Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 1, February 2026, pp. 755~769
ISSN: 2302-9285, DOI: 10.11591/eei.v15i1.10789

A multimodal framework for secure digital document fortification using Morse code and biometric watermarking

Tresa Maria Josylin[1], Ganeshayya Shidaganti[2], Vishwachetan Dasegowda[2], Anasuya Jadagerimath[3], Prakash Sheelvanthmath[4]

[1]Department of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru, India
[2]Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India
[3]Department of Artificial Intelligence and Machine Learning, Don Bosco Institute of Technology, Bengaluru, India
[4]Department of Computer Science, School of Engineering, Dayananda Sagar University, Bengaluru, India

Article Info

Article history:

Received May 31, 2025
Revised Oct 10, 2025
Accepted Dec 6, 2025

Keywords:

Biometric watermarking
Convolutional neural network
Morse code authentication
Multi-layered authentication
Multi-task cascaded convolutional neural network
Rubik's encryption

ABSTRACT

In an era of escalating cybersecurity threats, traditional authentication methods become more susceptible to attacks like phishing, brute force, and identity theft. With the aim to counter these difficulties, this paper introduces a multi-layered authentication that merges facial recognition, eye-tracking based Morse code verification, biometric verification using convolutional neural network (CNN) and cryptographic watermark with Rubik's encryption. The document fortification system proposed here improves security by integrating biometric authentication, behavioral verification, and encryption-based watermarking to provide both user authentication and document integrity. The authentication process begins with facial recognition, where multi-task cascaded convolutional neural network (MTCNN) detects facial features and FaceNet generates unique embeddings for identity verification. Upon successful authentication, users input a Morse code password via an eye-blinking mechanism, which is decoded and validated. Additionally, fingerprint and iris recognition using CNN models further enhance security. The Rubik's encryption algorithm secures biometric watermarks within digital documents, preventing tampering. An one-time password (OTP)-based re-authentication mechanism ensures only authorized users can access encrypted files. Experimental results demonstrate the system's high accuracy and resilience against security threats, making it a robust and scalable authentication framework. This research highlights the potential of multi-factor authentication (MFA) in modern cyber-security, offering a future-ready solution for securing sensitive digital documents such as images and pdf files.

Corresponding Author:

Ganeshayya Shidaganti
Department of Computer Science and Engineering, Ramaiah Institute of Technology
Bengaluru, Karnataka, India
Email: ganeshayyashidaganti@msrit.edu

1. INTRODUCTION

The growing use of online platforms for communication, record-keeping, and transactions has increased the need for reliable authentication mechanisms and document security. The commonly used password-based authentication schemes are greatly vulnerable to cyberattacks in the form of phishing, brute-force, and credential compromise. These vulnerabilities have sparked an increased interest in multi-factor authentication (MFA) methods [1], which integrate a combination of several layers of security to improve security from unauthorized entry. Current authentication models are largely based on either password-based

systems, single-factor biometric authentication, or conventional digital watermarking. These methods have several disadvantages: i) vulnerabilities in passwords: passwords can be hacked, and reuse of passwords [2] on several systems raises security concerns, ii) limitations of single-layer biometric authentication: independent biometric systems may be spoofed [3] or tampered with, causing identity theft, and iii) weaknesses of basic watermarking: conventional watermarking methods [4] offer weak encryption and are vulnerable to tampering or removal by unauthorized parties.

These drawbacks underscore the necessity for a strong, multi-layered authentication system that combines several verification methods to provide greater security, tamper resistance, and convenient access control. To overcome these constraints, this study suggests a document fortification system, which combines facial recognition, Morse code-based password input, multimodal biometric authentication (iris and fingerprint), and cryptographic watermarking to enhance security and access control of digital documents including images and pdf files. This work presents a novel, multi-layered security framework that enhances authentication and document integrity. The primary contributions of this work are: i) creation of a multi-modal authentication system, combining facial recognition, Morse code-based password input, and biometric authentication (iris and fingerprint), ii) use of biometric watermarking through encryption of user biometric information and embedding it within digital documents for increased authenticity, iii) implementation of a re-authentication system, where users must authenticate themselves before decrypting or viewing the document, vi) leveraging high-level cryptographic mechanisms, such as Rubik's encryption for encrypting biometric templates and one-time password (OTP)-based authentication for extra security, and v) use of machine learning models, such as multi-task cascaded convolutional neural network (MTCNN) for face recognition, facial landmark tracking for entering Morse code, convolutional neural network (CNN) for biometric identification, and deep-learning-based watermarking mechanisms for stronger security.

By layering physiological, behavioral, and cryptographic elements, the proposed system significantly raises the barrier for unauthorized access and manipulation of sensitive data. The design of this system aims to strike a balance between usability, resilience, and scalability, ensuring that legitimate users can authenticate seamlessly while maintaining stringent protection against attackers.

