GENERATION AND DETECTION OF FACE MORPHING ATTACKS

Mr.S.Vamshi Krushna[1], Voluru Saranya[2], Kotha Sneha[3], N Ajay Kumar Reddy[4] and Bukya Rajkumar[5]

[1]*Assistant Professor, Department of CSE(DS), Samskruti College Of Engineering And Technology, Kondapur (V), Ghatkesar (M), Medchal (D), Hyderabad, India.*

[2,3,4,5]*Student, Department of CSE(DS), Samskruti College Of Engineering And Technology, Kondapur (V), Ghatkesar (M), Medchal (D), Hyderabad, India.*

Corresponding email ID: csevamshi@samskruti.ac.in

To Cite this Article

Mr.S.Vamshi Krushna, Voluru Saranya, Kotha Sneha, N Ajay Kumar Reddy, Bukya Rajkumar, "Generation And Detection Of Face Morphing Attacks", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 10, October 2025,pp: 54-68, DOI: http://doi.org/10.64771/jsetms.2025.v02.i10.pp54-68

Submitted: 20-09-2025 *Accepted: 24-10-2025* *Published: 31-10-2025*

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: Morph-2 and Morph-3 images, Celebrity2000, Extended Yale, FEI, FGNET, GT-DB, MULTI-PIE, FERET and FRLL.

1 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. Therefore, an automatic border control system is used for authentication and approval of passports. Border control systems are now deployed in more than 180 airports around the world. This automatic system uses face recognition system to compare the live captured images of the traveler 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 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 availabilityof 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 away 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. Furthermore, the ratio of merger of different persons in the morphed image is controlled in such a way that human inspection is also extremely difficult. Example of morphed images is shown in which two separate morphed images are created from two subjects that are resembling both subjects. 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, hairstyle, facial hair, head gear, eyewear) are used as different type of ID cards have different back ground colours and specifications.

2 LITERATURESURVEY

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 morphingaccomplice'sfacial restoration remains achallengingproblem. 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 separatetheidentity featureofthemorphing accomplice. By exploiting the captured facial image from the face recognition system and the morphed image stored in thee-pass port 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 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.

The vulnerability of facial recognition systems to face morphing attacks is well known. Many different approaches for morphing attack detection (MAD) have been proposed in the scientific literature. However, the MAD algorithms proposed so far have mostly been trained and tested on datasets whose distributions of image characteristics are either very limited or rather unrealistic (e.g.,noprint-scantransformation). As a consequence, these methods easily overfit on certain image types and the results presented cannot be expected to apply to real-world scenarios. For example, the results of the latest NIST FRVT MORPH show that the majority of submitted MAD algorithms lacks robustness and performance when considering unseen and challenging datasets. In this work, subsets of the FERET and FRGCv2 faced at a base are used to create a realistic database for training and testing of MAD algorithms, containing a large number of ICAO compliant bona fide facial images, corresponding unconstrained probe images, and morphed images created with four different face morphingtools. Furthermore, multiple post-processings are applied on the reference images,e.g., print-scan and JPEG2000 compression. On this database, previously proposed differential morphing algorithms are evaluated and compared. In addition, the application of deep face representations for differential MAD algorithms is investigated. It is shown that algorithms based on deep face representations can achieve very high detection performance (less than 3% D-EER) and robustness with respect to various post-processing. Finally, the limitations of the developed methods are analyzed.

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 data bases for evaluation and obtaining training examples for data-hungry machine learning algorithms. However, currently, the reisnopublicly available face database that includes more than two modalities for the same subject. In this work, we introduce the Tufts Face Data base 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 Data base 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.

3 System Analyses

3.1 Existing System

The matter of morph attack detection has enticed 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, Face Fusion 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. Several approaches with different benchmarks are proposed in the literature. Previous work has succeeded in achieving high accuracy but the results were achieved on databases having limited features.

Thetechnologyrequiredtogeneratemorphingattacksisbecomingincreasinglyaccessible,which could 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.

