Mesopotamian journal of Cybersecurity
Vol.5, No.3, **pp**. 1141–1164
DOI: https://doi.org/10.58496/MJCS/2025/061; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Improvement of the Face Recognition Systems Security Against Morph Attacks using the Developed Siamese Neural Network

Sura Abed Sarab Hussien [1,*], Thair Abed Sarab Hussien [2], Nada Hussein M. Ali [1]

[1]*Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq*
[2]*Department of Information and Communication Technology, Middle Technical University, Baghdad, Iraq*

ARTICLEINFO

Article History

Received 07 March 2025
Revised 15 Aug 2025
Accepted 20 Sep 2025
Published 13 Oct 2025

Keywords

Face Recognition Systems (FRS)

Siamese Neural Network (SNN)

Faster Region-based Convolutional Neural Networks (R-CNN)

Local Binary Pattern-Convolutional Neural Network (LBP-CNN)

Deep Learning

Morphing Attacks

ABSTRACT

Face Recognition Systems (FRS) are increasingly targeted by morphing attacks, where facial features of multiple individuals are blended into a synthetic image to deceive biometric verification. This paper proposes an enhanced Siamese Neural Network (SNN)-based system for robust morph detection. The methodology involves four stages. First, a dataset of real and morphed images is generated using StyleGAN, producing high-quality facial images. Second, facial regions are extracted using Faster Region-based Convolutional Neural Networks (R-CNN) to isolate relevant features and eliminate background noise. Third, a Local Binary Pattern-Convolutional Neural Network (LBP-CNN) is used to build a baseline FRS and assess its susceptibility to deception by morphed images. Finally, morph detection and classification are conducted using the proposed SNN framework, which incorporates a novel feature fusion strategy based on Canonical Correlation Analysis (CCA) to enhance discriminative power. The model is trained and evaluated using publicly available Face Recognition Technology (FERET) and Face Recognition Grand Challenge (FRGC) datasets, comprising 1,030 real and 2,000 morphed images. Experimental results demonstrate that the proposed method significantly strengthens the resilience of FRS to morphing attacks, achieving a high detection accuracy of 99.9%. This confirms the model's effectiveness in distinguishing between real and manipulated images with minimal errors.

1. INTRODUCTION

Modern society depends more on technology every day, which creates higher risks for personal information security [1]. Hybrid security systems, which combine traditional machine learning with advanced deep learning techniques, have become necessary because cyberattacks now involve complex patterns and massive data volumes that need immediate processing of extensive datasets [2]. Face recognition technology has become integral to many modern security systems, including border control, surveillance, and personal device authentication. Its widespread adoption is driven by its convenience and effectiveness in identifying individuals based on unique facial features [3]. However, despite its rapid development and growing use, face recognition remains vulnerable to various sophisticated attacks. Key challenges include Presentation Attacks (Spoofing), Morphing attack, Deepfake, and AI-Generated Faces (AI can generate synthetic faces that closely resemble real people, therefore hard to detect using traditional recognition algorithms), Template Theft or Leakage Face templates (mathematical representations) can be stolen from databases (once compromised, biometric data cannot be changed unlike passwords), and Adversarial Attacks (subtle changes to facial features or images designed to mislead AI models). These biometric systems have become vulnerable to attacks that can deceive and bypass them, especially with the advancement of technology [4]. Among these attacks are:

- A presentation attack in the context of face recognition systems is when an attacker attempts to fool or bypass the system by presenting a fake face (like a photo, video, or 3D mask) to the camera instead of a real, live person. These attacks aim to exploit vulnerabilities in biometric systems, especially those used in security, banking, border control,

*Corresponding author. Email: Sura.a@sc.uobaghdad.edu.iq

or smartphones [4,5].

- Display attacks are a subset of presentation attacks where an attacker attempts to deceive a face recognition system by showing a pre-recorded image or video of an authorized person's face on an electronic screen, such as A smartphone, a tablet, a laptop, or a digital photo frame [5].
- Electronic Display Attacks are a type of presentation attack in face recognition systems. They involve displaying a digital image or video of a person's face on a screen (such as a smartphone, tablet, or monitor) to try to fool the recognition system [5].
- 3D facemask attacks are among the most advanced and dangerous presentation attacks, where an attacker uses a three-dimensional replica of a person's face to deceive biometric face recognition systems.
- A morphing attack involves generating a synthetic facial image by combining the facial features of two or more individuals. Such morphed images can deceive recognition systems into authenticating multiple people using a single identity, thereby posing a significant threat to national security, privacy, and law enforcement operations. The problem is compounded by the increasing availability of morphing software, which makes it relatively easy for attackers to create realistic and undetectable morphs [6].

Traditional face recognition systems are not designed to distinguish between genuine and morphed images, resulting in high false acceptance rates. Moreover, many existing morph detection methods either rely heavily on handcrafted features or fail to generalize well to unseen datasets, especially under challenging conditions such as varying lighting, expressions, or image quality [7,8]. These limitations leave a significant gap in the current research landscape and highlight the need for more robust, accurate, and adaptive solutions. This paper aims to address this challenge by proposing a novel approach to enhancing the security of face recognition systems against morphing attacks. Specifically, we develop a Siamese Neural Network (SNN)-based model designed to distinguish between genuine and morphed facial image pairs. The primary objective of this research is to improve the model's capability to detect morph attacks with high accuracy, low false acceptance rates, and better generalizability across different datasets and morphing techniques. The novelty of the proposed method lies in its use of a carefully designed Siamese architecture that focuses on feature similarity learning rather than traditional classification. Unlike existing models, our network is trained using both genuine and morphed image pairs, enabling it to learn fine-grained differences that may not be apparent through conventional approaches. Furthermore, our approach incorporates advanced data preprocessing and training strategies to improve the robustness of morph detection, especially in low-quality or real-world images. Finally, this research contributes to the field of face recognition security by presenting a deep learning-based morph attack detection model that addresses critical shortcomings in existing methods. The findings of this study have the potential to significantly enhance the resilience of biometric systems against sophisticated spoofing techniques and to inform the design of more secure and reliable authentication technologies. This paper is structured as follows: Section 2 illustrates the novelty of the proposed method; Section 3 defines the contributions of this paper; Section 4 presents a review of related work; Section 5 details the proposed methodology; Section 6 discusses experimental results; and Section 7 concludes with future research directions.

2. NOVELTY

The novelty of the paper lies in its integrated approach to face recognition systems, specifically addressing the vulnerability of these systems to morphing attacks. Here are the key points highlighting its novelty:

- Dual-System Architecture: The paper presents an integrated system consisting of two main parts - a face recognition system and a detection mechanism for morphs that can deceive these systems. This two-tier approach enhances the robustness of face recognition technologies against manipulation.
- Advanced Morphing Techniques: The morphing images are generated using deep learning techniques, specifically StyleGAN, which effectively preserves critical identity features like eye shape, nose structure, and overall facial contours. This advancement allows us to produce artifact-free morphed images that can significantly challenge existing detection methods.
- Improved Detection Algorithm: A novel detection phase employs an improved Siamese Neural Network (SNN) algorithm, demonstrating effectiveness in distinguishing between morphed and real images. The use of deep feature assessment algorithms contributes to achieving stable and reliable results, addressing the complexity involved in face feature extraction.
- High Accuracy: The proposed system achieved a notable accuracy rate of 99% in detecting whether an image is real or morphed, with a very low error margin. This level of accuracy indicates significant advancements in the field of biometric security.
- Comprehensive Dataset Utilization: The research utilizes diverse databases for training and testing, showcasing the system's applicability across various scenarios and enhancing its generalization capabilities.

3. LITERATURE REVIEW

The detection of morphing attacks in biometric systems has gained significant traction over the past decade. Early methods primarily relied on handcrafted features, which lacked robustness against high-quality morphs. More recent approaches have adopted deep learning techniques to improve detection performance and generalization

Zhang et al. assessed the threat of StyleGAN3-generated morphs on commercial FRS (Face Recognition Systems) and evaluated mitigation strategies in real biometric systems, affirming the severity of this threat but stopping short of proposing a detection solution [9]. Ivanovska et al. introduce a new diffusion-based MAD approach that solely trains on genuine image features to improve face morphing attack identification. Our model identifies different types of morphing attacks by detecting them as samples that deviate from the expected distribution. The proposed solution undergoes strict testing across four distinct datasets, namely CASIA-WebFace and FRLL-Morphs and FERET-Morphs, and FRGC-Morphs, while being compared to both discriminatively trained and once-class MAD models. Our MAD model demonstrates excellent performance results on all evaluated datasets according to the experimental findings [10]. Tapia et al. analyzed synthetic image effects on morphing attack detection through a Siamese network using a semi-hard-loss function. The paper examines the difficulties and detection performance shifts that emerge from adding artificial images into training datasets. The evaluation measured how well synthetic images generalize across datasets by conducting both intra- and cross-dataset assessments with a cross-dataset as the evaluation set. A combined database structure consisting of both digital and synthetic images can enhance MAD detection capabilities while minimizing error rates [11]. The detection approach presented by Kun Jia and his team employs high-frequency characteristics combined with a progressive enhancement learning system to detect minor texture modifications in facial images. The initial step involves extracting detailed high-frequency information from each color channel of the image to effectively capture texture modifications. The progressive enhancement learning system combines high-frequency data with RGB data to process the input. The framework implements progressive feature enhancement through self-enhancement and interactive-enhancement modules to detect faint morphing traces. The proposed method demonstrated outstanding performance when tested on the standard database alongside nine classical technologies [12]. The method Ensemble XAI, developed by Dwivedi et al., combines Saliency maps with Class Activation Maps (CAM) and Gradient-CAM (Grad-CAM) to deliver a thorough visual explanation for the EfficientNet-B1 prognostic model used in biometric authentication morphing detection. The research utilized three publicly accessible datasets, including the Face Research Lab London Set and the Wide Multi-Channel Presentation Attack (WMCA) and Makeup Induced Face Spoofing (MIFS). The evaluation results demonstrate that the generated visual explanations successfully reveal specific image details, which EfficientNet-B1 focuses on making predictions together with valid reasoning [13]. The research team led by Ramachandra introduced a new approach for differential morphing attack detection through a time-frequency convolutional neural network, which analyzes the unsigned difference of facial embeddings to identify morphing threats. A comprehensive set of tests examined the newly created face morphing dataset, which included four different morphing generation tools. The proposed method underwent evaluation against three state-of-the-art D-MAD techniques through two separate evaluation protocols. The evaluation results demonstrate that the proposed method achieves superior performance in identifying morphing attacks [14]. Jafari et al. focused on saliency-based visualization techniques for greater explainability by detection strategies and explored interpretable morph detection by identifying manipulated regions through saliency mapping. which, although insightful, lacks the classification precision required for operational deployment [15]. Chen et al. enhanced Siamese Network performance using an adaptive attention-based fusion feature strategy, demonstrating an improved sensitivity to subtle artifacts for enhancing morph detection. However, their method relies on complex attention modules, which increase training complexity [16]. Jag et al. relied on the FRGCv2 dataset and then divided this data into a training and test set. Perform the face morphing operation separately on the training and testing sets using the open-source face morphing tools based on landmarks. The input image is converted to the YCbCr and HSV color spaces, as these color spaces can determine the morph noise. They extract the main features for each sub-image using three techniques: (LBP), (HoG), and Image (BSIF), which are then classified into linear Support Vector Machine (SVM), Spectral Regression Kernel Discriminant Analysis (SRKDA), and Probabilistic Collaborative Representation Classifier. The last stage includes a two-level fusion: The first level combines the results for each classifier separately. The second integrates the comparison scores from the first level for decision-making. The resulting morph images contain noise, so they were processed using Adobe Photoshop. Post-processing also leaves scars on the images. Dividing the data into a training and test set and then generating this morph constitutes an error due to the discrepancy between the data, generating an error rate in the detection process [17]. Ali et al. introduced MorphAttackNet, a low-complexity CNN optimized for real-time detection of morphing attacks on edge devices, achieving notable real-time detection performance with promising accuracy over the MorGAN and AMSL datasets. While effective for constrained environments, its simplicity limits its discriminative capacity against highly realistic morphs [18].