2. RELATED WORKS

The increasing demand for secure authentication systems has led to significant advancements in Morse code-based authentication, biometric watermarking, and multimodal biometric security. Morse code-based authentication uses eye-blink patterns or touch inputs to create secure passwords, improving accessibility for disabled users. Recent developments incorporate AI-based signal detection and real-time processing for enhanced security and usability. Nayak *et al.* [5] proposes a gaze-based Morse code authentication system using real-time eye tracking and face recognition for hands-free security. Wang *et al.* [6] constructed a versatile tactile sensor based on carbon nanotube/polyurethane sponge (CNT/PUS) material for accurate Morse code identification. This approach significantly enhances accessibility, particularly for users with motor impairments. Their model with long short-term memory (LSTM) provided high accuracy rates (99.17% for digits, 95.37% for characters), proving effective capture of tactile features. A gaze-based Morse code authentication system was proposed [7], utilizing Morse net with shared convolutions and a convolutional recurrent neural network (CRNN) for real-time personal identification number (PIN) entry through eye tracking, achieving state-of-the-art results on simulated datasets, though performance may be affected by inconsistent eye movements and complex backgrounds. Sushmitha *et al.* [8] proposed a real-time eye-blink detection algorithm using image processing to convert intentional blinks into Morse code, enabling secure, non-verbal communication. Biometric watermarking places distinctive biometric marks (e.g., fingerprints, iris scans, and facial features) within digital documents for guaranteeing authenticity and tamper resistance. Sophisticated methods employ zero-bit watermarking as well as multimodal biometric fusion for robust security. Singh *et al.* [9] proposed a robust multimodal biometric watermarking system combining fingerprint and face recognition to enhance digital image security without compromising quality. The approach focuses on developing efficient embedding and extraction algorithms for secure identity verification. Deepika *et al.* [10] proposed a zero-bit watermarking technique for biometric images, such as iris scans, that embeds unique identifiers without altering the original data. This method ensures data integrity and security while remaining imperceptible and resistant to tampering or identity forgery. Fernandez and Nithyanandam [11] developed a multimodal biometric watermarking framework using T-norm-based fusion, enhancing watermark robustness against compression and noise, making it suitable for secure online authentication and digital forensics. Singh *et al.* [12] introduced a watermarking system for multimodal medical images (magnetic resonance imaging (MRI) and computed tomography (CT) scans) to ensure confidentiality and integrity in telehealth, preventing unauthorized access to sensitive data. Multimodal biometric authentication combines multiple biometric traits (e.g., face, iris, and

fingerprints) to improve verification accuracy and fraud detection. Deep learning-driven feature fusion techniques enhance recognition performance and robustness. Li *et al*. [13] analyzed hand-based multimodal biometric fusion techniques, focusing on feature, score, and decision-level fusion to enhance accuracy and robustness. Alay and Al-Baity [14] suggested a multimodal biometric recognition system that combines iris, face, and finger vein authentication based on CNNs. Their model showed high accuracy rates. Behavioral biometrics examine user-specific behavior (e.g., mouse movements, touchscreen usage, and keystroke dynamics) for verification. Soft-biometric characteristics like age, gender, and facial texture enhance the accuracy of recognition when used together with conventional biometrics. Terhörst *et al*. [15] demonstrated that incorporating soft-biometrics into facial embeddings enhances identity verification and spoof resistance, though scalability and demographic diversity pose ongoing challenges. Nnamoko *et al*. [16] presented a large dataset of behavioral biometrics, such as keyboard, mouse, and touchscreen dynamics, gathered using a graphical user interface (GUI) application mimicking online card payments. The dataset is a basis for creating sophisticated behavioral biometric models. Hybrid security systems combine biometric verification with sophisticated cryptographic methods for increased data security. These methods offer more secure encryption keys and unauthorized access resistance, allowing secure transmission of biometric data. Khudzaifah *et al*. [17] proposed a hybrid security mechanism that combined Rubik's Cube algorithms with RSA encryption to secure the transmission of iris digital images. They used exclusive encryption keys derived from Rubik's Cube settings, which will make it harder for unauthorized persons to access. The research shows enhanced security encryption, but more research should be carried out to check its applicability in everyday use and its effectiveness against conventional encryption methods. The survey of recent advancements in biometric recognition systems reveals significant progress in enhancing security and user identification through innovative techniques. Moreover, recent studies emphasize the effectiveness of combining three or more modalities for multifactor authentication to increase resistance against spoofing and single-point failures. Adaptive or fallback MFA mechanisms have also been explored to dynamically switch between biometric traits (e.g., from facial recognition to eye blinks or fingerprints) based on context or user ability [18], [19]. Fusion of visual (face, iris, and fingerprint), behavioral biometrics (eye blink and keystroke dynamics) has shown to improve recognition accuracy and system robustness [20], supporting the multimodal integration approach adopted in our work.

3. PROPOSED METHOD

The traditional authentication methods are prone to brute force attacks, phishing attacks, biometric spoofing and credential leakages. To address these shortcomings, a multimodal authentication mechanism is proposed that ensures only authorized users have the access and verify of sensitive digital documents (image and pdfs) and prevent unauthorized access and document forgery. We propose a methodology that combines various approaches to biometric data security and authentication: face recognition using MTCNN, Morse code authentication, fingerprint, and iris classification using CNNs, Rubik's Cube encryption and decryption and an OTP-based authentication. The user is first validated using face recognition and Morse code-based password input. Upon success, fingerprint and iris data are validated using CNN-based classifiers. The extracted biometric information is encrypted using the Rubik's Cube encryption algorithm and then embedded into digital documents using least significant bit (LSB) steganography. An OTP is then sent to the user's registered device for real-time re-authentication before granting document access. A visual representation of the architecture is provided in Figure 1.

