RESEARCH ARTICLE OPEN ACCESS

Stablishing and Discovering Appearance Forming Techniques

GUPTA SOURAB,UG scholar,CSIT,Sri Indu College Of Engineering & Technology(A)
MAILA SRAVANI,UG scholar,CSIT,Sri Indu College Of Engineering & Technology(A)
ANNEDLA ABHISHEK REDDY,UG scholar,CSIT,Sri Indu College Of Engineering & Technology(A)
SAMREDDY AKSHITHAREDDY,UG scholar,CSIT,Sri Indu College Of Engineering & Technology(A)
Mrs.S.GEETHA,Asst.Prof.CSIT,Sri Indu College Of Engineering & Technology(A)

Abstract: ***Face morphing attacks are a growing concern in the digital world, with the potential to compromise personal privacy and security. In this project, we investigate the application of deep learning methods for both generating and detecting face morphing attacks. For the generation of morphed, we use a combination of convolutional neural networks and auto encoders to learn the underlying facial features and generate realistic-looking images. On the detection side, we develop a framework based on facial feature consistency analysis to differentiate distorted images from real ones. The proposed framework achieves high accuracy in detecting face morphing attacks, even in cases where the morphed images are visually similar to the genuine ones. Thisproject highlightsthepotentialof deep-learning basedapproachesforaddressingthe problem of facemorphingattacksand provides insights for further research and development in this area.***

Keywords:MorphingAttackDetection,FaceRecognition,Deep Learning,ImageMorphing,vulnerability

I. INTRODUCTION

Face morphing assaults use facial image manipulation to combine two distinct people's faces into one image. These assaults can be utilised for political influence, identity theft, and other types of fraud or deception. A variety of techniques, including picture warping, mixing, and texture creation, can be employed to create face morphs. Machine learning models and forensic analysis techniques, which commonly use counters and pixel values, can be used to detect face morphing attacks. Nevertheless, it might be difficult to spot. face morphing attacks because morphs may be made to deceive detection systems and frequently look genuine. These morphing attacks have been documented in the various fields providing threat in real world scenarios such as political campaigns, social media, and identity theft cases. It is expected that continued study and the creation of more advanced detection systems will be necessary for the effective detection and prevention of face morphing attacks.

The number of people that travel has significantly increased as a result of these numerous transportation options. Manual travel document and facial identity verification is impossible with such a huge mobility population. Therefore, the authentication and approval of passports is done by an automated border control system. There are now border control systems installed in more than 180 airports worldwide. [1].

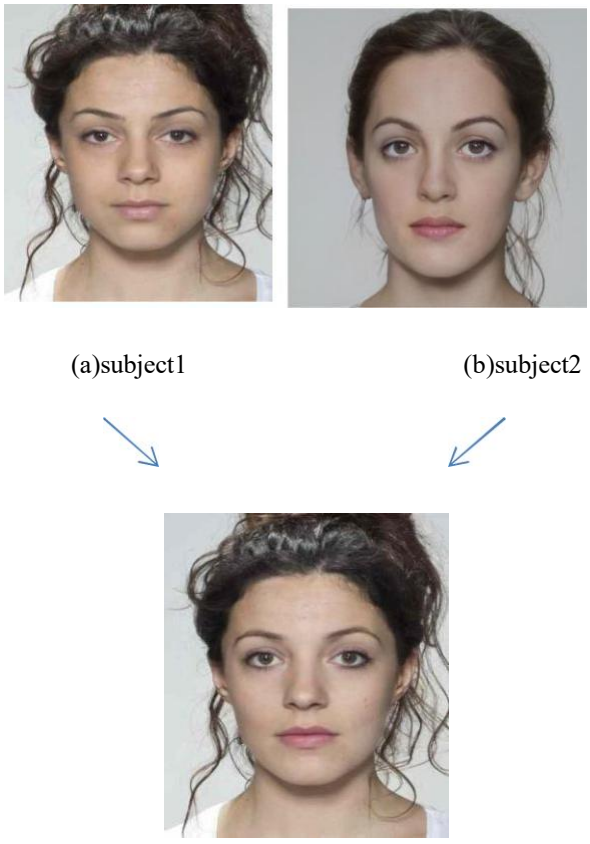
Face biometrics are frequently used in border control applications to secure people identity, where a person's identity is confirmed using either