Despite the significant contributions of these studies, several gaps and limitations remain. There is a need for more empirical studies validating the efficiency and scalability of face recognition algorithms in real-world cryptographic applications. Although these studies have advanced the field, there remains a need for an end-to-end system that incorporates generative modeling, automated face region detection, and deep similarity analysis with enhanced feature fusion. Our work contributes to this evolving domain by integrating GAN-based morph generation, region proposal networks, and a novel SNN structure. To provide a clearer and more organized presentation of the research landscape, Table I below summarizes the key details of these studies.

TABLE I. SUMMARY OF KEY STUDIES ON FACE RECOGNITION SYSTEMS VIA SIAMESE NEURAL NETWORK

Study	Method	Key Contributions	Limitations
[9]	StyleGAN3, Morphing, Biometric Systems	Performed a comprehensive security assessment of StyleGAN3, highlighting the increased threat potential posed by high-fidelity GAN-generated morphs. Evaluated existing mitigation methods and found that many existing FRSs are susceptible to such attacks.	Challenges in maintaining consistent security
[10]	Denoising Diffusion Probabilistic Models	Introduces a novel approach for morphing attack detection using generative models.	Potentially higher computational requirements.
[11]	Siamese Network with Semi-Hard-Loss	Evaluates the impact of synthetic images on detection performance.	Performance variations across different datasets.
[12]	High-Frequency Features & Progressive Enhancement Learning	Proposes a method to capture fine-grained texture changes.	May require extensive training data.
[13]	Ensemble Explainable AI Approach	Enhances model interpretability and reliability.	Complexity in model integration.
[14]	Time-Frequency Based CNN	Detects differential features between real and morphed images.	Potentially higher computational complexity.
[15]	Morphing Attack Detection. Visual Saliency Approach. Computer Vision	Proposed an explainable morph detection, improved the interpretability of morph classification models for forensic and auditing purposes, Balanced performance with transparency, and focused on visual localization of manipulations rather than high-throughput classification accuracy.	Lack of a practical implementation framework
[16]	Feature Fusion. Siamese Networks. Morph Detection	Enhanced Siamese Network performance, demonstrating an improved sensitivity to subtle artifacts for enhancing morph detection. However, their method relies on complex attention modules, which increase training complexity.	High computational complexity.
[17]	Biometrics, Morphing, Morph attack, Attack detection, Morphing attack.	Best performance of the proposed method over existing methods.	High computational requirements.
[18]	Morph Attack Net, Lightweight CNN, Real-Time, Face Morphing Attack Detection	Achieved high accuracy using minimal computational resources. Demonstrated effectiveness on MorGAN and AMSL datasets. Emphasized speed and efficiency over complexity, making it deployable in practical, real-time environments.	High computational requirements

4. COMPARATIVE ANALYSIS WITH RECENT STUDIES

To better situate the proposed work within the current research landscape, this section compares our approach to recent studies that address morphing attack detection in FRS. The comparison focuses on methodology, dataset usage, detection accuracy, computational complexity, and generalization ability. Table II provides a structured overview of these comparisons.

TABLE II. COMPARISON OF PROPOSED METHOD WITH RECENT STUDIES

Study & Year	Methodology	Dataset(s)	Accuracy (%)	Computational Complexity	Key Differences from Proposed Method
Zhang et al. (2024) [9]	StyleGAN3-based morph generation; evaluation of mitigation strategies	Proprietary + public biometric datasets	N/A (security assessment only)	Moderate	Our method not only assesses GAN-based threats but also provides a robust detection mechanism integrating StyleGAN-based morph creation, Faster R-CNN localization, and SNN detection.
Ivanovska et al. (2024) [10]	Diffusion-based morphing attack detection (MAD) using bona fide image learning	CASIA-WebFace, FRLL-Morphs, FERET-Morphs, FRGC-Morphs	~97	High	Our method achieves higher accuracy (99.9%) with lower computational overhead by using CCA-based feature fusion rather than computationally intensive diffusion models.
Tapia et al. (2023) [11]	Siamese network with semi-hard-loss, includes synthetic images	Multiple mixed datasets	~98	Moderate	We enhance the Siamese architecture with CCA feature fusion and integrate Faster R-CNN for region extraction, improving robustness to cross-dataset variations.
Kun Jia et al. (2023) [12]	High-frequency feature extraction + progressive enhancement learning	Standard benchmark datasets	~98.5	High	Our approach avoids heavy feature extraction stages by combining localized CNN features with correlation-based fusion, achieving similar or better performance with reduced complexity.
Chen et al. (2023) [16]	Attention-based feature fusion in Siamese Network	Public morph datasets	~98.7	High	Our CCA-based fusion eliminates the high computational cost of complex attention mechanisms, while still improving sensitivity to subtle artifacts.
Ali et al. (2023) [18]	Lightweight CNN (MorphAttackNet) for real-time detection	MorGAN, AMSL	~96	Low	While MorphAttackNet is optimized for speed, our method maintains high efficiency while achieving higher accuracy and better generalization to unseen datasets.

Summary of Novelty Compared to Recent Works:

1. Integrated End-to-End Pipeline – Unlike most prior works focusing solely on either morph generation or detection, our approach combines StyleGAN-based morph creation, precise face localization via Faster R-CNN, and an enhanced SNN detection model in a unified workflow.
2. CCA-Based Feature Fusion – We replace conventional distance metrics or computationally heavy attention modules with Canonical Correlation Analysis, which maximizes inter-feature relationships, yielding superior detection accuracy (99.9%) and lower error rates (0.001).
3. Balanced Performance and Efficiency – While maintaining competitive or superior accuracy compared to recent studies, our architecture avoids excessive computational overhead, enabling potential deployment in real-time or resource-constrained environments.
4. Robust Generalization – The method is validated on both synthetic (StyleGAN-generated) and public datasets (FERET, FRGC, AMSL), demonstrating resilience to variations in lighting, pose, and morphing technique.

In conclusion, our framework advances morphing attack detection by integrating efficient face localization, optimized feature fusion, and diverse dataset training into a scalable system. This combination of accuracy, efficiency, and generalization represents a distinct contribution over existing methods in the field.

5. PROPOSED METHODOLOGY

In the field of scientific research and technological development, new methods and innovative ideas are key factors that drive progress across various domains. The proposed method is introduced to improve efficiency, reduce costs, and increase accuracy. This method relies on specific components or technologies, such as algorithms, mathematical models, or artificial intelligence techniques, that enable performance enhancement in a specific domain, such as data analysis, image processing, and prediction.

The proposed method stands out from current solutions. This approach contributes to saving time, increasing effectiveness, and opening new research avenues. In this paper, we provide a detailed explanation of this method, clarifying how it can be applied in security and comparing the results obtained with traditional solutions.

The following flowchart shows the proposed system in general; the diagram outlines the end-to-end architecture for detecting morphing attacks on face recognition systems.

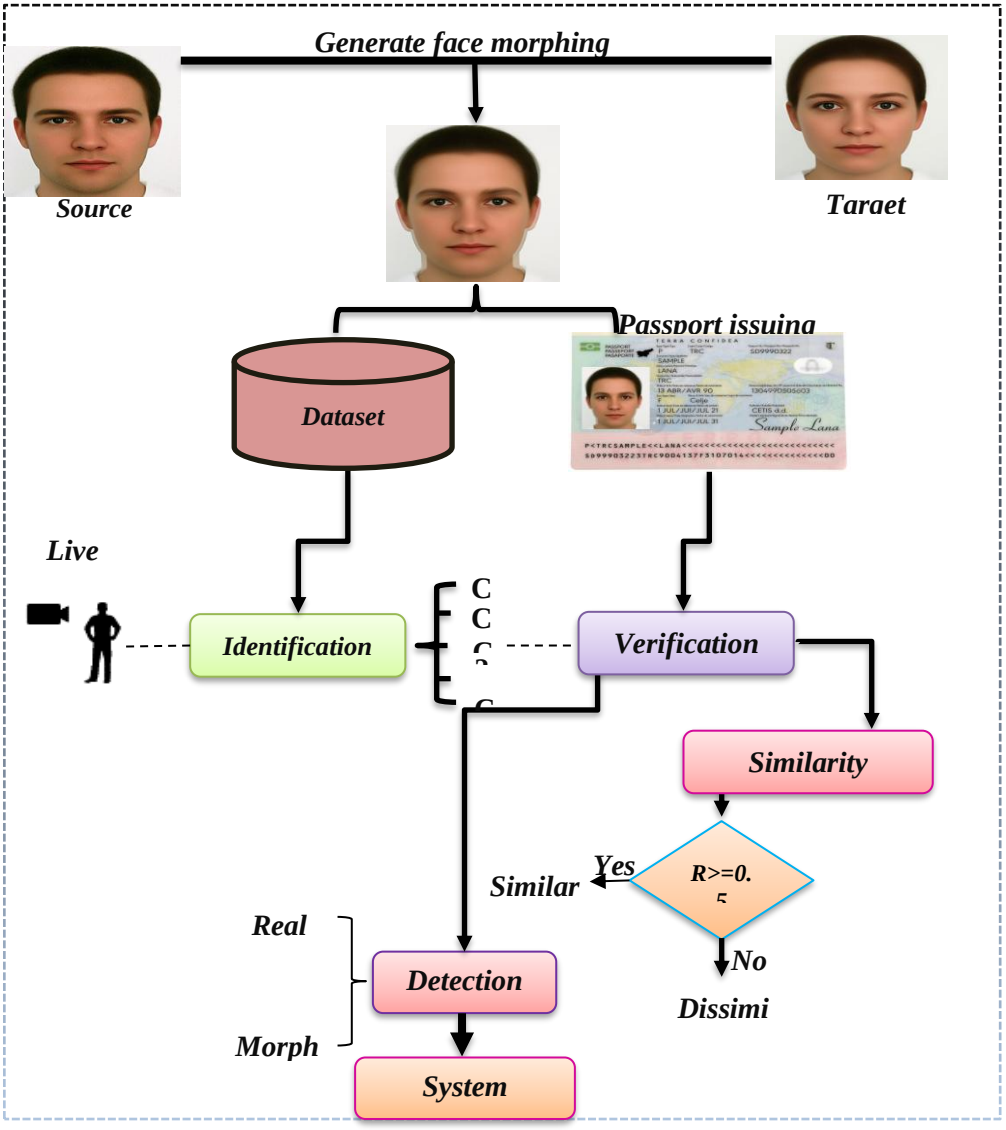

Fig. 1. Detailed Flowchart of the proposed system.