3.1. Face recognition

The primary authentication mechanism in this work is facial recognition, ensuring security and user verification. The system leverages deep learning-based face recognition techniques, combining MTCNN for face detection and FaceNet for feature extraction and identity matching. Capturing real-time facial images and developing unique embeddings of facial features allows the system to effectively distinguish authorized users from impostors.

3.1.1. Face detection using multi-task cascaded convolutional neural network

Multi-task MTCNN is a deep learning-based face detection algorithm that efficiently detects faces and their key landmarks such as eyes, nose and mouth. MTCNN is a sequence of three sequential convolutional networks that each refines the face detection results. The face detection pipeline consists of three stages as shown in Figure 2. The proposal network [P-Net] scans the image at multiple scales, generating face proposals with bounding boxes and confidence scores, with non-maximum suppression (NMS) removing redundant proposals. The refine network [R-Net] then refines these bounding boxes, classifies face and non-face regions, and improves [21] localization accuracy. Finally, the output network

[O-Net] further refines detections and performs fine facial landmark detection, identifying key features like the eyes, nose, and mouth for alignment, recognition, and biometric authentication.

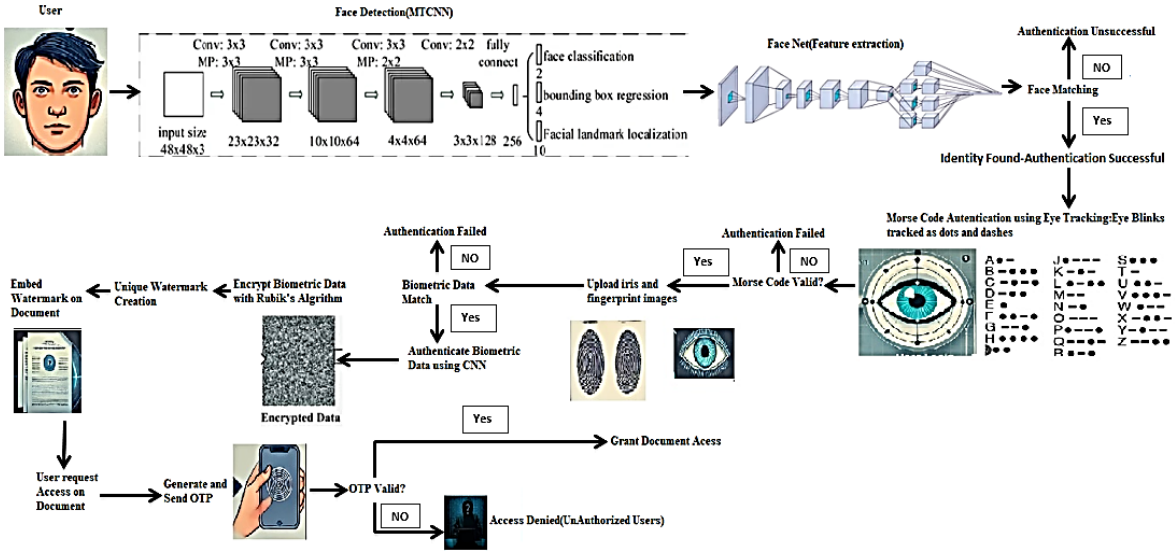


Figure 1. System architecture diagram of multilayered security framework

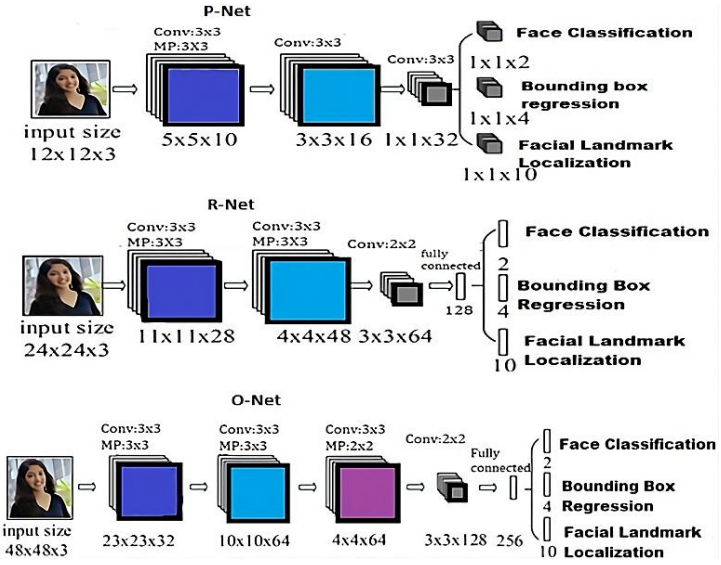


Figure 2. MTCNN architecture

3.1.2. Feature extraction using FaceNet

FaceNet [22] takes a detected face and returns a 128-dimensional feature vector (known colloquially as a face embedding) as each of which represents a unique numerical representation of the individual 's facial structure, such that the system can recognize a distinct identity between different identities. Mathematically, given an input facial image X, FaceNet transforms it into an embedding f(X)**,** represented as (1):

$$f(X) \in \mathbb{R}^{128} \quad (1)$$

where, f(X) is a 128-dimensional feature vector that uniquely encodes the facial characteristics. To verify a user's identity, the extracted face embedding is compared with stored embeddings in the database. The Euclidean distance between two embeddings determines their similarity. Given two facial embeddings, $f(X_1)$

[feature vector of the input face] and f(X_2) [feature vector of the stored face], their similarity score is computed as (2):

$$d(X_1, X_2) = ||f(X_1) - f(X_2)||_2 \quad (2)$$

Decision rule for identity matching:
- If d (X_1, X_2) <τ (where τ is the predefined threshold), then X1 and X2 belong to the same identity → authentication successful.
- If d (X_1, X_2) ≥τ, the system classifies the user as Unknown, prompting additional verification.