an electronic passport or an identification card given by the government of the concerned nation. While in a few nations the face photograph for thepassportistaken under strict supervisionwithin areputableauthoritystructure.In thevastmajorityof nationsthe applicants arerequired to provide a face photograph. Therefore, the applicants may use morphing techniques to create any facial image that more closely resembles the applicant original face. [2]

Theseattackscauseafacerecognition system tomistakenlyidentifytwodistinctpeoplewith a singlefakefaceimage. Both subjects can use a piece of formal identification—such as a passport or identity card—that has such a picture encoded init to prove who is theright owner includeaprinted photofor thepaperwork when applyingfor a passport.Thismakes it possibletoinserta fakefacial image into a real official identification paper. Free morphing software makes it simple to combine two face photos into a single composite image that combines the features of both facial photographs and deceives border control biometric verification systems. Toensurethereliabilityofsuch systems, itiscrucial todetect this form offraud. Attacksthat contain morph posea seriousconcern, particularly to border security [3] Anti-spoofing methods are the focus of numerous recent research studies.

The tremendous difficulty of being recognized makes morphing attacks one of the most hazardous types of attacks. It can be performed bythe use of different morphing methods using facial images captured during morphing attacks. In anyevent, this work primaryfocus is

It was discovered that an original identity theft scenario can readily fool ABC's FRS. The fundamental idea behind these attacks is that a malicious morphed face image is an amalgam of at least two actual facial photos to look like a largenumber of different real people, suchas anaccomplice to a crime. The modified image is thenis then registered withthe FRS as anidentificationtemplate. In a successful attack,theperpetrator andanyhelper can besimilar totheimages data keptin thesystem which recognizes faces. It indicates thatadesired lawbreakerwho is notallowed to traveloutof the city canuse facialimage morphing to combine the faces of two accomplices to have a valid passport. The altered facial picture samples are displayed in Fig1[5].



(a)subject1 (b)subject2

(c)morph

Fig.1.Exampleofa morphedimagecreatedusingOpenCV

A.Objectiveofthe Project

The objective of this project is to analyse the photos to find any anomalies or artefacts that might suggest that the image has been altered is necessary to detect face morphing assaults for morph 3 images. Numerous methods, like comparing face landmarks, examining image gradients, and checking for differences in skin texture and lighting, can be used to do this. [1]

This detection method is to accurately differentiate between real facial photos and altered ones. This will improve the security of numerous systems and applications that use face recognition technology while also assisting in the prevention of various forms of fraud and identity theft. [7]

Following theintroduction of this concept, some inquiries about the commercial FRS's susceptibilityto morphing face attacks have been morphing attacks. Some face morphing detection techniques which are proposed to numerous articles mention impressive detection rates, however these findings hardly ever apply to real-world situations. Firstly, the evaluation's datasets are not realistic. Particularly, most papers do not take into account different image post-processing, such as print-scan transformation or extreme compression, that happens in real situations and may significantly reduce variation that can be seen in morphing distortions. Additionally, the numerous publications from earlier research on differential MAD make extensive use of photographs that don't accurately portray within-subject variation, including lighting, the subject's look, which may include spectacles, a beard, hair, cosmetics, ageing, and clothing, as well as facial expression.[6] [11]

II. RELATEDWORK

As morphing techniques have been the subject of numerous experimental investigations over the past few years, there has been a notable advancement and improvement in a number of areas, including visual quality and the development of altered images intended to trick the systems.[4]