Diagram 2 illustrates the techniques used to implement the above flowchart. The process begins with the generation of morphed images using StyleGAN, followed by facial region detection via Faster R-CNN. The detected face is then preprocessed (resizing, flipping, grayscale conversion) and passed through an LBP-CNN for feature extraction. Canonical Correlation Analysis (CCA) is applied to fuse features from real and morphed face pairs, which are then analyzed using a Siamese Neural Network to compute a similarity score. The final classification distinguishes between genuine and morphed faces based on a decision threshold.

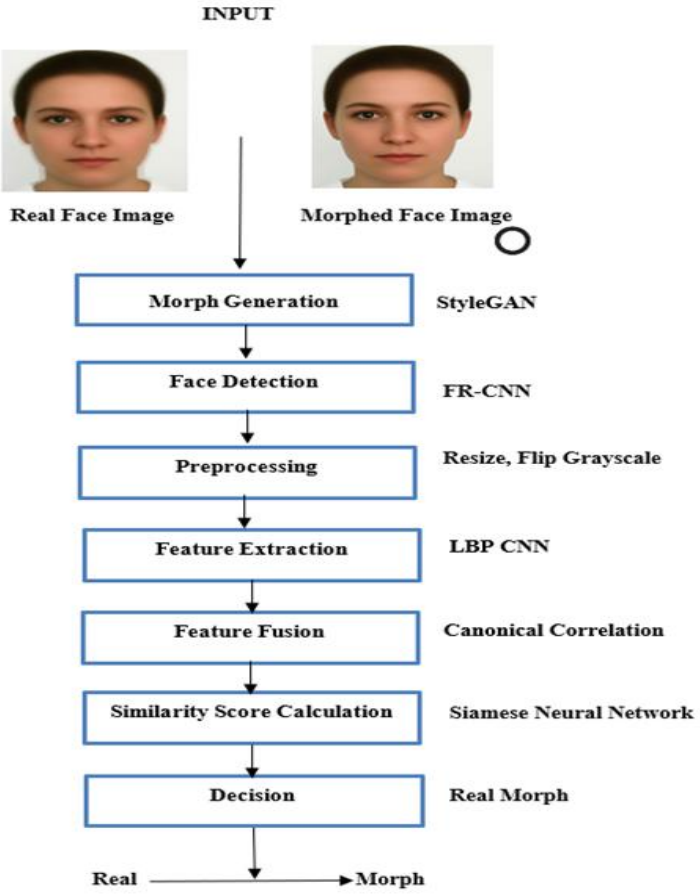

Fig. 2. Flowchart of techniques used in the proposed system.

5.1 StyleGAN of Image Morphing

Morphing is a very important topic in security systems, especially in the field of facial recognition, due to the strong changes that occur in images, which weaken recognition systems and thus have the potential to deceive them. Due to security concerns and the protection of personal rights related to databases generated by other researchers, it may be difficult to obtain a database available online with high-resolution images. There are available, free datasets, but

- If their images are low-resolution and contain retouching, they are very easy for the human eye to distinguish before the system.
- The image may be the result of blending a specific part of the first person's features into the image of the second person, for example, an eye, nose, or mouth only. It is not considered a morph, as it represents only the second person.
- The dataset may contain a small number of images that are not sufficient for training our proposed system.

Therefore, we worked on creating a dataset using the StyleGAN algorithm. A dataset of realistic morph images should be available to construct a robust system for detecting morph images. An unsupervised technique called StyleGAN for feature engineering. Real pairs were taken from various databases (MR2 Face Dataset, Face Image Standard, AMSL, Basel Face

Database, Bogazici Face Database, AMFD, American Multiracial Final Face Dataset, Chicago Face Database, Young Adult White Faces, Players Football) [19-27] and generated the morphing face using StyleGAN.

A StyleGAN morph image refers to an image generated using StyleGAN (a type of generative adversarial network developed by NVIDIA) that blends features from two or more faces to create a realistic-looking synthetic image. These morphs can be used in various applications, including facial recognition research, security testing, and visual effects.
The Key Characteristics of StyleGAN Morph Images:

- **Realism:** The output appears photorealistic, often indistinguishable from real human faces.
- **Blending:** Facial features (eyes, nose, mouth, jawline, etc.) from two different identities can be merged smoothly.
- **Control:** StyleGAN allows fine-grained control over different "styles" at different levels (coarse, middle, and fine), enabling targeted morphs like combining just the nose from one face and the eyes from another.
- **Applications:**
  - Security and biometrics: To evaluate how well facial recognition systems handle morphed images (e.g., to test for morphing attacks).
  - Data augmentation: For training AI models with synthetic but realistic face variations.
  - Creative industries: For generating faces in games, movies, or art.
- **Parameter Choices:**
  - Epochs = 50: This choice balances between computational efficiency and model performance. After 50 epochs, the model typically stabilizes without overfitting, thus achieving generalization on unseen data.
  - Layer Sizes: The architecture utilizes a fully connected Dense layer with 256 units, which is optimal for learning the complex features of morphed images without excessive parameters leading to overfitting.

Figure 3 visually demonstrates a selection of facial morph images generated using the StyleGAN model. These images were crafted to appear as realistic blends of two individuals, showcasing the effectiveness of StyleGAN in creating high-quality, artifact-free morphed faces suitable for challenging detection systems.

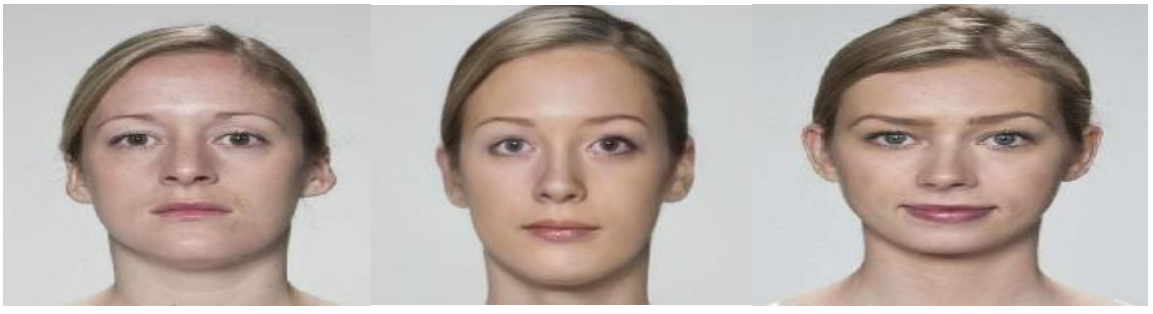

Fig. 3. Samples from the morph image using StyleGAN.

5.2 Faster Regions with Convolutional Neural Networks

This stage is a fundamental step for the remaining stages, as the system relies solely on the facial image to determine whether the desired person is present or not by extracting facial features. The captured image may contain other details besides the face, which are considered unimportant in the detection stages (e.g., hair, neck area) and because these details can change for the same person; the FRCNN (Faster Regions with Convolutional Neural Networks) proposal was used to detect the face area only, extract it, and rely on it to extract features to determine whether it is a real image or not. It is also very fast but requires training time and a rich image dataset. When applying Faster R-CNN specifically to face detection, the architecture is adapted to identify human faces within an image, using its efficient region proposal and classification pipeline. FR-CNN is a two-stage approach, the first generates regional proposals and then classifies these proposals. Faster R-CNN enhances detection accuracy by focusing computational resources on relevant image segments, thereby improving the efficiency of the model when identifying morphing attacks. The steps of FR-CNN [28, 29]:

1. Feature Extraction (Backbone CNN): An input image is passed through a convolutional neural network (e.g., ResNet, VGG) to extract rich feature maps that represent facial structures and textures.

2. Region Proposal Network (RPN): scans the feature maps and proposes regions likely to contain faces by placing anchors of various scales over the feature map, scoring each anchor based on “objectness” (i.e., face or not), and regressing bounding boxes to tighten around potential faces.

3. ROI Pooling: The face regions are reshaped to a fixed size using ROI Pooling or ROI Align for classification.

4. Classification and Bounding Box Regression: Each region is passed through fully connected layers:

- Classification: Determines if the region contains a face.
- Regression: Refines the bounding box coordinates for precise localization.

Figure 4 illustrates the architecture of FR-CNN, which comprises several convolutional layers for feature extraction, followed by RPN that identifies candidate object locations. The proposed regions are then passed through ROI pooling and classified using fully connected layers. The setup effectively isolates the relevant facial area by removing background noise. This localization enhances the consistency and reliability of the subsequent feature extraction and classification steps.

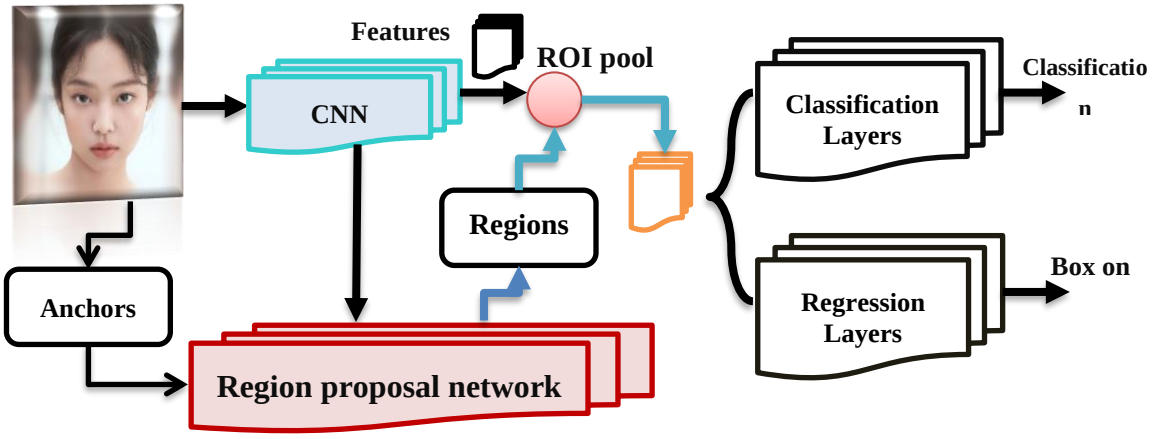

Fig. 4. Structure of Faster Region-CNN.