3.2. Morse code authentication using eye tracking

Morse code authentication introduces a new, non-traditional and secure method of user authentication using eye-tracking technology to input Morse code passwords. The implementation of this method provides a higher level of security by requiring an input of a unique Morse code sequence. Morse code is a binary encoding that represents each character using a unique set of dots (•) which represent quick blink/tap and dashes (−) which represent prolonged blink/tap. Each Morse code sequence is time-dependent, meaning the duration of a signal is a critical factor in differentiating between dots and dashes and is represented in (3):

$$Ts = \sum_{i=1}^{n} Ti + \sum_{j=1}^{m} Gj \quad (3)$$

where, T_i represents the duration of dots and dashes and G_j represents the spacing between elements, characters, and words. This ensures that the system accurately detects and interprets user input based on timing thresholds. The Table 1 represents various characters and Morse code associated with it. Aspect ratio is critical for detecting and distinguishing between dots (•) and dashes (-) based on eye blinks.

Table 1. Morse code table

Character	Morse code	Character	Morse code	Character	Morse code	Character	Morse code
A	.-	B	-...	C	-.-.	D	-..
E	.	F	..-.	G	--.	H	....
I	..	J	.---	K	-.-	L	.-..
M	--	N	-.	O	---	P	.--.
Q	--.-	R	.-.	S	...	T	-
U	..-	V	...-	W	.--	X	-..-
Y	-.--	Z	--..	0	-----	1	.----
2	..---	3	...--	4	....-	5	.....
6	-....	7	--...	8	---..	9	----.
. (Dot)	.-.-.-	, (Comma)	--..--	? (Q-Mark)	..--..	Space	*

As the aspect ratio of the eye opening is related to blink duration, it is critical for accurately mapping Morse code sequences. The eye aspect ratio (EAR) [23] is a mathematically well-known measure of openness of the eye and is calculated using the Euclidean distances between eye landmark points detected by Dlib's facial landmark detector. Dlib's facial landmark model detects eight major facial features including eyes, eyebrows, nose and lips, and for eye tracking it uniquely identifies six key landmark points per eye. The facial landmarks defining the eye region as shown in Figure 3 where P1, P2, and P3 (upper eyelid points), P4, P5, and P6 (lower eyelid points).

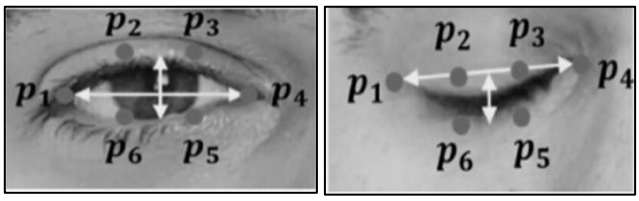


Figure 3. Eye opening and closing landmarks

The EAR formula is defined as in (4):

$$EAR = \frac{||P2-P6|| + ||P3-P5||}{2 \times ||P1-P4||} \quad (4)$$

where, ||P2-P6||+||P3-P5|| represent vertical distances between eyelids and ||P1-P4|| represent horizontal distance between the outer corners of the eye. Lower EAR value indicates that eye closing. The blinking ratio helps detect if the eyes are open or closed and is computed using (5):

$$Blink\ Ratio = \frac{Horizontal\ Eye\ Distance}{Vertical\ Eye\ Distance} \quad (5)$$

where,

- Horizontal eye distance → distance between the outermost eye landmarks.
- Vertical eye distance → distance between upper and lower eyelid landmarks.

This ratio helps detect if the eyes are open or closed. The system calculates the blink duration time T_b between eye closure and reopening. If Tb<=T, register a dot(.) else If Tb>=3T, register a dash (-). Morse code-based authentication provides many advantages over most existing password systems, the main benefits being the following: security; improved accessibility Morse code includes a unique authentication experience, allowing for more interactive and user-friendly authentication. There is no fixed mode of input, such as eye blinking or hand-tapping, which can be used in different environments. Morse code is also relatively safe against common password hacking techniques such as reuse of passwords, or brute force attack.

3.3. Convolutional neural network

CNN [24] is a type of deep learning model that is specifically developed for processing structured grid data such as images. It is widely used in computer vision tasks such as image classification. The key layers of a CNN are convolutional layer, pooling layer and fully connected layer. Convolutional layer applies learnable filters (kernels) to the input image to detect patterns like edges, textures, and objects. The output is called a feature map which shows the particular characteristics of the image. The data employed in this research is the MMU iris dataset which contained 460 iris images, and thus data augmentation was performed to expand the number of images. The Sokoto Coventry Fingerprint Dataset (SOCOFing) is a fingerprint database intended for use in academic research and is employed in fingerprint dataset processing. We have utilized a total of 4960 images, where 3240 fingerprint images and 1720 iris images. All the iris and fingerprint datasets were marked as fake and real. Biometric images (fingerprint and iris) are loaded and authenticated using a CNN. Images are preprocessed (resized to 50×50, normalized, and labeled as [1,0] for fake and [0,1] for real). The CNN architecture includes convolutional layers (ReLU), max pooling, fully connected layers, and a SoftMax layer for classification. A dropout layer (0.8) prevents overfitting. The model is trained using the Adam optimizer (learning rate=0.001) and categorical cross entropy over 20 epochs. Both the SOCOFing and MMU datasets have certain limitations. Their relatively small size and restricted demographic representation may limit generalizability when applied to diverse populations. As they were collected in controlled settings, they may not capture real-world challenges such as varying sensor quality, environmental noise, or spoofing attempts, which could introduce bias when deploying the system in practical scenarios.