3.2 PROPOSEDSYSTEM

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

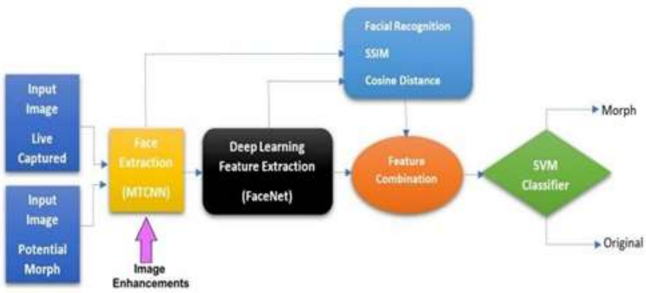
 ISSN: 3049-0952
www.jsetms.com

systemcomprisestwoprimarycomponents:morphgenerationandmorphdetection.Inthemorph 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 identifymorphedimages.Itusesmachinelearningmodelstrainedonadiversedatasetofauthentic and morphed images to recognize subtle inconsistencies and artifacts introduced during the morphingprocess.Thedetectionalgorithmsanalyzespatialandfrequencydomainfeatures,along with leveraging deep neural networks, to effectively distinguish between genuine and morphed images.Additionally,thesystemincorporatesacontinuouslearningmechanismthatadaptstonew morphingtechniquesandcountermeasures,ensuringitseffectivenessagainstevolvingthreats.By integrating morph generation and detection, the system not only tests the resilience of facial recognitionsystemsbutalsoenhancestheirsecuritybyprovidingareliablemethodtoidentifyand counter morphing attacks.

Thepositivesideisresearchinthisareaiscriticalforenhancingthesecurityofbiometricsystems. Morphing attacks, which involve blending two or more facial images to create a new, realistic image, pose a threat to systems that rely on facial recognition, such as passport controls and smartphone unlocks. By understanding how these attacks are generated, researchers can develop morerobustdetectionmechanisms,ultimatelyleadingtoimprovedsecurityprotocolsandreducing the risk of unauthorized access. Additionally, this research drives technological innovation, encouraging the development of advanced algorithms that can differentiate between genuine and morphed images with high accuracy.

4 SYSTEMDESIGN

SYSTEMARCHITECTURE



A. IMAGEMORPHING

Visual effects in movies and animations were enhanced with face image morphing in the late 80s and 1990s. In order to combine two facial photographs, image morphing first compared their features and then found the spatial link between them. Color interpolation is used to generate a new image once the two photos have been aligned through warping. Input photos and the resulting image are combined. As a transition control, the warping and color interpolation were varied. The construction of transformed faces has been accomplished using several morphing techniques, such as mesh warping, field morphing, and radial basis morphing. Mesh warping involves connecting various points on two subjects' images, such as landmarks or control points, using meshes. By freezing some sections of the image and bending others using control points, the original image can be transformed into the desired image. A pair of lines were utilized in fieldmorphing to map related features between two photos. Distance from each line used as the basis for mapping various spots on the photos. The visual features were thought of as being represented by a set of points in radial basis functions. The image's different lines and curves were treated as a collection of points. The two surfaces that were taken into account on both photos were used for the mapping process.

B. METHODSOFMORPHATTACKDETECTION

Therearetwobasictypesofmorphattackdetection(MAD)methodsthatareprevalentintheliterature.

1) SINGLEIMAGEMADMETHOD

These techniques merely look for evidence of a morphing attempt in the altered image. When you morph an image, you leave behind artifacts that can be used to detect morphs. When it comes to classifying textures, tools like binary statistical image features (BSIF) come in handy. In addition, some photos also show signs of shading artifacts or ghosting. Similarly, provided the training data contains a variety of images, deep neural networks can likewise be trained to detect such artifacts.

2) DIFFERENTIALMAD METHOD

Inthesetypesofmethodsboththepotentialmorphandthelivecapturedimagesareanalysed,compared and processed to detect morphing attempt ,Feature vectors from both images are extracted for comparison .Demorphing process is also donein someofthesetechniquesto extract the identity ofthe accomplice by subtracting the live captured image from the morphed image.