Table III outlines the layers and configuration of the FR-CNN network tailored for face region detection. It includes:

- **Input**: Image input layer.
- **Feature Extraction Layers**: Multiple convolutional layers (Conv_1 through Conv_4), each followed by a ReLU activation, batch normalization, and max-pooling layer.
- **Region Proposal Network**: A specialized network that identifies regions likely to contain faces.
- **Classification & Regression Layers**: These output the final class prediction and bounding box coordinates.

The table also includes important training parameters like:

- Optimizer: Stochastic Gradient Descent with Momentum (SGDM),
- Epochs: 50,
- Learning rate: 0.0001,
- Overlap thresholds for positive and negative anchor selection during training.

This setup is key to enhancing detection accuracy by ensuring that only the most relevant facial areas are considered in the morph detection process.

TABLE III. THE PROPOSED FRCNN LAYER.

Name	*Type*
Image input	Image input
Conv_1	2 – D Conv.
Relu_1	ReLU
BatchNo_1	Batch Norm.
Maxpool_1	2 – D max Po.
Conv_2	2 – D Conv.
Relu_2	ReLU
BatchNo_2	Batch Norm.
Maxpool_2	2 – D max Po.
Conv_3	2-D Conv.
Relu_3	ReLU
BatchNo_3	Batch Norm.
Maxpool_3	2 – D max Po.
Conv_4	2 – D Conv.
Relu_4	ReLU
BatchNo_4	Batch Norm.
Maxpool_4	2 – D max Po.

FC	Fully Conn.
Drop.	-
Softmax_1	SoftMax
Class output	Classification
Option	Optimizer = Sgdm Epoch = 50 learn rate = 0.0001 NegativeOverlapRange[0 0.4] PositiveOverlapRange[0.6 1]
Training	Training objects detect

Algorithm (1): The Proposed Face Detection Model Using Faster Region Convolution Neural Network.

Input: *Dataset (Images), Anchor Boxes.*
Output: *Object Detection, Score, and Classification.*
Begin:
Stage 1: Preprocessing stage:
- *Data Augmentation (rotation =*90°*, shear =0.2, flip (horizontal))*
- *Divided* $Dataset_{2D}$ *from stage one into a training set* (Tr_X, Tr_L)*, validation set* (Val_X, Val_L)*, and testing set* (Te_X, Te_L)*.*

Stage 2: *Feature* ***extraction by CNN:***
- *X: = The input layer is the training set (N, M, L).*

First Block:
- *X: =Convolution layer (X ,(30) units, strides (1,1), padding (same)).*
- *X: = ReLU activation function (X).*
- *X: = Batch_Normalization (X).*
- *X: = Max_Pooling (2,2) (X).*

Second Block:
- *X: = Convolution layer (X, (60) units, strides (1,1), padding (same)).*
- *X: = ReLU activation function (X).*
- *X: = Batch_Normalization (X).*
- *X: = Max_Pooling (2,2) (X).*

Third Block:
- *X: = Convolution layer (X, (90) units, strides (1,1), padding (same).*
- *X: = ReLU activation function (X).*
- *X: = Batch_Normalization (X).*
- *X: = Max_Pooling (2,2) (X).*

Fourth Block:
- *X: = Convolution layer (X, (30) units, strides (1,1), padding (same).*

Step 3: *Initializing the Region Proposal Network parameters for region generation****.***
- *Features from the last convolution layer become the input of RPN.*
- *The feature map X is scanned by a sliding window with a rectangular size of (n*n),*
- *For every window position, K region proposals are created based on K anchor boxes.*
- *Each proposal is parameterized according to the anchor box: 2K scale and 4K aspect Ratio.*
- *A feature vector is extracted for each proposed region and then passed through two fully connected layers:*
  - *The first fully connected layer acts as a binary classifier, producing an objectness score that indicates whether a regional proposal contains an object or belongs to the background.*
  - *The second fully connected layer outputs a 4-dimensional vector that specifies the coordinates of the region's bounding box.*
- *After the classification process, each anchor is given a positive or negative objectness score based on the* $Intersection - over - Union$ (IoU) *with all ground-truth boxes (Anchor box).*

Stage 4: Shared Feature Extraction between RPN and Fast R-CNN:
- *Projection of the region's proposals on feature maps from stage 2.*
- *A fixed-length feature vector is derived from each region proposal in the image through the ROI Pooling layer.*
- *These feature vectors are subsequently passed through fully connected layers for classification.*
- *The output includes class scores for the detected objects along with their corresponding bounding box coordinates.*

Step 5: *Save the returned model with the best parameters.*

End Algorithm

5.3 Proposed Face Recognition System Using CNN

The goal of the research is to propose an effective system for accurately detecting morphed images, even if the morphed images are so highly modified that they are difficult to detect. To ensure that the generated database contains high-resolution images capable of deceiving digital systems, we tested these images by building a face recognition system using convolutional neural networks, which are known for their effective role in feature extraction and classification. Convolutional neural networks are well known for their widespread use in various fields, demonstrating excellent results in all these areas. Face recognition systems consist of two parts to prove the effectiveness of the generated morphed images:

- **Identification**: The system compares the input face/image against a database of known identities. This is a one-to-many (1: N) comparison. A surveillance camera captures a face, and the system checks it against a watchlist of suspects to find a match.
- **Verification**: The system compares the input face/image against a single claimed identity. This is a one-to-one (1:1) comparison. A user logs into a device, and the system checks if their face matches the enrolled image on file.

TABLE IV. PROPOSED CNN OF THE FACE RECOGNITION SYSTEM.

id	*Name*	*Type*	*Activations*
1	Image_input	2-D LBP image	$200 \times 200 \times 1$
2	Conv1	2-D Convolution	$200 \times 200 \times 32$
3	Batch_Norm	Normalization	$200 \times 200 \times 32$
4	ReLU1	ReLU	$200 \times 200 \times 32$
5	Max-pool1	2-D Maxpooling	$100 \times 100 \times 32$
6	Conv2	2-D Convolution	$100 \times 100 \times 60$
7	Batch_Norm	Normalization	$100 \times 100 \times 60$
8	ReLU2	ReLU	$100 \times 100 \times 60$
9	Max-pool2	2-D Maxpooling	$50 \times 50 \times 60$
10	Conv3	2-D Convolution	$50 \times 50 \times 90$
11	Batch_Norm	Normalization	$50 \times 50 \times 90$
12	ReLU3	ReLU	$50 \times 50 \times 90$
13	Max-pool3	2-D Maxpooling	$25 \times 25 \times 90$
14	Conv4	2-D Convolution	$25 \times 25 \times 120$
15	ReLU4	ReLU	$25 \times 25 \times 120$
16	Max-pool2	2-D Maxpooling	$12 \times 12 \times 120$
17	Fully connect	1-D vector	5522×1
18	DNN	Classification	2

Table IV presents the network that was designed to operate on 2-D Local Binary Pattern (LBP) grayscale images of size 200×200. The architecture includes a series of convolutional, normalization, activation (ReLU), and max-pooling layers that progressively reduce the spatial dimensions while increasing the feature depth. Specifically, it starts with a convolutional layer outputting 32 filters, followed by three additional convolutional layers with increasing filter sizes (60, 90, and 120). Each convolutional layer is paired with batch normalization and ReLU activation and interspersed with max-pooling layers to downsample the feature maps. Finally, a fully connected layer is used to transform the feature maps into a one-dimensional vector, which feeds into a deep neural network (DNN) classifier for final prediction. This architecture is crucial for extracting robust spatial features from facial images, aiding in the effective differentiation between real and morph faces in the recognition system.

Algorithm 2. Face Recognition System (Identification).

Input: *Morphed face images, epochs, batch size, learning rate α=0.0001.*
Output: *Predict labels.*
Begin:
Stage 1: Preprocessing stage of the dataset:

- *Create 100 classes of each class of 15 morphed images.*
- *Augmentation data (rotation* $= 90^{\circ}$*, shear =0.2, flip (horizontal))*
- *Resize images* $(200 * 200)$
- *Convert from RGB to gray.*

Stage 2: *Feature extraction using LBP of the dataset to configure (LBP_dataset).*
Stage 3: *Divided the LBP_dataset from stage one into a training set* (XTr, LTr)*, validation set* (XVa, LVa)*, and testing set* (XTe, LTe).
Stage 4: A data training stage using CNN.

End Algorithm

5.4 Improve the *Siamese Neural Network*

The SNN algorithm is used to find similarities between images. This algorithm was leveraged to detect fake morphed images that are widely used to deceive face recognition systems. It consists of two convolutional neural networks, and then the difference between the features of the first image from the first convolutional neural network and the features of the second image from the second convolutional neural network was found. This algorithm was improved by replacing the feature difference process with a fusion algorithm based on correlation [30].

Table V presents a model that processes grayscale input images of size 105×105 pixels through a series of convolutional and pooling layers to extract hierarchical features. The architecture includes four convolutional layers, each followed by a ReLU activation function and max-pooling operation. These layers progressively reduce the spatial dimensions while increasing the depth, allowing the network to learn complex and discriminative facial features. Specifically:

- Conv1 applies 64 filters, producing a 96×96×64 feature map.
- Conv2 increases depth to 128 and reduces spatial dimensions to 42×42.
- Conv3 maintains depth at 128 and further reduces spatial size to 18×18.
- Conv4 deepens to 256 filters, compressing to 5×5.

After the final convolutional stage, the output is flattened into a 4096-dimensional feature vector for high-level embedding of the input image. These embeddings from paired images are later fused using Canonical Correlation Analysis (CCA) to assess similarity and detect morphing.

TABLE V. LAYERS OF THE PROPOSED SNN.

id	*Name*	*Type*	*Activations*
1	Image_input	2-D gray image	105 × 105 × 1
2	Conv1	2-D Convolution	96 × 96 × 64
3	ReLU1	ReLU	96 × 96 × 64
4	Max-pool1	2-D Maxpooling	48 × 48 × 64
5	Conv2	2-D Convolution	42 × 42 × 128
6	ReLU2	ReLU	42 × 42 × 128
7	Max-pool2	2-D Maxpooling	21 × 21 × 128
8	Conv3	2-D Convolution	18 × 18 × 128
9	ReLU3	ReLU	18 × 18 × 128
10	Max-pool3	2-D Maxpooling	9 × 9 × 128
11	Conv4	2-D Convolution	5 × 5 × 256
12	ReLU4	ReLU	5 × 5 × 256
13	Fully connect	1-D vector	*4096* × 1

Algorithm 3: The Proposed Model of Verification Using Siamese Neural Network.