Themethods which wereused in recent investigations has number of limitations. In order torecover theaccomplice's facial picture, a facede-morphing generativeadversarialnetwork (FD-GAN) is suggested in this paper. It uses two tiers ofrestoration losses and a dual network design that is symmetric to isolate the morphing accomplice's identifying feature. The analysis and outcomes of the experiments show how effective the suggested plan is. In this paper images with participants who were expressing expression, posture, or some degree of occlusion had a worse time being accurately restored. They only used morph-2 photos fewer morphing resources. [5]

The research paper presents a conceptual categorization, criteria for evaluating such strategies, and a thorough literature review of pertinent works. Along with outstanding problems and difficulties in the field, the methodology surveyed the technical issues and trade-offs are also investigated. The observed assault detection accuracyusing facial picture morphinghas not yet been generalized to datasets that include a widerange of capture situations encountered in thereal world. There are several unresolved problems and obstacles in face morphing and face morphing assault detection research, such as qualityand comparability. [9][10]

Another study looks at techniques that can detect differential morphing attacks. It is demonstrated that deep face representation- based approachesoffer incrediblyhigh detection sensitivityandrobustnessareshown tohaveextremelyhigh detection processings. Themethodologies and flaws arethen examinedin detail**.** However, excellentmorphsandmorphsthat arequitecomparabletolive- captured imagesweren't given theproper classification. Themisclassification ofphotographswasalsoaided bydifferencesin facial expression, headgear, eyewear, illumination, and focus. There was also lack of a database that accurately represents a real-world circumstance. [6]

Thede-morphingarchitectureput forth in thisresearch is tobuild on a machinelearning based convolutionalneuralnetwork (CNN) architecture. This method depends on the usage of two images: the passport photo that may have been altered and the person's current live picture in the system for Automatic Border Control. The de-morphing process aims to decode the picture. [4]

III. PROPOSEDMETHODOLOGYANDARCHITECHTURE

A. Architechture

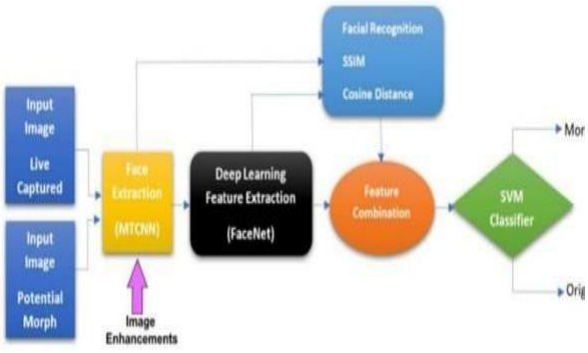


Fig2:Architecturetodetectthemorphedimages

In this method, a reliable detection method is proposed that can account for age, lighting, eye, and headgear variations. A classifier and a feature extractor based on deep learning are used. To improve the detection outcomes, image enhancement and feature combination are also suggested. In this work, a distinctive and varied morphing database is manually constructed utilising expert software. This work includes morphed photos made from twoand three topics. On the newlycreated database, the use of extraction of features with deep learning model like FaceNet and an artificial intelligence-based classifier like SVM forms the basis of a contemporary morph detection algorithm.

This study's goal is to evaluate the suggested morph attack detection model's performance on various morphed and

1) *Feature Extraction:* Extract features from the facial images, such as geometric features, texture features, or frequency domain features.
2) *Morphing Image Generation:* Generate morphing images using various techniques, such as image warping, averaging, or deep learning-based methods.
3) *TrainingofMorphingDetectionModel:*Traininga machine learningmodelto discriminate betweenrealphotosand altered images, such as a Support Vector Machine (SVM).
4) *DetectionofMorphingAttacks:*Applythetrainedmodeltodetect morphedimagesintest datasets.