C. STATEOFTHEARTRESEARCH WORK

Morph attack detection has been the subject of a great deal of research. The generation of morph images makes use of many tools, preprocessing methods, and databases. While there have been some promising studies on the topic of morph attack detection, they have all relied on datasets with very few mutations and have not included any real-world examples. Numerous studies fail to make use of or fail to adequately account for characteristics such as age, race, facial hair, head gear, eye wear, illumination, expression, and posture. Similarly, morph attack detection only makes use of a small number of databases. In addition, rather than using random contribution weights from the attacker's and accomplice's photos, fixed contribution weights are utilized while creating morphed images. Misclassification of original photos as morph images occurred in photographs that had headgear and eyewear. Previous studies have shown that the quality of live-captured photos is very high. However, this may not be applicable to all checkpoints because the resources available can vary.

4.2 UML DIAGRAM'S:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

TheUnifiedModelingLanguageisastandardlanguageforspecifying,Visualization,Constructing anddocumentingtheartifactsofsoftwaresystem,aswellasforbusinessmodelingandothernon- software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software developmentprocess.TheUMLusesmostlygraphicalnotationstoexpressthedesignofsoftware projects.

5 IMPLEMENTATION

```
# ============================================
# MORPH DETECTION USING FACENET + SVM
# ============================================

# Import libraries
import cv2
import numpy as np
from mtcnn import MTCNN
from keras_facenet import FaceNet
from sklearn.svm import SVC
from sklearn.metrics.pairwise import cosine_similarity
from skimage.metrics import structural_similarity as ssim

# --------------------------------------------
```

ISSN: 3049-0952
www.jsetms.com

```
# STEP 1: INITIALIZE MODELS
# ----------------------------------------------
detector = MTCNN()             # Face extraction
embedder = FaceNet()           # Feature extraction (FaceNet)
svm_model = SVC(kernel='linear', probability=True)  # Classifier

# ----------------------------------------------
# STEP 2: FACE EXTRACTION FUNCTION
# ----------------------------------------------
def extract_face(image):
    detections = detector.detect_faces(image)
    if len(detections) == 0:
        return None
    x, y, w, h = detections[0]['box']
    face = image[y:y+h, x:x+w]
    face = cv2.resize(face, (160, 160))
    return face

# ----------------------------------------------
# STEP 3: FEATURE EXTRACTION USING FACENET
# ----------------------------------------------
def get_embedding(face_pixels):
    face_pixels = face_pixels.astype('float32')
    mean, std = face_pixels.mean(), face_pixels.std()
    face_pixels = (face_pixels - mean) / std
    samples = np.expand_dims(face_pixels, axis=0)
    embedding = embedder.embeddings(samples)
    return embedding[0]

# ----------------------------------------------
# STEP 4: FEATURE COMBINATION
# ----------------------------------------------
def combine_features(embedding1, embedding2, image1, image2):
    # Cosine similarity
    cosine_sim = cosine_similarity([embedding1], [embedding2])[0][0]

    # Structural Similarity Index (SSIM)
    image1_gray = cv2.cvtColor(image1, cv2.COLOR_BGR2GRAY)
    image2_gray = cv2.cvtColor(image2, cv2.COLOR_BGR2GRAY)
    image1_gray = cv2.resize(image1_gray, (160, 160))
    image2_gray = cv2.resize(image2_gray, (160, 160))
    ssim_val = ssim(image1_gray, image2_gray)

    # Combine into feature vector
    combined_feature = np.array([cosine_sim, ssim_val])
    return combined_feature

# ----------------------------------------------
```

```
# STEP 5: TRAINING FUNCTION (For Demonstration)
# ----------------------------------------------
def train_svm(features, labels):
    svm_model.fit(features, labels)
    print("□ SVM model trained successfully!")

# ----------------------------------------------
# STEP 6: MORPH DETECTION FUNCTION
# ----------------------------------------------
def detect_morph(image1_path, image2_path):
    # Load images
    img1 = cv2.imread(image1_path)
    img2 = cv2.imread(image2_path)

    # Face extraction
    face1 = extract_face(img1)
    face2 = extract_face(img2)
    if face1 is None or face2 is None:
        print("□ Face not detected in one or both images.")
        return

    # Feature extraction
    emb1 = get_embedding(face1)
    emb2 = get_embedding(face2)

    # Feature combination
    combined_feature = combine_features(emb1, emb2, face1, face2).reshape(1, -1)

    # Classification
    prediction = svm_model.predict(combined_feature)
    if prediction[0] == 1:
        print("□ Morph Detected!")
    else:
        print("□ Original Image Pair.")

# ----------------------------------------------
# EXAMPLE USAGE
# ----------------------------------------------
# Suppose 1 = morph, 0 = original
# Example training data (synthetic for demonstration)
features = np.array([[0.8, 0.75], [0.6, 0.9], [0.3, 0.2], [0.4, 0.3]])
labels = np.array([1, 1, 0, 0])
# Train SVM
train_svm(features, labels)

# Test on a new pair
detect_morph("live_image.jpg", "potential_morph.jpg")
```