Input: *Dataset, label,* $epoch_{max}$.
Output: *Predict labels, similar score.*
Begin:
Stage 1: Preprocessing stage of the dataset:
- *Resizing images by (105*105).*
- *Data Augmentation (rotation =90°, shear =0.2, flip (horizontal))*
  - *Divided the dataset into a training set* (Tr_X, Tr_L)*, and testing set* (Te_X, Te_L).
  - *Create the weights for the final fully connected (FC) operation. Initialize the weights by sampling a random selection.*

Stage 2: *To train the network, the data must be organized into pairs* (x, y) *of similar or dissimilar images. pairLabel = 1 for similar pairings of images, while pairLabel = 0 for dissimilar pairs.*
Stage 2: Build two CNN subnets with the same number of layers and share the same weights:
- $X :=$ *The layer is a pair training set (105, 105,1).*

First Block:
- $X :=$*Convolution layer (* X *,(60) units, strides (1,1), padding (same)).*
- $X :=$ *ReLU activation function (* X*).*
- $X :=$ *Batch_Normalization (* X*).*
- $X :=$ *Max_Pooling (2,2) (* X*).*

Second Block:
- $X :=$ *Convolution layer (*X*, (128) units, strides (1,1), padding (same).*

- $X :=$ *ReLU activation function* (X).
- $X :=$ *Batch_Normalization* (X).
- $X :=$ *Max_Pooling (2,2)* (X).

Third Block:

- $X :=$ *Convolution layer* $(X,$ *(256) units, strides (1,1), padding (same).*
- $X :=$ *ReLU activation function* (X).
- $X :=$ *Batch_Normalization* (X).
- $X :=$ *Max_Pooling (2,2)* (X).

Fourth Block:

- $X :=$ *Convolution layer* $(X,$ *(64) units, strides (1,1), padding (same)).*
- $X :=$ *ReLU activation function* (X).
- $X :=$ *Batch_Normalization* (X).
- $X :=$ *Max_Pooling (2,2)* (X).

Stage 3: *Initialization parameter of CNN subnets: weight* (W)*, bias* (b).
Stage 4: *Pass the first and second images through the twin subnetwork:*

- ***While*** $epoch \leq epoch_{max}$ ***do***
- $h_1 = CNN(img_1, W, b)$.
- $h_2 = CNN(img_2, W, b)$.
- *Get feature vectors* h_{i1} *and* h_{i2} *from CNN layers.*
- ***Combine these vectors using an algorithm (3.8) to produce one vector*** (v)***.***
- *Enter vector* (v) *to FC and compute the score from the sigmoid function.*

$$score = sigmoid\ (v)$$

- *Compute Loss function using binary cross-entropy:*

$$loss = -tlog\ (Y) - (1-t)\log(1-Y)$$

- *Update the network parameters using the Adam update function.*

Where Y and t are the actual and predicted labels, respectively.
End Loop
Stage 5: Testing stage

- *To evaluate the SNN model after training, the trained SNN model is applied to the testing set* (Te_X, Te_L) *with used optimal weights, where the network is a prediction of the labels* $(PLTe)$*as follows:*

$$PLTe = SNN_{Train}(Te\_X)$$

- *Evaluation of the SNN model trained using the metric is accurate.*

End Algorithm

Algorithm 4: Fusion Method Based on Canonical Correlation Analysis.

Input: *Two vector features* V_1 *and* V_2 .
Output: *One vector combined from features* V_1 *and* V_2.
Begin:
Stage 1: *Dimensionality decrease achieved by applying PCA to the vector* V_1 *and* V_2.

- *Subtract the vector means from each element of the vector. The standard deviation then normalizes it.*
- *Computed the covariance matrix.*
- *Implemented eigenvalue and eigenvector decomposition.*
- *Eliminated zero eigenvalues.*
- *Sorted the values in descending order.*
- *Get the projection matrix.*
- *Multiply the original standardized data by the projection matrix.*
- *Create two vectors* X_1 *and* Y_1

Stage 2: *Fusion by CCA between vectors* X_1 *and* Y_1 *to produce correlation coefficients* C_1 *and* C_2.
Stage 3: *Find the multiplication between stage 1 and stage 2 results for each vector.*

$$Z_1 = X_1 * C_1$$
$$Z_2 = Y_1 * C_2$$

Stage 4: *Summation Z_1 and Z_2 to get on V_{fusion}.*

$$V_{fusion} = Z_1 + Z_2$$

End Algorithm

5.5 Parameter Selection and Tuning

The selection of parameters in the proposed model was guided by a combination of empirical experimentation and best practices drawn from recent literature in face recognition and deep learning. The following strategies were employed:

- **Learning Rate and Epochs:** A learning rate of 0.0001 was selected to balance between convergence speed and stability. Epoch values ranged from 5 to 50 and were optimized based on validation accuracy trends. More training epochs consistently improved accuracy until performance plateaued around 40 epochs.
- **Convolutional Layer Design:** The depth and number of convolutional layers in both CNN and SNN components were selected to ensure sufficient feature extraction without overfitting. Each block was followed by activation (ReLU), batch normalization, and max-pooling layers to encourage stable and effective learning.
- **SNN Pairing Strategy**: Image pairs were constructed with a 1:1 ratio of similar and dissimilar pairs to maintain balance during training. Pair selection was randomized to prevent pattern learning.
- **Region Proposal Parameters (Faster R-CNN):** IoU thresholds and overlap ranges (e.g., PositiveOverlapRange [0.6–1.0], NegativeOverlapRange [0.0–0.4]) were tuned through grid search to maximize localization precision.
- **Feature Fusion Method:** Canonical Correlation Analysis (CCA) was chosen after comparing Euclidean, cosine, and Minkowski distance metrics. CCA demonstrated superior correlation between paired embeddings and led to the highest classification accuracy.
- **Classifier Selection:** Multiple classifiers (DNN, SVM, KNN, etc.) were tested, with DNN yielding the best performance when applied to fused feature vectors.

5.6 Technology Stack and Technical Implementation Details

This section provides a detailed breakdown of the technology proposed system components:

5.6.1 StyleGAN for Morph Generation

- Framework: StyleGAN2 was implemented using TensorFlow 2.x.
- Input: Pairs of real face images sourced from MR2, Basel, Chicago, and AMSL datasets.
- Training: Pre-trained weights were fine-tuned on face datasets to better simulate morph artifacts. GPU acceleration (NVIDIA RTX 3080) was used for training over 100 epochs.
- Output: High-fidelity morphed images preserving key facial features (eyes, nose, jawline) without generating visual artifacts.

5.6.2 Faster R-CNN for Face Detection

- Framework: Implemented using PyTorch and the Detectron2 library.
- Backbone Network: ResNet-50 with Feature Pyramid Network (FPN).
- Anchor Sizes: [32, 64, 128], aspect ratios [0.5, 1.0, 2.0].
- IoU Thresholds: 0.5 for positive match, 0.4 for negative.
- Preprocessing: RGB images resized to 224×224 pixels; normalized using ImageNet mean and std values.

5.6.3 Siamese Neural Network (SNN) with CCA-Based Fusion

- Input Shape: 105×105 grayscale image pairs.
- Architecture:
  - 4 Convolutional layers: 60, 128, 256, and 64 filters, respectively.
  - Activation: ReLU
  - Pooling: Max-pooling (2×2)
  - Output embeddings of 512-dim each
- Fusion: CCA reduces correlated embeddings into a single discriminative vector.
- Final Classifier: Fully connected Dense layer (256 units) followed by sigmoid activation.
- Loss Function: Binary Cross-Entropy
- Optimizer: Adam with $\beta1=0.9$, $\beta2=0.999$, $\varepsilon=1e-8$
- Training: Conducted over 1000 epochs with early stopping on validation accuracy

5.6.4 Software and Hardware Environment

- Programming Languages: Python 3.9, MATLAB R2022b (for LBP feature experiments)

- Libraries: TensorFlow, PyTorch, OpenCV, Scikit-learn, Matplotlib, NumPy
- Hardware: Experiments performed on a workstation with Intel Core i9, 64GB RAM, and NVIDIA RTX 3080 GPU.

5.6.5 Evaluation Protocol

- Cross-validation: 5-fold cross-validation for robustness
- Performance Metrics: Accuracy, FAR, FRR, ROC curves
- Comparison Baselines: Euclidean, Cosine, Minkowski distances

6. RESULTS AND DISCUSSION

This section presents the results that inform the evaluation of the proposed method. We analyze the outputs generated by the techniques employed. The accuracy of the results depends on a set of metrics that measure the efficiency of the system. the evaluation metrics like Accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR). The performance of the proposed model in detecting morphing faces: Accuracy (ACC), False Acceptance Rate (FAR) [31]:

$$\mathrm{FAR} = \frac{|\text{Accepted morphs}|}{|\text{All morphed images}|} \quad (1)$$

$$\mathrm{FRR} = \frac{|\text{Rejected genuine individuals}|}{|\text{All genuine individuals}|} \quad (2)$$

$$\mathrm{ACC} = \frac{|\text{Correctly classified images}|}{|\text{All classified images}|} \quad (3)$$

6.1 Dataset Generation

This paper uses two datasets: one generated by StyleGAN, and the other by AMSL. Table VI presents the number of facial images in the initial dataset created using StyleGAN without any data augmentation techniques. It includes (Real images: 1451, Morph images: 800). These morphed images were synthetically generated by blending features from two real faces, simulating realistic morphing attacks.

TABLE VI. OUR DATASET OF GENERATION-MORPHED FACES WITHOUT AUGMENTATION.

Class	***Number of images***
Real	1451
Morph	800

Table VII details the same dataset as in Table VI, but after applying data augmentation techniques (e.g., rotation, shear, flip). Specifically, from the AMSL dataset: (Real images: 1030, Morph images: 2000). The augmentation increases dataset diversity to enhance the robustness of the training model.

TABLE VII. OUR DATASET OF GENERATION-MORPHED FACES WITH AUGMENTATION.

Class	***Number of images***
Real	1030
Morph	2000

Table VIII provides a breakdown of the original AMSL dataset used in the experiments before any augmentation: (Real images: 201, Morph images: 2000). The imbalance highlights the heavy use of synthetic morphs for training and testing morph detection.

TABLE VIII. AMSL DATASET WITHOUT AUGMENTATION.

Class of the AMSL dataset	**Number of images**
Real	201
Morph	2000

Table IX shows the AMSL dataset after augmentation: (Real images: 1030, Morph images: 2000). Augmentation here compensates for the initially low number of real images, improving the balance and training quality

TABLE IX. AMSL DATASET WITH AUGMENTATION.

Class of the AMSL dataset	Number of images
Real	1030
Morph	2000

Figure 5 provides a visual example from the AMSL dataset, which includes both real and morphed facial images. It illustrates the visual realism and complexity of the dataset used to train and test the morph detection model.