B. Dataset

Attack samples developed for research databases may not be the same as attack samples from the actual world. The creation of a largenumber of attack samples, which can be done automatically, is required to provide meaningful evaluation findings. A method must be utilized to enhance the deep learning model's performance such that the model's architecture has been appropriately improved and modified to attain the best outcomes.As aresult, the primary aimof this researchis to create a database that would aid the model in learning and enhancing its performance. The FERET, FRGC, and FRLL datasets which are available were used to create morphs for the photos using the OpenCV and FaceMorpher programming tools, which were obtained from prior studies [1].There are also another methods where the criminals use different tools to create a realistic image

Inthisstudy,twodifferentkindsofalteredimagesareproduced:

1) Morph-3,imagesmadebycombiningthefacesofthreeseparatepeople.
2) Morph-2,whichsimplycombinesthefacialimagesoftwopeopletoproduceimages.

As various features like variation in lighting effects known as illumination cause artefacts in morphs and lower the quality of morphs, no attempt has been made to produce morphs by combining photos

from various databases. Comparable facial photos are modified to produce better results because they have comparable facial structure and features.

Fig3:Dataset

C. Methodology

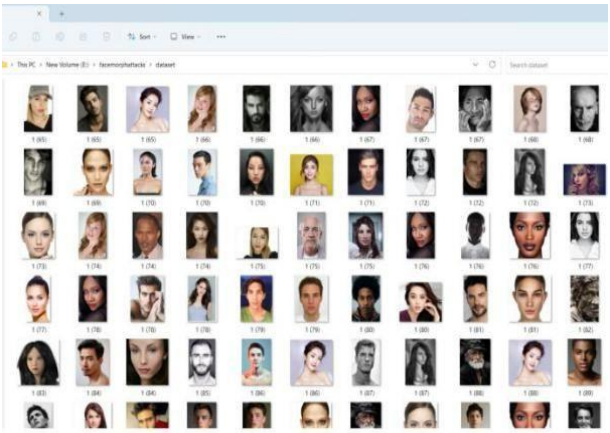
Theprojectcomestoanendinvolvingvariousstages.Theprojectcanbeperformedintwomainstageswhichincludelotof different processings. The stages can be divided as:

1) GenerationofMorphed Image
2) DetectionofMorphedImage

a) Generation

Generating a good morph with the best algorithm for morph3 involves a number of steps, including selecting appropriate images,detecting and aligning facial landmarks, morphing the images, and blending the resulting morphed image.

Select twoor threeimagesthathavesimilarfacialfeatures, suchasthesamepersonindifferentposesor with different expressions. Detect facial landmarks using a suitable facial landmark detection algorithm, such as the dlib libraryin Python.



Usethedetectedlandmarkstoalignthetwoimagessothatthefacialf eaturesareinthesamelocationandorientationinboth images.
Generate an intermediate image by morphing the two aligned images. There are several algorithms available for morphing images, such as linear blending, weighted averaging, and thin-plate splines.
Blendtheintermediateimagewiththetwooriginalimagestoprodu ceafinalmorphedimage.Therearevariousmethodsfor blending images, such as cross-dissolve, alpha blending, and Poisson blending.

Fig4:Detectinglandmarksforsubject1

Fig5:Detectinglandmarksforsubject2

b) Detection

Inthisproject, thedeeplearningtechniquesareusedtodetect themorphedimage.
Face detectionusingMTCNN:MTCNN is adeeplearning algorithmthatdetects faces inanimage.Inthis stage, the images are given as the input one which is the live captured image and other the potential morph.
Thefacialregionoftheinputimageisextractedusingthisapproach. MTCNNiscapableofdetectingfacesatdifferentscales, orientations, and positions in an image, which makes it a useful tool for various face-related applications.