ISSN: 3049-0952
www.jsetms.com

6 RESULTS/DISCUSSION

Thepurposeoftestingistodiscovererrors.Testingistheprocessoftryingtodiscovereveryconceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub- assemblies, assemblies and/orafinishedproduct It is theprocess ofexercising softwarewith theintent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.2 TESTCASES

Testcase1forLoginform:

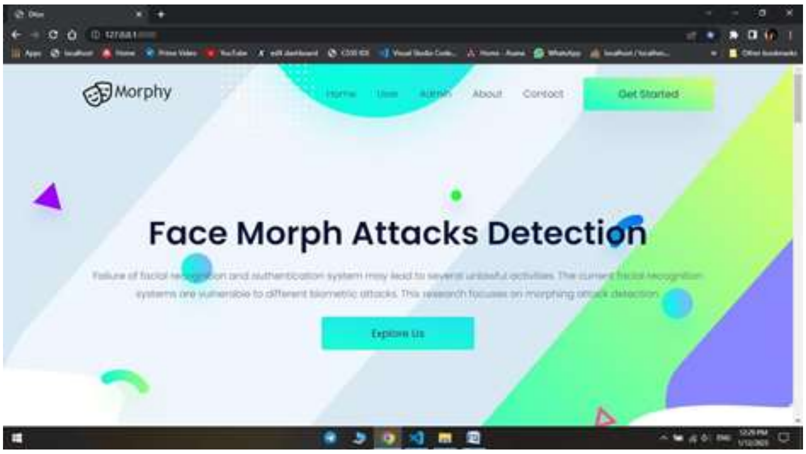
FUNCTION:	**LOGIN**
EXPECTEDRESULTS:	ShouldValidatetheuserandcheckhis existence in database
ACTUALRESULTS:	Validatetheuserandcheckingtheuseragainst the database
LOWPRIORITY	**No**
HIGHPRIORITY	**Yes**

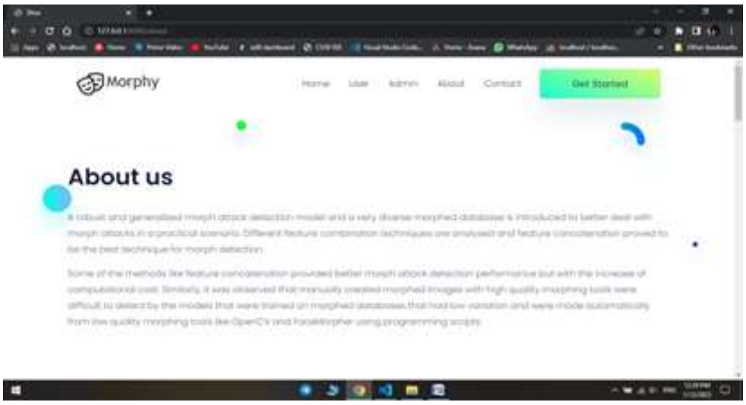
Testcase2:

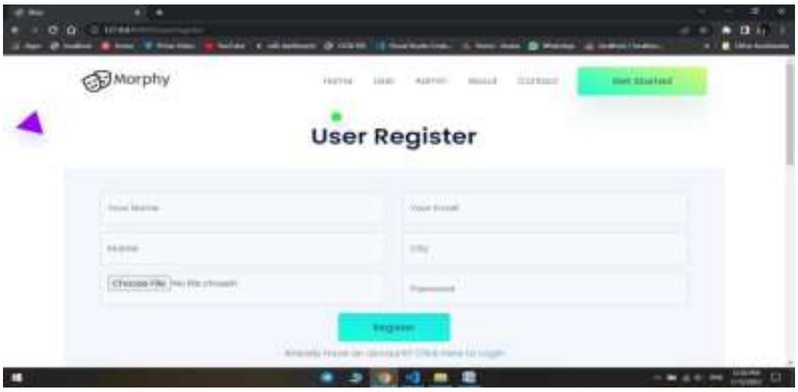
TestcaseforUserRegistration form:

FUNCTION	USERREGISTRATION
EXPECTEDRESULTS:	Should checkifall the fieldsarefilledby the userand savingthe userto database.
ACTUALRESULTS:	Checking whether all the fields are filled by userornotthroughvalidationsandsavinguser.
LOWPRIORITY	No
HIGHPRIORITY	Yes