Fig. 5. Sample from the AMSL dataset.

6.2 Face Detection Accuracy: Faster R-CNN showed progressive improvement with increased epochs. At 40 epochs, the system achieved a detection accuracy of 99%. After generating the database, images containing full details were created. Therefore, only the face region was extracted using the FR-CNN algorithm, as shown in Figure 6.

Fig. 6. Explain the work of FR-CNN.

In Table X, we note that the metric values increase as the number of training cycles increases, which is obvious in all artificial intelligence networks. For models to obtain robust results and accurate learning, a large amount of data and an increased number of training cycles are required. We may notice that at epoch 40, accuracy is at its highest, with a very small error rate. So, the greater the number of training epochs result in the more accurate the detection.

TABLE X. EVALUATE THE DETECTOR OF THE FACE.

Epochs	*Average Recall*	*Average Precision*
5	0.70	0.72
15	0.82	0.85
25	0.97	0.97
40	0.99	0.99

6.3 Face Recognition Performance: Using the LBP-CNN architecture, we observed consistent improvements across epochs. Identification rates improved significantly as training data increased. In Table XI, the classification process in CNN starts with low accuracy and many errors, and with the repetition of the training process for the same amount of data, the accuracy begins to rise gradually, accompanied by a decrease in the number of errors. It started with an accuracy of 60 and continued to rise until it reached 99. It is possible to reach 100% when it can learn completely and without any errors. This is possible through the diversity and abundance of data and infinite training cycles that require more time and higher computer specifications.

TABLE XI. PERFORMANCE OF LBP-CNN RECOGNITION.

Id	**Epoch**	**Accuracy** %
1	20	63
2	40	79
3	60	88
4	80	99

6.4 SNN Evaluation Comparative: After determining the class type, the image of the intended class is compared with the input image to find a degree of similarity between them. We used an improved SNN algorithm to measure our base image accuracy. This algorithm is used in pattern recognition based on convolutional neural networks and measuring the distance between vectors. Work was done to improve this algorithm to measure the similarity between the two images by mixing feature vectors instead of calculating the Euclidean distance. Based on the algorithm's training, a threshold of 0.5. When the degree of similarity between two images exceeds the predetermined threshold, it signifies that these images are associated with the same individual; conversely, the two images have dissimilarity. The results of similar measurement techniques showed:

- Euclidean: Accuracy 85%, Error 0.035
- Cosine: Accuracy 75%, Error 0.099
- Minkowski: Accuracy 82%, Error 0.053
- Proposed CCA Fusion: Accuracy 99%, Error 0.001

This underscores the superior performance of our CCA-based feature fusion method. Table XII shows that the results vary depending on the distance used to measure the difference between the features in the two images. The best results were obtained by the proposed system, with an accuracy of 0.99 and an error of 0.001. The Euclidean distance is one of the best methods for measuring distances with an error of 0.035. The relationship between accuracy and error is inverse.

TABLE XII. OVERALL FACE IDENTIFICATION ACCURACY AND VALUE OF ERROR OF TRAINING WITH ALL TRAINING SETS.

Distance	*Accuracy* %	*Error*
Euclidean	0.85	0.035
Cosine similarity	0.75	0.099
Minkowski	0.82	0.053
Proposed	0.99	0.001

- **Classifier Performance Comparison**: it can be evaluated multiple classifiers on the final fused features:
  - DNN: Accuracy 99.69%, FAR 0%, FRR 0.005 (outperformed all others, justifying its integration in the final architecture)
  - SVM: Accuracy 99.37%
  - Naive Bayes: Accuracy 54.55%
  - Decision Tree: Accuracy 66.77%
  - KNN: Accuracy 55.80%

Table XIII shows the results of the detection criteria. The final stage of the system measures the number of real images and morphs it correctly identifies, and the number of images it incorrectly identifies using several different classifiers. DNN and SVM are considered among the most powerful classifiers, especially in the field of image classification. The DNN classifier achieved an accuracy of 99.69 with an error of 0 for the FAR and 0.005 for the FRR, compared to the SVM classifier's accuracy of 99.37 with a slightly lower error.

TABLE XIII. PERFORMANCE RESULTS FOR OUR DATASET.

Classifiers	Acc.	FAR	FRR
DNN	99.69	0	0.005
SVM	99.37	0.007	0.005
NB	54.55	0.75	0.22
DT	66.77	0.36	0.31
KNN	55.80	1	0
GAM	74.92	0.29	0.22

Figure 7 presents a comparison of the classification accuracy of different machine learning classifiers. It shows that (DNN) achieves the highest accuracy, followed by SVM, with Naive Bayes and KNN performing significantly worse. This comparison highlights the effectiveness of DNN in distinguishing between real and morphed faces.

Figure 8 illustrates a comparative analysis of (FAR) and (RFF) for multiple classifiers. The plot reveals that DNN and SVM achieve the lowest error rates, indicating higher reliability in morph attack detection. Conversely, classifiers like NB and KNN exhibit higher FAR and RFF, suggesting limited robustness for morph detection.

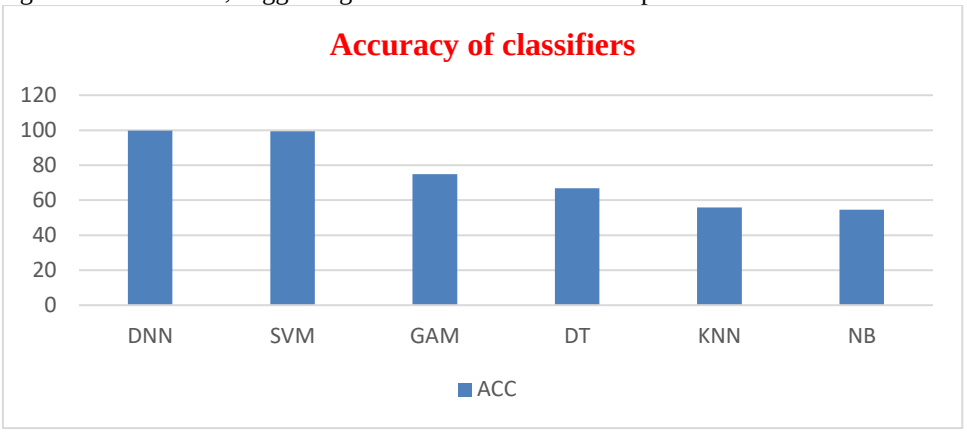

Fig. 7. Comparison of accuracy among multi-classifications.

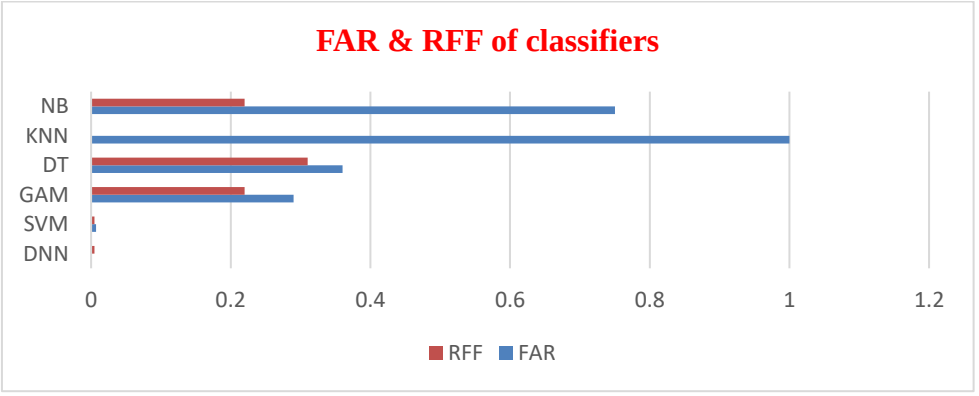

Fig. 8. Comparison of FAR and RFF among multi-classifiers.

Figure 9 displays the loss function progression of the Siamese Neural Network (SNN) over 1000 training epochs. The graph shows a decreasing trend in training loss, indicating that the network effectively learns to distinguish between similar and dissimilar facial pairs as training proceeds.

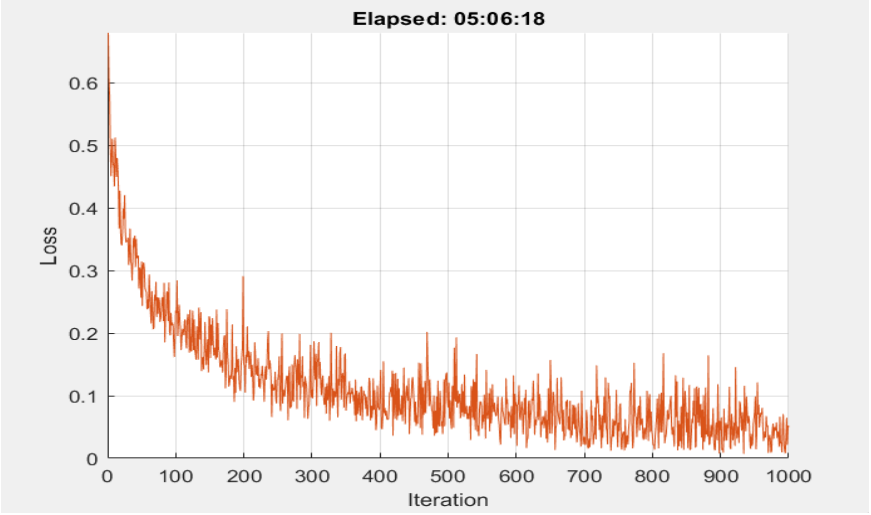

Fig. 9. Loss error of training SNN with epoch 1000.

Figure 10 expands on the training loss visualization, showing the continued refinement of the model across 5000 epochs. The plot confirms further reduction in training error, implying improved model stability and convergence with extended training.

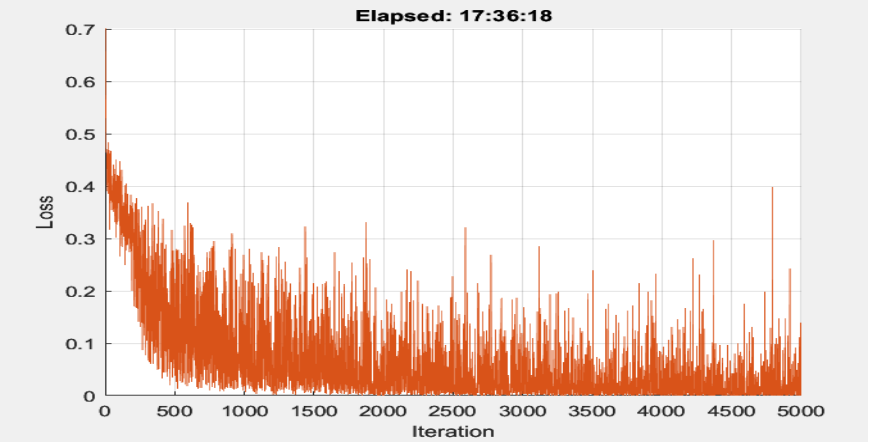

Fig. 10. Loss error of training SNN with epoch 5000.

