / grayscale, illumination, expression, posture, gender, race, facial hair, hair style.
FRLL (Face research lab London) [27], [28]	204	102	2	Gender, race, facial hair, hair style.

TABLE 3. Details and features of images in the morphed database.

Source databases	Quantity of morph-3 images	Quantity of morph-2 images	Normal images
Celebrity2000	827	148	2777
Extended Yale	21	17	97
FEI	63	23	235
FGNET	34	24	150
GTDB	18	18	90
PIE	82	39	324
FERET [29]	0	1058	1058
FRLL [29]	0	570	570
FRGC [29]	0	1928	1928
Total	1045	3825	7229
Grand total	12099		

RELATED WORK

The issue of detecting morph attacks has garnered considerable interest from the scholarly community in recent years. Various studies have been undertaken in this topic, employing different methodologies to accurately identify morph attacks. Various facial databases are employed to construct

morph picture databases due to the scarcity of readily available morph photos for research purposes. Image morphing refers to the process of smoothly transforming one image into another by creating a sequence of intermediate images. During the late 1980s and 1990s, facial picture morphing was employed to include visual effects into movies and cartoons [4]. Image morphing involves co mparing the characteristics of two facial photographs and determining the spatial relationship between these characteristics in order to create a combination. Once the photos have been aligned via warping, a process called colour interpolation is used to create a new image. The new image is a combination of both input photos [7]. The manipulation of warping and colour interpolation was termed as transition control.

Various morphing techniques, such as mesh warping [8], field morphing [9], and radial basis morphing, have been employed to generate transformed faces. Mesh warping involves utilising meshes to establish connections between distinct landmarks or control points on the photographs of two subjects. The source image is transformed into the target image by immobilising certain areas of the image while distorting others using control points. Field morphing involved the utilisation of a pair of lines to establish a correspondence between corresponding features in two photographs. The photos were mapped by determining the distance of various spots from their corresponding line. Radial basis functions treat the features on the image as a collection of points. The collection of points that formed a mesh on a picture consisted of various lines and curves. The mapping process involved considering two surfaces from each photos.

Methods for detecting morph attacks There are two primary categories of morph attack detection (MAD) approaches that are commonly seen in the literature.

1. The Single Image MAD (Multiple Anomaly Detection) method.

These approaches solely analyse the transformed image to detect any effort at morphing. When a picture is morphed, it may contain artefacts that can be traced and detected to identify the morphing process. Texture descriptors, such as binary statistical image features (BSIF) [10], are employed for the purpose of texture classification. In addition, these photos also exhibit the presence of ghosting or shading anomalies. Furthermore, a deep neural network may be effectively trained to identify these artefact's, provided that the training dataset includes a diverse range of images [5].

2) Differential Mean Absolute Deviation (MAD) Method

These approaches analyse, compare, and process both the prospective morph and the live collected photos to detect any effort at morphing [5]. Feature vectors are extracted from both pictures for the purpose of comparison [1], [5], [11]–[15]. The demorphing procedure is utilised in certain techniques to extract the identity of the accomplice by subtracting the live caught image from the morphed image [1], [2], [11].

Current cutting-edge research

A substantial body of research has been conducted in the domain of morph attack detection. Various technologies, preprocessing techniques, and databases are utilised for the generation of morphed images. Table 1 presents an overview of the associated literature work.

Many research investigations in the field of morph attack detection have yielded positive detection outcomes. However, these studies have been conducted using datasets that have restricted variability and do not accurately represent real-world settings. Many studies fail to fully utilise or completely disregard features such as age, race, facial hair, head gear, eye wear, illumination, expression, and posture [1], [2], [5], [11], [12], [16]. Only a small number of databases are used for detecting morph attacks. In the generation of morphed photos, fixed contribution weights from both the attacker and accomplice are utilized instead of randomly selecting contribution weights from their respective images [5]. The presence of head gear and eye wear in photos led to the misclassification of the original images as morph images [5]. The previous studies have shown that the quality of live captured photos is

consistently good [1], [2], [5], [12], [16]. However, it is important to note that this high quality may not be relevant to all checkpoints due to variations in available resources.
Another significant issue with existing morph detection datasets is present. The datasets in question have exclusively focused on the morph of two individuals, namely morph-2 photos. As a result, the detection of morphs has been rather straightforward in these datasets, as indicated by references [1], [2], [5], [12], and [16]. In addition, the utilisation of subpar programming scripts such as FaceMorpher, OpenCV, and FaceFusion [3] for morphing purposes results in the automatic generation of morphed photos. However, a significant portion of these manufactured morphed images may be easily identified by visual examination by a human observer. Consequently, criminals seldom employ these strategies, thereby failing to accurately represent real-world situations. Although methods tested on the datasets with the discussed restrictions may yield high detection rates, they are unlikely to be effective in real-world circumstances. Classifying morphs that exhibit both high quality and high variance remains a challenging task [5].