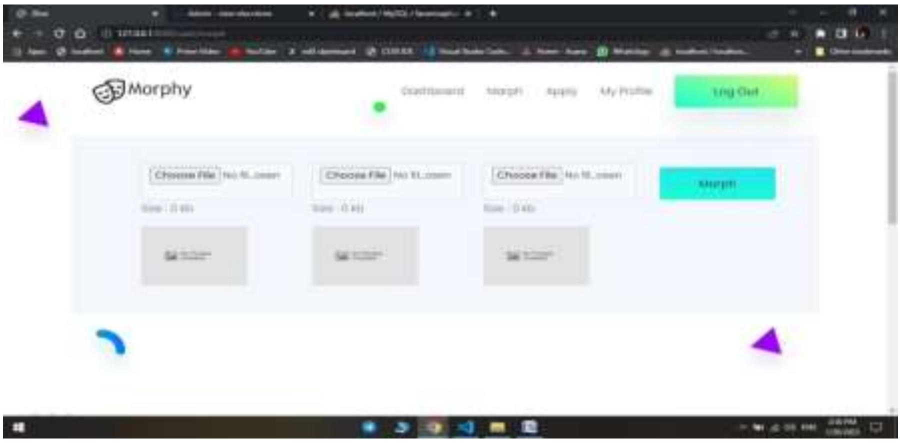
6.3 SCREENSHOTS



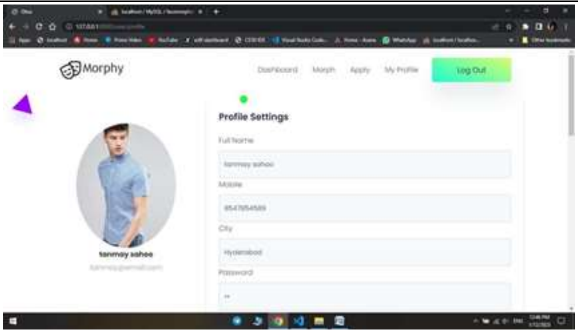


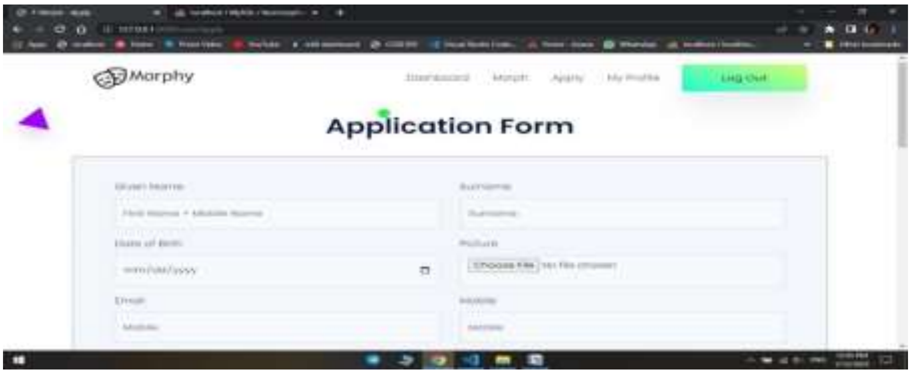


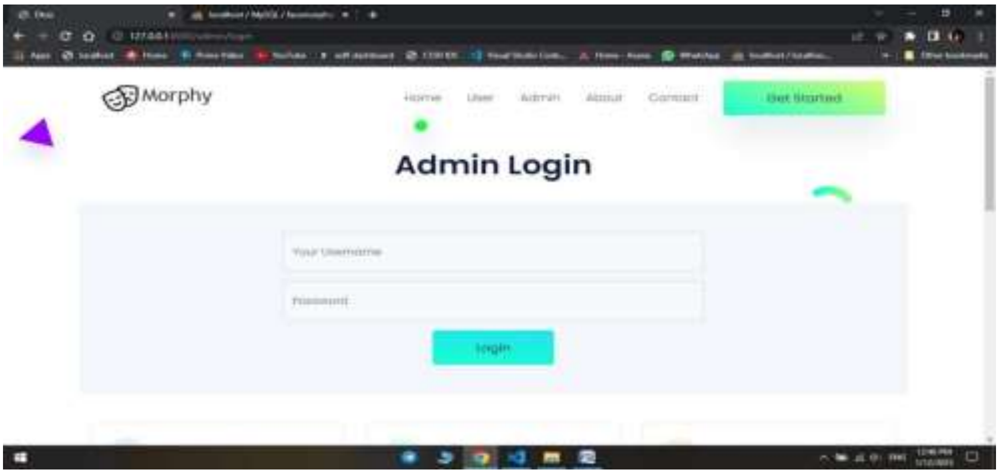
ISSN: 3049-0952
www.jsetms.com

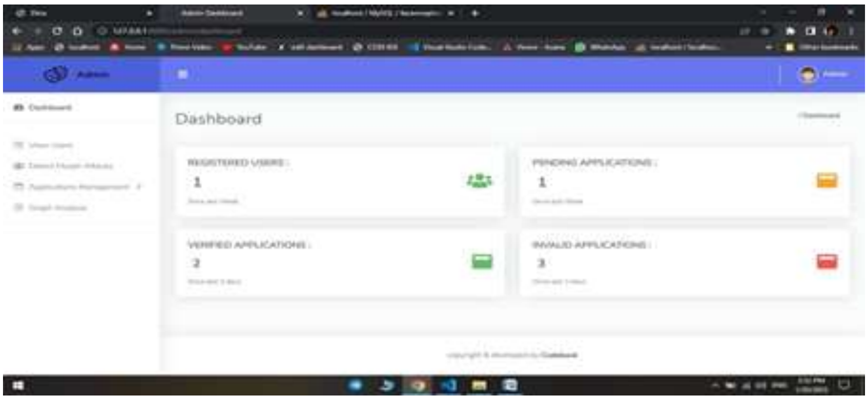


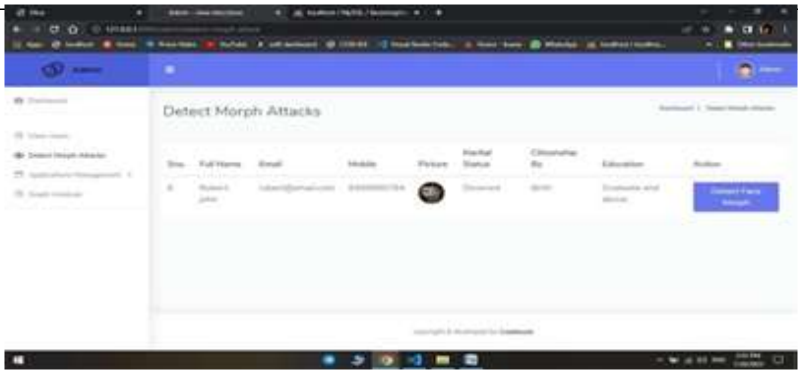