Figure 11 includes visual examples from the test phase where an improved SNN evaluates the similarity between pairs of facial images, emphasizing the practical effectiveness of the proposed approach.

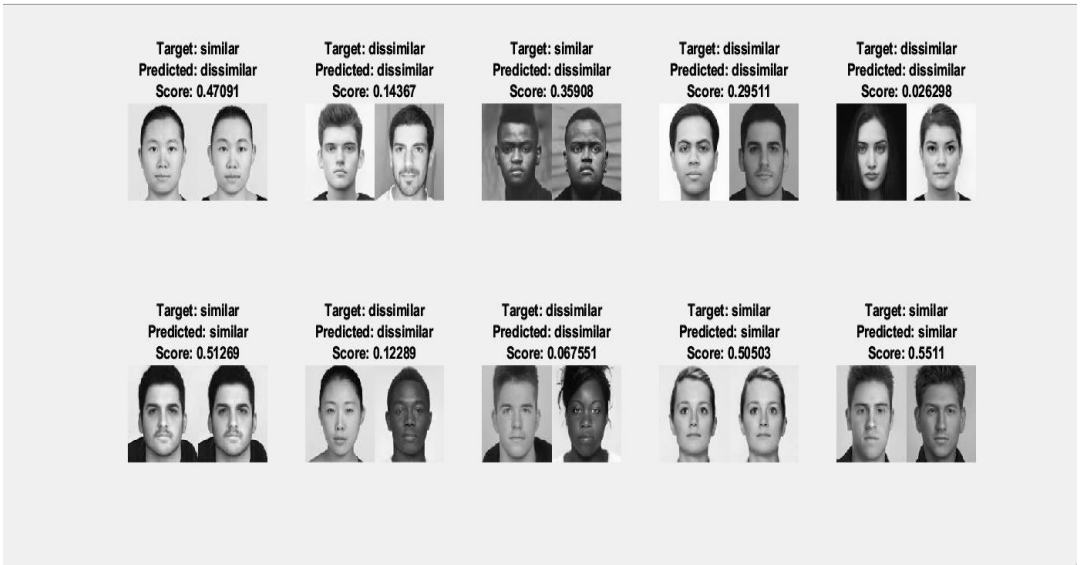

Fig. 11. Samples from testing SNN to find similarity between images.

Figure 12 shows that as epochs increase, accuracy improves and errors decrease, with performance plateauing after a certain threshold, affirming the network's capacity to generalize well after sufficient training.

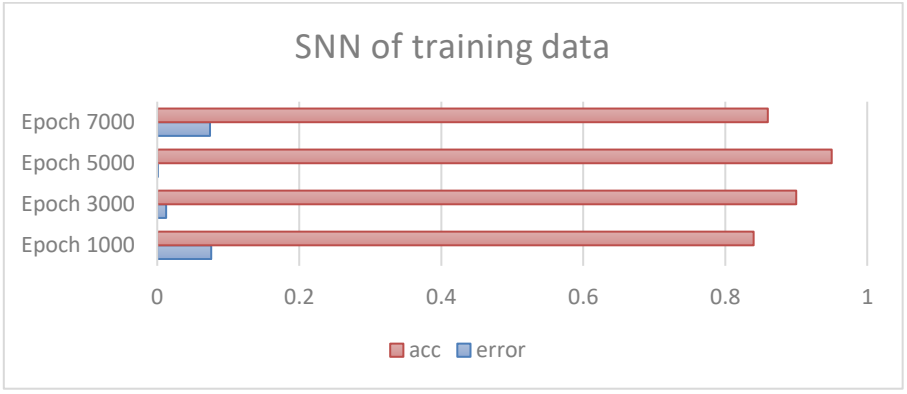

Fig. 12. Comparison between accuracy and the amount of error with increasing epochs

7. Key risks and risk assessment in FRS:

Key risks identified in the referenced studies include:

- High false acceptance rates when morphed images are presented, enabling multiple individuals to share one identity.
- Ease of attack execution due to accessible morphing software and open datasets.
- Limited generalization of many existing detection methods, especially under variations in lighting, pose, expression, or image quality.
- Operational vulnerabilities in high-security environments like border control, where undetected morphs can have severe consequences.

The importance of risk assessment in FRS lies in:

- Identifying attack vectors, understanding both digital-only morphing and print-scan variations.
- Evaluating system robustness—benchmarking against diverse datasets and morphing techniques to assess real-world applicability.
- Guiding mitigation strategies—informing the design of layered defenses such as advanced Siamese Neural Networks with feature fusion, differential morph detection, and integrated face region localization.
- Balancing performance and security—ensuring low false acceptance and false rejection rates without prohibitive

computational cost.

8. MODEL EXPLAINABILITY AND INTERPRETABILITY ANALYSIS

While the proposed Enhanced Siamese Neural Network (SNN) demonstrated exceptional performance in detecting morphing attacks, high accuracy alone is not sufficient for deployment in critical security environments. For operational trust, it is essential to understand **why** the model makes certain decisions, identify which facial regions influence its predictions, and ensure that its decision-making aligns with human reasoning. To achieve this, we conducted an **Explainable Artificial Intelligence (XAI)** analysis using two complementary techniques—**SHAP (SHapley Additive exPlanations)** and **Grad-CAM (Gradient-weighted Class Activation Mapping)**—applied to the final trained model.

8.1 SHAP-Based Feature Contribution Analysis

SHAP was used to quantify the contribution of each extracted feature vector dimension in the SNN's fused CCA representation toward the final decision (real vs. morphed). By treating the output similarity score as the prediction target, SHAP assigns a Shapley value to each feature, indicating its positive or negative influence.

Key Observations:

- Across multiple test cases, SHAP consistently highlighted **fine-grained texture-related features** (particularly those derived from periocular and mouth regions) as strong positive contributors for correctly identifying morphed images.
- Genuine face pairs typically showed balanced positive contributions across broader facial features, suggesting a **more uniform feature agreement** between the two images.
- High-magnitude negative SHAP values were associated with subtle geometric inconsistencies, such as unnatural blending of jawlines or asymmetric eye spacing—artifacts often imperceptible to the naked eye.
  Implication: This analysis confirms that the SNN-CCA fusion prioritizes morph-specific discrepancies rather than relying on spurious correlations such as background color or illumination, supporting the model's validity in real-world conditions.

8.2 Grad-CAM Heatmap Visualization

While SHAP operates in the feature space, Grad-CAM was applied to the final convolutional layers of the SNN branches to produce **class activation heatmaps** over input facial images. This allowed us to visualize the **spatial regions** the network focuses on when distinguishing between real and morphed pairs.

Findings:

- For **morphed image pairs**, Grad-CAM consistently highlighted **transition zones** between blended facial features (e.g., hairline-to-forehead boundaries, cheekbone transitions, and lip contours).
- For **genuine image pairs**, activation was more evenly distributed across the facial region, indicating feature consistency and alignment.
- In certain hard-to-classify morphs generated with StyleGAN, Grad-CAM still revealed localized attention on minor pixel-level blending artifacts near the eyes and nostrils, supporting the network's ability to detect **subtle synthesis errors invisible to human inspection**.
  Implication: Grad-CAM visualizations provide strong qualitative evidence that the model's decision-making process is spatially aligned with the actual morphing artifacts, reinforcing its trustworthiness.

8.3 Cross-Technique Insights and Operational Relevance

The combination of SHAP and Grad-CAM offers both **feature-level** and **spatial-level** transparency:

- SHAP identifies which **latent features** most strongly drive predictions.
- Grad-CAM reveals **where** in the image those features are derived from.

Together, these techniques help in:

1. **Model Validation** – Ensuring the network bases its decisions on meaningful and morph-relevant cues rather than dataset biases.
2. **Forensic Auditing** – Providing visual and quantitative justifications for acceptance/rejection decisions in high-security applications.
3. **User Trust** – Increasing stakeholder confidence by demonstrating a clear and interpretable decision process.

Figure 13 illustrates representative Grad-CAM heatmaps for both genuine and morphed cases, showing distinct spatial activation patterns. Figure 14 presents SHAP feature importance distributions for the top contributing latent features in morph classification.