CONCLUSION

In this review, a strong and summed up transform assault discovery model and an e x c e p t i o n a l l y d i f f e r e n t t r a n s f o r m e d information base is presented to all the more likely arrangement with transform assaults in a common sense situation. Different component blend procedures are broke down and include connection ended up being the best procedure for transform discovery. A portion of the techniques like element concatenation gave better transform assault discovery execution yet, with the increment of computational expense. Likewise, it was observed that morphed images created manually had high quality transforming instruments were hard to distinguish by the models that were prepared on transformed data sets that had low variety also, were made consequently from bad quality transforming instruments like OpenCV and FaceMorpher utilising programming scripts. The preparation of model on physically made transformed data sets with great apparatuses ended up being useful in achieving excellent results and the model's results on testing information improved fundamentally. Proposed model gives extremely reassuring and further developed brings about instance old enough, light, stance and articulation varieties. Testing of transformed pictures was additionally done utilising different machine 72574 VOLUME 10, 2022 M. Hamza et al.: Age and Discovery of Face Transforming Assaults learning based classifiers and SVM delivered the best outcomes. Additionally, a variety of image enhancement techniques were used. on picture data sets and it was seen that data sets with low variety in light and variety profited from picture enhancement. Morph-3 images created manually were extremely challenging to distinguish when the model was just prepared on transform 2 pictures made from bad quality apparatuses. In the wake of preparing the model on transform 3 pictures made from excellent instruments, the The morph-3 detection performance significantly improved. It further hardens the way to deal with incorporate assorted scope of transforms in the preparation data set to work on the power of model for morph detection. The FGNET database was found to be most challenging image database for morph detection as it very well may be found in Fig. 9 that this information base has an immense reach of variety concerning age, picture quality, variety expression and These outrageous degrees of varieties prompted the creation of morphed images that were extremely complex and challenging to group by the transform assault discovery model. Work that can be done to improve this model in the future furthermore, train it for all conceivable transform assaults in a genuine world arrangement situations will require the obtaining of genuine transformed pictures that were submitted to various organisations like air terminals, personality card giving specialists, travel offices, colleges and security foundations. The design ought to then be prepared and tried on the genuine pictures to guarantee better execution. Moreover, a versatile transform assault location model ought to be planned that naturally adjusts to the info pictures by applying the picture upgrades as per necessity. Multiple pictures may likewise be utilised for transforming.

REFERENCE

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, R. Breithaupt, and C. Busch, ''Face recognition systems under morphing attacks: A survey,'' IEEE Access, vol. 7, pp. 23012–23026, 2019.
4. A. W. Yip and P. Sinha, ''Contribution of colour to face recognition,'' Perception, vol. 31, no. 8, pp. 995–1003, 2002.
5. 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.
6. 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.
7. G. Wolberg, ''Image morphing: A survey,'' Vis. Comput., vol. 14, no. 8, pp. 360–372, 1998.
8. D. B. Smythe, ''A two-pass mesh warping algorithm for object transformation and image interpolation,'' Rapport Technique, vol. 1030, p. 31, Mar. 1990.
9. T. Beier and S. Neely, ''Feature-based image metamorphosis,'' ACM SIGGRAPH Comput. Graph., vol. 26, no. 2, pp. 35–42, Jul. 1992.
10. J. Kannala and E. Rahtu, ''Bsif: Binarized statistical image features,'' in Proc. 21st Int. Conf. pattern Recognit. (ICPR2012), pp. 1363– 1366, IEEE, 2012.
11. 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.
12. C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, ''Accurate and robust neural networks for face morphing attack detection,'' J. Inf. Secur. Appl., vol. 53, Aug. 2020, Art. no. 102526.
13. 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. 10–18.
14. S. Venkatesh, R. Ramachandra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch, ''Detecting morphed face attacks using residual noise from deep multi- scale context aggregation network,'' in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Mar. 2020, pp. 280–289.
15. 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.
16. 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 Trans. Biometrics, Behave., Identity Sci., vol. 3, no. 1, pp. 72–88, Jan. 2021.