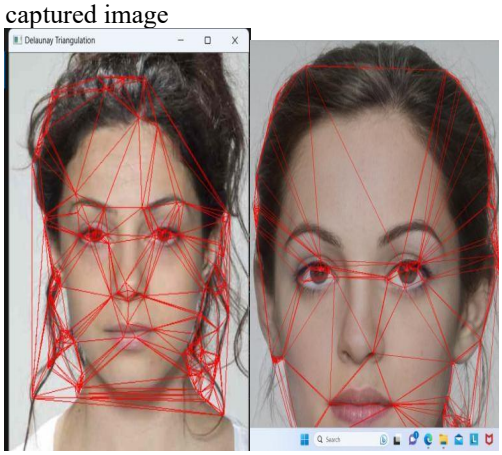


Fig6:FormationofDelaunaytrianglesusingdetectedfeatures

Face representation using FaceNet: FaceNet is a deep learning algorithm that generates a high-dimensional feature vector that representstheface. In this stage, thealgorithmis used toextract a featurevector from thefaceregion detected in theprevious stage. The facial recognition component is also incorporated to identifythe individual in the face image. This can help in identifying any anomalies in the feature vector that may be caused by morphing.

Morphing detection using featurecombination: In this stage, thefeaturevectors generated byFaceNet arecombined with additional parameters such as SSIM, PSNR and cosine distance to improve the accuracy of morphing detection. The cosine distance measures the separation between two feature vectors, whereas the SSIM measures the similaritybetween two images. Byincorporating these parameters, the algorithm can better distinguish between morphed and non-morphed faces.

Through theuse of various parameters, such as concatenation, addition, or subtraction, thelive-captured input image's attributes are combined with the potential morph image. SSIM and cosine distance verification from the facial acknowledgement system afterwards, the features of the prospective morph and the corresponding live acquired image are integrated. Between theconceivable morph photos and the collected corresponding live-captured images, the cosine distance and SSIM score are computed. Cosine distance uses the generated feature vectors derived from the source photos, as opposed to SSIM, which uses the retrieved uploading face images formeasurement of similarity. PSNR scores are also calculated to understand the changes in accuracy metrics of detection. An average is used to integrate the cosine distance and SSIM scores. Using the lowest SSIM similarity score and cosine combination, the live image is merged with the characteristics of a potential altered image. [1]

Classification using SVM: Finally, theSVM is trained on thecombined featurevector to classifythegiven inputs. After classifying the input images, it produces the output as either morphed or a valid image which thepassport of the user valid.

IV. RESULTS

Fig7:Webuser Interfacefor Detection

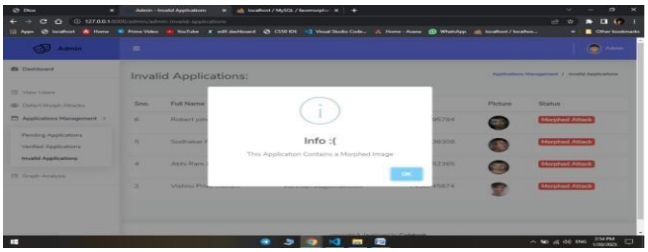
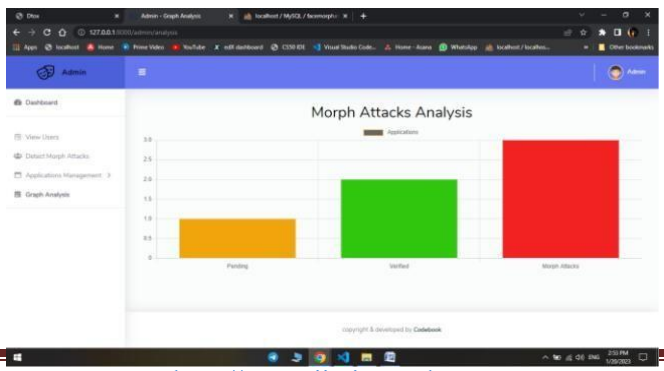


Fig8:MorphedAttackDetection



CONCLUSION

It can be concluded that, we explored different techniques for generating and detecting face morphing attacks. The generation process involved the use of deep learning models to morph two or more faces to create a single image, while the detection process focused on identifying the inconsistencies in the facial features of a morphed image compared to genuine images.