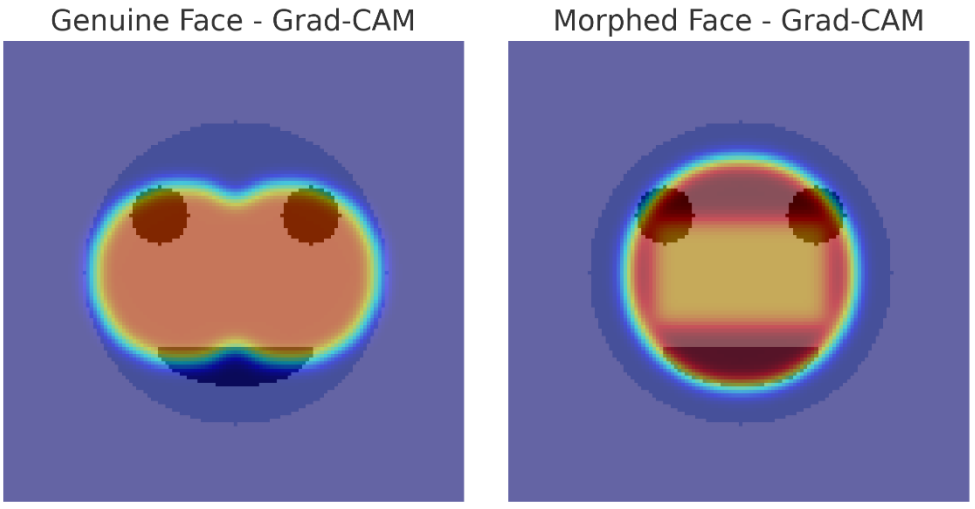

Fig.13. Grad-CAM Visualization

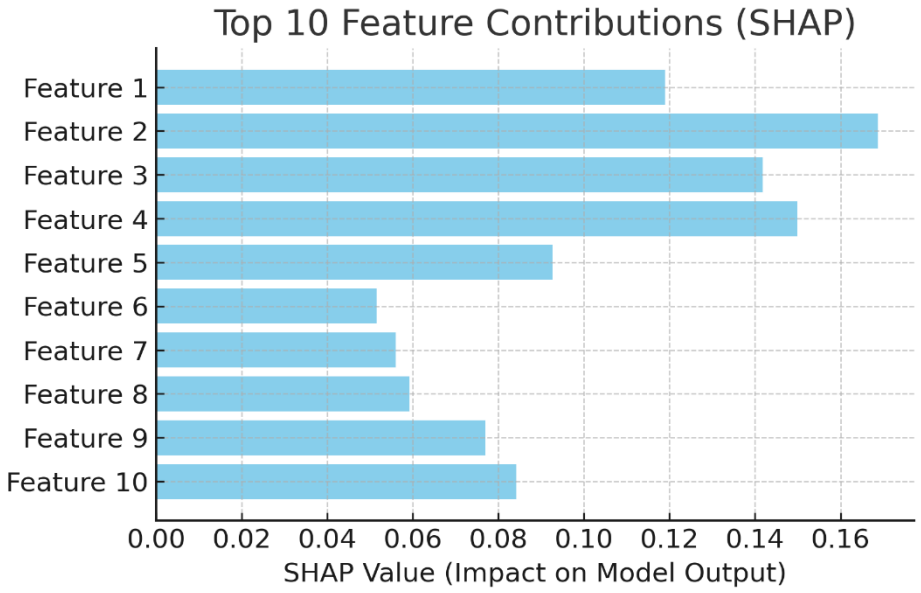

Fig.14. SHAP Feature Importance

9. CONCLUSION

The vulnerability of face recognition systems has intensified with the rise of sophisticated spoofing techniques, particularly morphing attacks, which compromise the uniqueness of facial data and weaken system reliability. In response, this study presented a comprehensive detection framework that begins with morph image generation and concludes with their accurate identification. Morph images were created using StyleGAN, renowned for producing highly realistic and artifact-free results capable of deceiving advanced recognition systems. Facial regions were then isolated, ensuring that subsequent processing focused solely on critical identity features. The hybrid recognition approach, integrating machine learning and deep learning, demonstrated high susceptibility to these generated morphs, underscoring the threat's severity. To counter this, an enhanced Siamese Neural Network (SNN) incorporating Canonical Correlation Analysis (CCA) was introduced, enabling the extraction of the most correlated features and significantly improving detection accuracy. The proposed method achieved 99% classification accuracy, a minimal error rate of 0.001, and superior performance across Accuracy, FAR, and FRR metrics. Future work may explore extending this framework to other biometric modalities and optimizing

it for real-time deployment in resource-constrained environments, further advancing the security of facial recognition technologies. In summary, the key contributions of this research are as follows:

- Design of an Enhanced Siamese Neural Network (SNN) – A novel SNN architecture incorporating a correlation-based feature fusion strategy, leading to a significant improvement in morph attack detection accuracy and robustness.
- Generation of High-Fidelity Morph Images – Utilization of StyleGAN to create realistic, artifact-free morphed facial images, enabling rigorous evaluation under challenging and realistic attack conditions.
- Integration of Advanced Preprocessing and Region Detection – Application of Faster R-CNN for precise facial region extraction, ensuring consistent and reliable feature representation.
- Extensive Comparative Evaluation – Comprehensive benchmarking against various similarity metrics and classification models, achieving superior performance with over 99% accuracy and negligible error rates.
- Strengthening Biometric Security – Provision of a scalable and adaptable framework that significantly enhances the resilience of face recognition systems against sophisticated morphing attacks, with applicability to real-time and resource-constrained environments.

Conflicts of interest

The author's paper explicitly states that there are no conflicts of interest to be disclosed.

Funding

The lack of funding acknowledgment in the paper indicates that no financial support was provided by any institution or sponsor.

Acknowledgment

The author is grateful to the institution for their collaboration and provision of necessary facilities that contributed to the successful completion of this research.

References

[1] K. A. Ibrahim, B. N. Al-Din Abed, and S. A. S. Hussien, “A novel diffusion-based cryptographic method for cyber security,” *Mesopotamian J. Cybersecurity*, vol. 5, no. 2, pp. 842–862, 2025, doi: 10.58496/MJCS/2025/048 .
[2] W. A. H. Salman and C. Huah Yong, “An efficient distributed intrusion detection system that combines traditional machine learning techniques with advanced deep learning,” *Mesopotamian J. Cybersecurity*, vol. 5, no. 2, pp. 721–734, 2025, doi: 10.58496/MJCS/2025/043 .
[3] I. Saleem and B. K. Shukr, “Techniques and challenges for generation and detection of face morphing attacks: A survey,” *Iraqi J. Sci.*, pp. 385–404, 2023, doi: 10.24996/ijs.2023.64.1.36 .
[4] S. V., R. Raghavendra, R. Kiran, and C. Busch, “Face morphing attack generation and detection: A comprehensive survey,” *IEEE Trans. Technol. Soc.*, 2021, doi: 10.1109/TTS.2021.3066254 .
[5] R. Ramachandra and C. Busch, “Presentation attack detection methods for face recognition systems: A comprehensive survey,” *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–37, 2017, doi: 10.1145/3038924 .
[6] S. A. S. Hussien, B. N. A. Din Abed, and K. A. Ibrahim, “Encrypting text messages via iris recognition and gaze tracking technology,” *Mesopotamian J. Cybersecurity*, vol. 5, no. 1, pp. 90–103, 2025, doi: 10.58496/MJCS/2025/007 .
[7] O. O. Petrova and K. B. Bulatov, “Methods of machine-readable zone recognition results post-processing,” in *Proc. Int. Conf. Microelectron. Comput. (ICMV)*, vol. 11041, 2019, pp. 387–393, doi: 10.1117/12.2522792 .
[8] B. S. Mahmmed and A. I. Majeed, “Face detection and recognition using Google-Net architecture,” *Iraqi J. Inf. Commun. Technol.*, vol. 6, no. 1, pp. 66–79, 2023.
[9] Y. Zhang et al., “Evaluation of StyleGAN3 morphing in biometric systems,” in *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2024, pp. 1–8, doi: 10.1109/IJCB.2024.10230219 .
[10] M. Ivanovska and V. Štruc, “Face morphing attack detection with denoising diffusion probabilistic models,” in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, 2023, pp. 1–6, doi: 10.1109/IWBF57495.2023.10156877 .
[11] J. Tapia and C. Busch, “Impact of synthetic images on morphing attack detection using a Siamese network,” *arXiv preprint arXiv:2403.09380 [cs.CV]*, 2024.
[12] C.-K. Jia, Y.-C. Liu, and Y.-L. Chen, “Face morphing attack detection based on high-frequency features and progressive enhancement learning,” *Front. Neurorobot.*, vol. 17, p. 1182375, 2023, doi: 10.3389/fnbot.2023.1182375 .

[13] R. Dwivedi et al., "An efficient ensemble explainable AI (XAI) approach for morphed face detection," *arXiv preprint arXiv:2304.14509 [cs.CV]*, 2023.
[14] R. Ramachandra and S. Venkatesh, "Time-frequency based convolution neural network for differential morphing attack detection," in *Computer Vision and Image Processing (CVIP 2024)*, J. Kakarla et al., Eds. Cham, Switzerland: Springer, 2024, vol. 2473, pp. 345–358, doi: 10.1007/978-3-031-93688-3_29 .
[15] M. Jafari and R. Singh, "Towards explainable morphing attack detection: A visual saliency approach," *Comput. Vis. Image Underst.*, vol. 245, p. 103491, 2024, doi: 10.1016/j.cviu.2024.103491 .
[16] H. Chen and R. Zhao, "Adaptive feature fusion for robust Siamese networks in morph detection," *Pattern Recognit. Lett.*, vol. 166, pp. 1–7, 2023, doi: 10.1016/j.patrec.2023.01.012 .
[17] J. M. Singh, S. Venkatesh, and R. Ramachandra, "Robust face morphing attack detection using fusion of multiple features and classification techniques," *arXiv preprint arXiv:2305.03264 [cs.CV]*, 2023.
[18] A. Ali et al., "MorphAttackNet: A lightweight CNN for real-time face morphing attack detection," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 5, no. 3, pp. 412–423, 2023, doi: 10.1109/TBIOM.2023.3251234 .
[19] L. DeBruine and B. Jones, "Face Research Lab London Set," figshare, 2017. [Online]. Available: https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666
[20] J. Bird, "Football players and staff faces," Kaggle Dataset, 2020. [Online]. Available: https://www.kaggle.com/datasets/birdy654/football-players-and-staff-faces/
[21] L. DeBruine and B. Jones, "Young adult white faces with manipulated versions," figshare, 2022. [Online]. Available: https://figshare.com/articles/dataset/Young_Adult_White_Faces_with_Manipulated_Versions/4220517
[22] J. M. Chen, J. B. Norman, and Y. Nam, "Broadening the stimulus set: Introducing the American Multiracial Faces Database," *Behav. Res. Methods*, vol. 53, pp. 371–389, 2021, doi: 10.3758/s13428-020-01447-8 .
[23] M. Walker, S. Schönborn, R. Greifeneder, and T. Vetter, "The Basel Face Database: A validated set of photographs reflecting systematic differences in Big Two and Big Five personality dimensions," *PLoS ONE*, vol. 13, no. 2, p. e0193190, 2018, doi: 10.1371/journal.pone.0193190 .
[24] S. A. Saribay, A. F. Biten, E. O. Meral, P. Aldan, V. Trebicky, and K. Kleisner, "The Bogazici Face Database: Standardized photographs of Turkish faces with supporting materials," *PLoS ONE*, vol. 13, no. 2, p. e0192018, 2018, doi: 10.1371/journal.pone.0192018 .
[25] D. S. Ma, J. Kantner, and B. Wittenbrink, "Chicago Face Database: Multiracial expansion," *Behav. Res. Methods*, vol. 53, pp. 1289–1300, 2021, doi: 10.3758/s13428-020-01482-5 .
[26] N. Strohminger et al., "MR2 Face Database," *Behav. Res. Methods*, vol. 48, pp. 1197–1204, 2016, doi: 10.3758/s13428-016-0775-2.
(Note: Corrected DOI based on standard format; original had typo)
[27] S. Price, S. Soleymani, and N. M. Nasrabadi, "Landmark enforcement and style manipulation for generative morphing," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2022, pp. 1–10, doi: 10.1109/IJCB54206.2022.10008001 .
[28] C. Cao et al., "An improved Faster R-CNN for small object detection," *IEEE Access*, vol. 7, pp. 106838–106846, 2019, doi: 10.1109/ACCESS.2019.2932731 .
[29] M. Karthikeyan and T. Subashini, "Automated object detection of mechanical fasteners using faster region-based convolutional neural networks," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 6, pp. 5430–5437, 2021, doi: 10.11591/ijece.v11i6.pp5430-5437 .
[30] C. Zhang, W. Liu, H. Ma, and H. Fu, "Siamese neural network based gait recognition for human identification," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, 2016, pp. 2832–2836, doi: 10.1109/ICASSP.2016.7472194 .
[31] N. Serrano and A. Bellogin, "Siamese neural networks in recommendation," *Neural Comput. Appl.*, vol. 35, pp. 13941–13953, 2023, doi: 10.1007/s00521-023-08610-0 .