3.4. Biometric watermark creation with rubik's encryption

Rubik's algorithm is a novel method of encryption that leverages the three-dimensional transformation principles of the Rubik's Cube to contribute to the security of biometric data storage. It offers a computationally cost-effective and highly secure encryption scheme for the protection of biometric templates [25] against brute-force attacks, cryptanalysis and access by unauthorized parties. In multimodal biometric systems, the application of Rubik's encryption prevents potentially vulnerable biometric data from being lost by scrambling the original metadata into an irreversible encoded data form which can only be decoded using a highly secure decryption key.

Rubik's encryption [26] process follows three primary transformations:

- Row circular shift: every row of the biometric image is shifted left or right according to the predefined row key vector (key KR).
- Column circular shift: each column is shifted upwards downwards by a separate key (KC) (column key vector).
- Bitwise XOR encoding: an additional XOR operation is made between the scrambled image and the key matrix to add a layer of security.

Step-by-step encryption process:

Key generation:
- Generate two random key vectors K_R (row-wise shift values) and K_C (column-wise shift values). These keys determine how the image undergoes row and column shifts. The key is stored in a file, encoded using Base64 for secure storage.
- Define ITERmax, the number of iterations to reinforce encryption.

Row circular shifting:
- Compute the sum of pixel intensities for each row as in (6):

$$\alpha(i)= \sum_{j=1}^{N} I_0(i,j) \quad (6)$$

- Perform left shift if $\alpha(i) \bmod 2=1$, otherwise right shift by $K_R(i)$ positions.

Column circular shifting:
- Compute the sum of pixel intensities for each column as in (7):

$$\beta(j) = \sum_{i=1}^{M} I_0(i,j) \quad (7)$$

- Perform up shift if $\beta(j) \bmod 2=1$, otherwise down shift by $K_C(j)$ positions.

Bitwise XOR transformation:
- Use vector K_C to perform a bitwise XOR operation on each row of the scrambled image as in (8):

$$I_1(2\,i-1,j) = I_{SCR}(2i-1,j) \oplus K_C(j) \quad (8)$$

$I_1(2\,i,j) = I_{SCR}(2i,j) \oplus rot_{180}(K_C(j))$, where rot 180($K_C$) is the 180° flipped version of K_C.
- Use vector K_R to perform a bitwise XOR operation on each column of image I_1 as in (9):

$$I_{ECN}(i,2j-1) = I_1(i,2j-1) \oplus K_R(j) \quad (9)$$

$I_{ECN}(i,2j) = I_1(i,2j) \oplus rot_{180}(K_R(j))$, where rot180($K_R$) is the 180° flipped version of K_R.

The process is repeated for ITERmax cycles to enhance security. The encrypted image I_{ENC} is obtained after the final iteration. Decryption process: to retrieve the original biometric data, the reverse transformations of the encryption steps are applied:
- Bitwise XOR inversion: reverse XOR operations using K_R and K_C.
- Column shift reversal: reverse the up/down shifts using $K_C(j)$.
- Row shift reversal: reverse the left/right shifts using $K_R(i)$.

Repeat the reversal process ITERmax times until the original image is reconstructed. The transformations are dependent on the exact key, decryption is only possible if the correct key file is used. The Rubik's encryption algorithm enhances biometric template security in authentication systems. It is part of a suite of multimodal biometric authentication algorithms that enables secure watermarking and template protection. The algorithm can scramble and reconstruct biometric data, which means even if an adversary intercepts a decrypted biometric template, the stored template cannot be used again without access to the secret key. Rubik's encryption thus, offers efficient real-time encryption and decryption, which can be used in biometric-based authentication applications.

3.5. Document embedding

LSB steganography [27] is used to embed encrypted biometric data into ancarrier image as watermark. It ensures that the embedded data remains imperceptible while preserving the visual integrity of the carrier image. The steps in embedding include:
- Embedding process: the biometric image (surreptitious image) is translated into a byte stream to be embedded. The translated byte data is then encrypted using advanced encryption standard (AES) algorithm in electronic codebook (ECB) mode so that the biometric watermark is made secure prior to embedding. Since AES is used for encryption, the ciphertext of the biometric image is computed as (10) where, P stands for Plaintext biometric image, k (secret encryption key), E_k (AES encryption function) and C is ciphertext (encrypted biometric watermark).

$$C = E_k(P) \quad (10)$$

To decrypt and recover the biometric watermark, computation takes place using (11) where, Dk stands for AES decryption data, C=encrypted biometric data and k for secret decryption key.

$$P = D_k(C) \quad (11)$$

The carrier image is read and translated to a NumPy array for pixel manipulation. The pixel values of RGB are flattened as a 1D array in order to carry out bitwise adjustments. The first 4 bytes (32 bits) contain metadata to represent the length of the encrypted image. Every digit of this length value is inserted into the LSB of carrier image pixels. The encrypted biometric information is inserted bit by bit into the LSB of the pixel values of the carrier image. Since the LSB change is very small, the visual quality of the carrier image is hardly affected. Every pixel of the carrier image is made up of red (R), green (g) and blue (B) values. The LSB change is given as (12):

$$P_{modified} = P_{original} - (P_{original} \bmod 2) + B_{data} \quad (12)$$

where, $P_{orginal}$ is the original pixel value, B_{data} is the bit of encrypted biometric data to be embedded (0 or 1) and $P_{modified}$ is the modified pixel value after embedding.