 ISSN: 3049-0952
www.jsetms.com

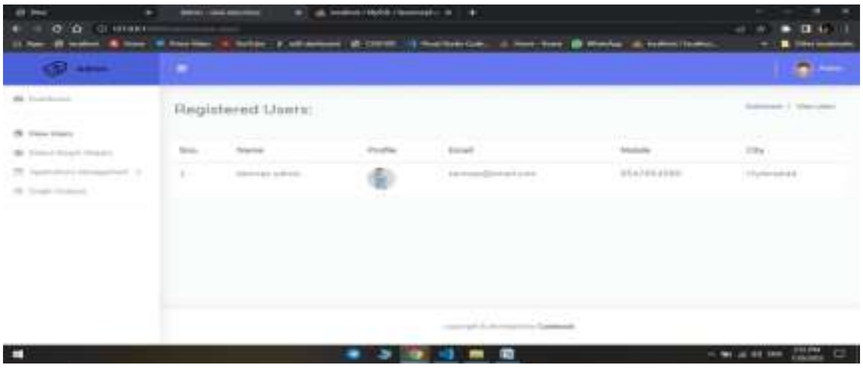


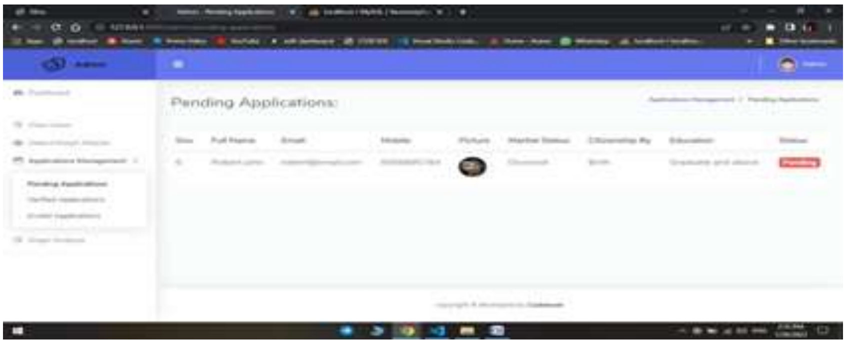


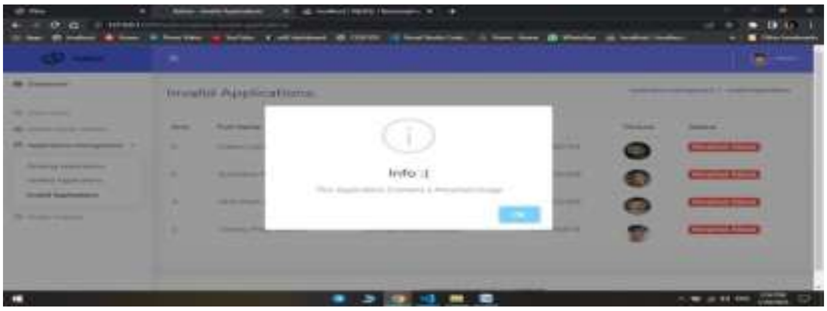


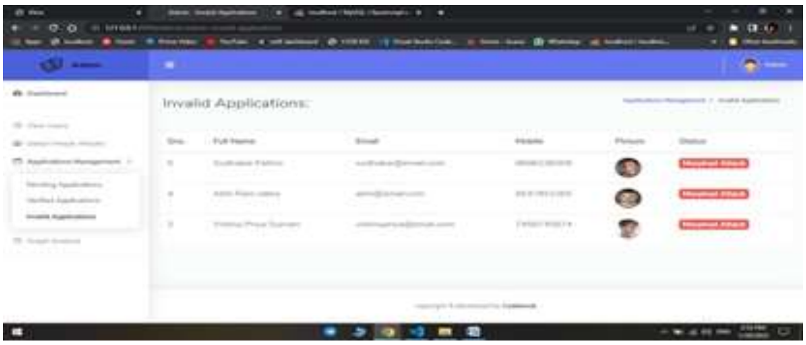


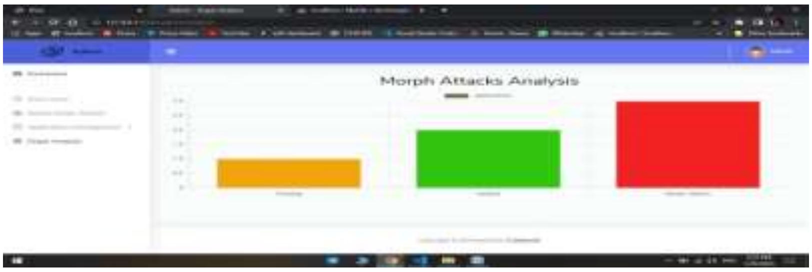

Detect Morph Attacks


Registered Users:


Pending Applications:


Invalid Applications
Info :|


Invalid Applications:



7 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. Differentfeaturecombinationtechniquesareanalyzedandfeatureconcatenation provedtobe 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 morphingtoolsweredifficulttodetectbythemodelsthatweretrainedon morpheddatabases that had low variation and were made automatically from low quality morphing tools like OpenCV and FaceMorpher using programming scripts.

Thetraining 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.Manuallycreatedmorph-3imageswereverydifficulttodetectwhenthemodel 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.

Itfurthersolidifiestheapproachtoincludediverserangeofmorphsinthetrainingdatabaseto improve the robustness of morph detection model. FGNET database proved to be the most difficult database of images in terms of morph detection as it can be seen in Fig. 9 that this database has a vast range of diversity in terms of age, image quality, colour variation and expression.Theseextremelevels of variations led to thecreation ofhighly complex morphed images that were very difficult to classify by the morph attack detection model.

FUTURESCOPE

Future work that can be done to improve this model and train it for all possible morph attacks in real world deployment scenarios will require the acquisition of real morphed images that were submit ted to different organizations like airports, identity card issuing authorities, travel agencies, universities and security institutions. The model should then be trained and tested on the real images to ensure better performance. Furthermore, an adaptive morph attack detection model should be designed that automatically adapts to the input images by applying the image enhancements as per requirement. More than three images may also be used for morphing.

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, 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 color 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 differentialmorphingattackdetection,''IEEETrans.Inf.ForensicsSecurity,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,''Imagemorphing:Asurvey,''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.BeierandS.Neely,''Feature-basedimagemetamorphosis,''ACMSIGGRAPHComput. 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 morphingattackdetectionwithaconvolutionalneuralnetworkde-morphingapproach,''IEEE Access, vol. 8, pp. 92301–92313, 2020.
12. C.Seibold,W.Samek,A.Hilsmann,andP.Eisert,''Accurateandrobustneuralnetworks forface morphing attack detection,''J. Inf. Secur. Appl., vol. 53, Aug. 2020, Art. no. 102526.
13. R.Raghavendra,K.B.Raja,S.Venkatesh,andC.Busch,''Transferabledeep-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 distortionandrobustmorphingattacksbasedonpartialfaceimagemanipulation,''IEEETrans. Biometrics, Behav., Identity Sci., vol. 3, no. 1, pp. 72–88, Jan. 2021.
17. D. ICAO,9303-MachineReadable Travel Documents—Part9:DeploymentofBiometric Identification and Electronic Storage of Data in EMRTDS, International Civil Aviation Organization (ICAO), Montreal, QC, Canada, 2015.
18. B.-C. Chen, C.-S. Chen, and W. H. Hsu, ''Face recognition and retrieval using cross-age referencecodingwithcross-agecelebritydataset,''IEEETrans.Multimedia,vol.17,no.6,pp. 804–815, Jun. 2015.
19. A.S.Georghiades,P.N.Belhumeur,andD.Kriegman,''Fromfewtomany:Illumination conemodelsforfacerecognitionundervariablelightingandpose,''IEEETrans.PatternAnal. Mach. Intell., vol. 23, no. 6, pp. 643–660, Jun. 2001. VOLUME 10, 2022 72575 M. Hamza et al.: Generation and Detection of Face Morphing Attacks
20. E.KussulandT.Baydyk,''Facerecognitionusingspecialneuralnetworks,''inProc.Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2015, pp. 1–7.
21. C. E. Thomaz and G. A. Giraldi, ''A new ranking method for principal components analysis and its

application to face image analysis,'' Image Vis. Comput., vol. 28, no. 6, pp. 902–913, 2010.