The project demonstrated the potential of deep learning-based approaches for both generating and detecting face morphing attacks. The performance of morph-3 identification dramaticallyimproved once the morph 3 photos produced using superior tools are used for training. Additionally, we investigated the effectiveness of other machine learning based classifiers, and the best outcomes are produced by SVM. Following an analysis of various feature combining strategies, feature concatenation emerged as the most effective method for morph identification. In terms of age and lighting, the proposed model provides better results. [1]

FUTURESCOP

Face morphing attacks are becoming increasingly common with the proliferation of social media and online identity verification systems. As such, there is a need for effective methods to detect and prevent such attacks. This project can be extended to explore more advanced techniques for generating and detecting face morphing attacks, such as the use of generative adversarial networks (GANs) or the integration of facial recognition technologies. The project can also be extended to develop practical solutions and tools to protectagainst face morphing attacks in real-world scenarios.

REFERENCES

[1] MuhammadHamza,SamabiaTehsin,HanenKaramti,"Generationand DetectionFaceMorphingAttacks"IEEEAccessVolume10,2022

[2] ChristophBusch,"SingleImageFaceMorphingAttackDetectionUsing EnsembleofFeatures",IEEEXplore,2020

[3] C. Seibold, W. Samek,A. Hilsmann, and P. Eisert, ''Accurate and robustneuralnetworks forface morphing attackdetection,'' J. Inf.Secur.Appl.,vol. 53,Aug. 2020, Art. no. 102526.

[4] D.Ortega-Delcampo,C.Conde,D.Palacios-Alonso,andE.Cabello,''Bordercontrolmorphingattackdetectionwithaconvolutionalneuralnetworkde-morphing approach,'' IEEE Access, vol. 8, pp. 92301–92313, 2020.

[5] F.Peng,L.-B.Zhang,and M.Long,''FD-GAN:Face de-morphing generativeadversarial network for restoringaccomplice's facialimage,'' IEEE Access, vol.7, pp. 75122–75131, 2019.

[6] U.Scherhag,C.Rathgeb,J.Merkle,andC.Busch,''Deep facerepresentations fordifferential morphingattack detection,''IEEETrans.Inf.ForensicsSecurity,vol. 15, pp. 3625–3639, 2020.

[7] G.Wolberg,''Imagemorphing:Asurvey,''Vis.Comput.,vol.14,no.8,pp.360–372,1998.

[8] D.B.Smythe,''Atwo-passmeshwarpingalgorithmforobjecttransformationandimageinterpolation,''RapportTechnique,vol.1030,p.31,Mar.1990.

[9] M.Ferrara,A.Franco,andD.Maltoni,''Facedemorphing,''IEEETrans. Inf.ForensicsSecurity,vol.13,no.4,pp.1008–1017,Apr.2018.

[10] U.Scherhag,C.Rathgeb, J.Merkle, R. Breithaupt,and C. Busch, ''Facerecognitionsystems undermorphingattacks:A survey,'' IEEEAccess,vol. 7,pp.23012–23026,2019.

[11] A.W.YipandP.Sinha,''Contributionofcolortofacerecognition,''Perception,vol.31,no.8,pp.995–1003,2002.

[12] R.Raghavendra,K.B.Raja,andC.Busch,''Detectingmorphedfaceimages,''inProc.IEEE8thInt.Conf.BiometricsTheory,Appl.Syst.(BTAS),Sep.2016, pp. 1–7.

[13] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, ''Transferable deep-CNN features for detecting digital and print-scanned morphed face images,'' inProc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jul. 2017, pp. 10–18.

[14] "DetectionofFaceMorphingAttacksbyDeepLearning",Conference: DigitalForensicsandWatermarking:16thInternationalWorkshop,IWDW2017,Lecture Notes in Computer ScienceVolume: 10431,DOI: 10.1007/978-3-319-64185-0_9