– Extraction process: the first 32 pixels of the carrier image are accessed to retrieve the 4-byte metadata carrying the encrypted data length. The following data length *8 pixels are scanned to extract the encrypted biometric watermark bitstream. The derived encrypted data is decrypted by employing AES decryption with the respective encryption key. The decrypted bytes are again transformed to an image representation to restore the original biometric watermark for the verification of authentication. To extract hidden data from the modified pixel:

$$B_{data} = P_{modified} \bmod 2 \quad (13)$$

In (13) ensures that the hidden bimetric watermark can be retrieved without significant distorsion.

3.6. One-time password-based re-authentication for document access

For protecting encrypted biometric-embedded documents against unauthorized access, an OTP-based authentication process is incorporated. This guarantees that even if the document is accessed by an unauthorized body, decryption is limited without OTP authentication. The document is secured with a safe cryptographic algorithm, limiting access to authorized users only. When a user tries to decrypt or view the document the system creates a random OTP and sends it to the registered Telegram device linked with the user's account for verification within the given expiration time. If the OTP is verified successfully, the system provides access to the document for decryption and viewing. If the OTP is invalid or expires, access is denied, and the user has to request a new OTP.

3.7. Error handling and failover strategy

If the MTCNN or FaceNet models fail to detect or verify the user's facial features, the system displays an “Unknown face detected” warning and requires the user to adjust their position or orientation. Progression is blocked until a correct facial match is achieved. If the eye-blink Morse code is not correctly detected within a predefined time window, the system continuously prompts the user to retry until a valid Morse sequence is captured and decoded. In the case of fingerprint or iris mismatch, the system notifies the user with a “Mismatch detected” message and allows multiple retries for the respective modality. No fallback or bypass mechanism is employed; authentication continues only after successful validation of each biometric trait. An OTP is used as a concluding verification step after all biometric checks have been passed. It is not intended as a fallback for failed biometric modalities, but rather as a secure final layer in the overall authentication pipeline.

4. RESULTS AND DISCUSSION

A multimodal solution based on Morse code authentication and biometrics was employed to increase digital document security by using a combination facial recognition, Morse code authentication, biometric verification, and cryptographic watermarking. All experiments were conducted on an Intel i5 vPro processor and 8 GB RAM, running Windows 10 with Python (TensorFlow/Keras, OpenCV, and supporting libraries).

4.1. Facial recognition-based user authentication

The authentication process starts with user registration where face embeddings are captured using OpenCV and saved for future verification. At login phase, live facial image is captured as Figure 4, processes it with MTCNN, and produces a 128-dimensional feature vector through FaceNet. Following

user registration, a login system based on Face ID was implemented to securely authenticate the users. The login process checks the identity of the user through face recognition before giving permission.

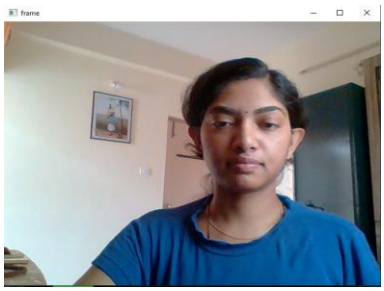


Figure 4. Capture of user image

4.2. Morse code entry for secure access

Upon successful authentication, the user is asked to input their Morse code password through blink-based input detection, which is decoded and verified. To strengthen security, Morse code authentication was integrated. Users were required to input a predefined Morse code sequence via a blinking pattern, which was captured using OpenCV and Dlib. Figure 5 indicates the detection of eye blinks for capturing the Morse code. The blink patterns captured by virtual keypad displayed in Figure 6 are translated into Morse code and matched them against the stored sequence. The system applies frame-based filtering to categorize blinks as dots (•) and dashes (−) for Morse code verification. The ratio of blinking is calculated through Dlib's landmark detection, and it then allocates a corresponding Morse code symbol depending on its value and length. The blink duration is based on frames processed. To reduce false positives caused by involuntary blinks or rapid flickers, a blink duration threshold (T) was empirically calibrated. Blinks shorter than T were discarded as noise, while valid Morse inputs were registered only when T_b<=T (dot) or T_b>=3T (dash). Filtering helped eliminate ~90% of involuntary blink interference during trials. Table 2 indicates how eye blinks are mapped to Morse code output. If the sequence of the Morse code is valid, authentication is successful.

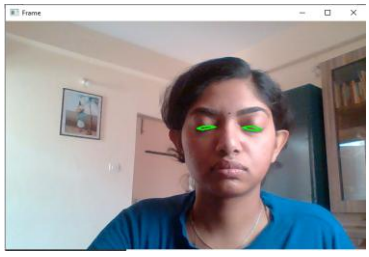


Figure 5. Detection of eye blink

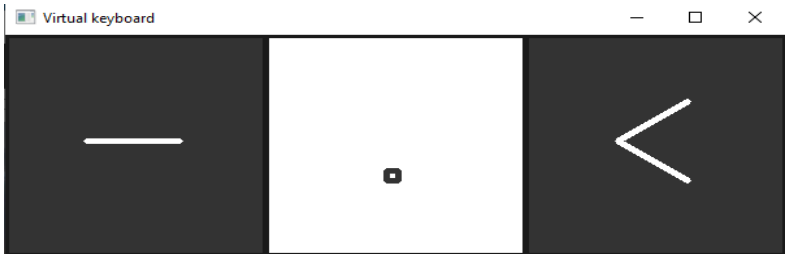


Figure 6. Virtual keypad

Table 2. Blink classification

Blink detection parameter	Condition	Mapped Morse code output
Eyes open (No input)	blinking_ratio<5	No Morse code input
Short blink (Dot •)	blinking_ratio>5 for frames_to_blink=6 frames	Dot (•)
Long blink (Dash −)	blinking_ratio>5 for 3×frames_to_blink=18 frames	Dash (−)

4.3. Model training using convolutional neural network

Each of iris and fingerprint dataset is divided into two sets of training and testing with an 80-20% split. Figures 7 and 8 shows a comparison of training vs validation accuracy and loss graph for iris and fingerprint images. For iris recognition**,** the model achieved a training accuracy of 98% and a validation accuracy of 100%, indicating excellent generalization with no signs of overfitting. The test accuracy of 100% further confirms the model's robustness in distinguishing live and fake iris samples. For fingerprint recognition, the model attained a training accuracy of 98% and a validation accuracy of 97%, demonstrating

strong feature extraction capabilities. The test accuracy of 97.9%~98% highlights the model's reliability in classifying live and fake fingerprints.

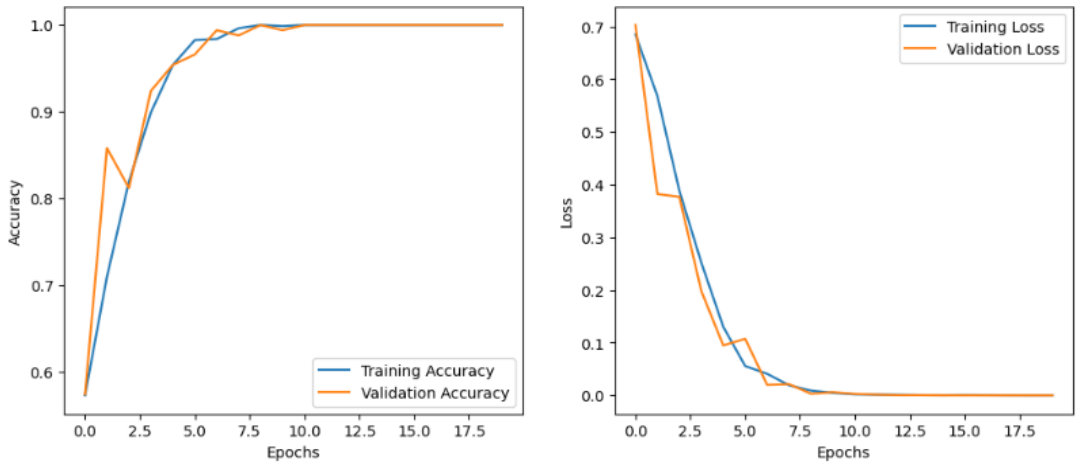


Figure 7. Training vs validation accuracy and loss graph-iris data

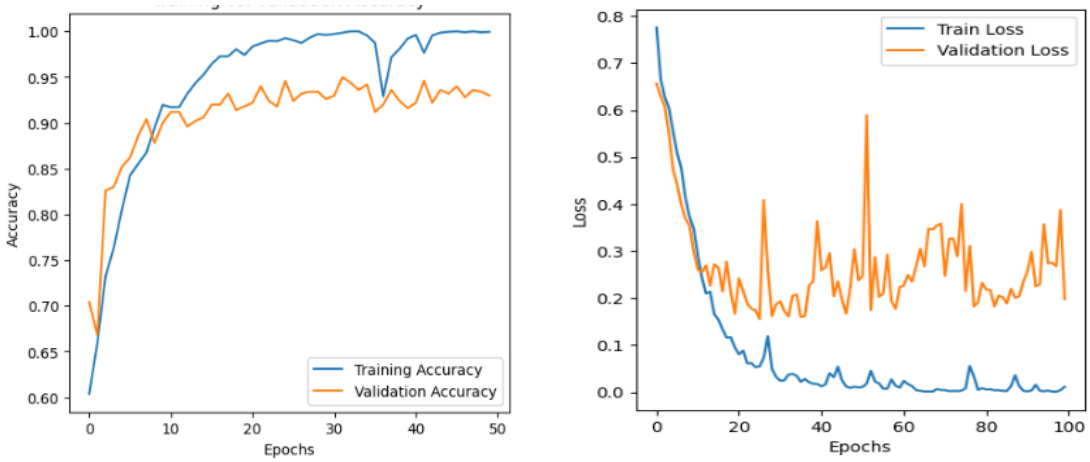


Figure 8. Training vs validation accuracy and loss graph-fingerprint data

The consistently high accuracy across training, validation, and testing phases suggests that the proposed system effectively prevents biometric spoofing while ensuring secure authentication. The classification results are given in Table 3. The confusion matrix shown in Figures 9 and 10 provides insights into the model's classification performance, showing the number of correctly and incorrectly classified samples. The system allows users to upload biometric images, including iris and fingerprint images, for further processing.

Table 3. Classification report of iris and fingerprint data

	Precision	Recall	F1-score	Support	Precision	Recall	F1-score	Support
	Iris data				Fingerprint data			
Fake	1.00	1.00	1.00	583	0.97	1.00	0.98	1599
Live	1.00	1.00	1.00	719	1.00	1.00	1.00	952
Macro average	1.00	1.00	1.00	1320	0.98	0.97	0.98	2551
Weighted average	1.00	1.00	1.00	1320	0.98	0.98	0.98	2551

4.4. Rubik's encryption, watermarking and one-time password verification

As an added layer of security, these images can be watermarked to ensure authenticity and prevent unauthorized modifications. The system encrypts verified biometric features using the Rubik's algorithm. A unique watermark is generated by using the biometric sources and is embedded into the uploaded digital documents. An OTP is sent to user's telegram account and then the iris and fingerprint data are created as watermark using LSB steganography which cannot be detected by human eye. The encrypted image will have a text on the image as an indication that it is encrypted in case of image data and pdf is represented as corrupted documents. In the decryption process only, authenticated users should be allowed to decrypt and access the original data. To ensure secure access to sensitive documents, an encryption key is generated and must be entered by the user. Our watermarking scheme shows similar resilience to tampering and compression as the zero-bit biometric embedding approach detailed in [10].

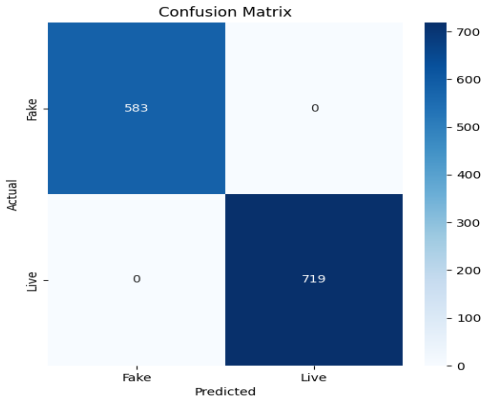


Figure 9. Confusion matrix-iris data

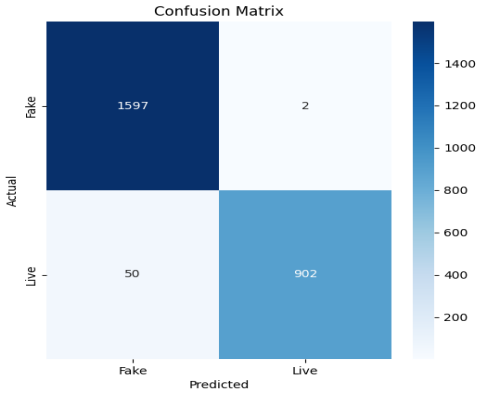
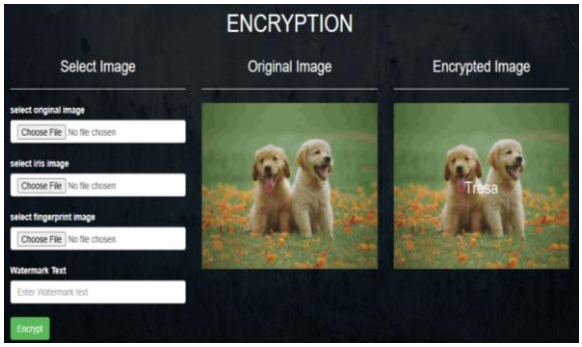
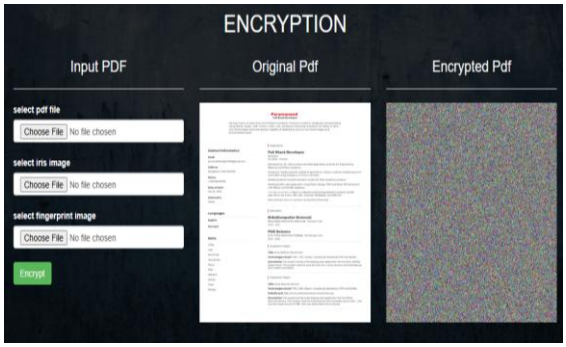


Figure 10. Confusion matrix-fingerprint data

Figures 11(a) and (b) shows the encryption process and Figures 12(a)-(d) shows the decryption process. Upon successful key entry, the system initiates an OTP verification step for decryption process. This process ensures that only the legitimate user, in possession of both the encryption key and the linked authentication device, can retrieve the original document. This multi-layered security system significantly enhances protection against unauthorized users, ensuring confidentiality, integrity, and controlled access to critical information.



(a)



(b)

Figure 11. Encryption and watermark generation process; (a) encrypted image with a text indication and (b) encrypted pdf file

Modules such as Morse code input via blinking, facial recognition (MTCNN+FaceNet), OTP verification, and Rubik's encryption-based watermarking, were validated through multiple real-time functional test runs. These modules reliably enforced authentication workflows and access control under test conditions, with the Morse code blink detection achieving consistent recognition under the defined threshold

criteria for dots and dashes. Empirical testing over 30–50 trials per module indicated successful end-to-end authentication in the majority of cases. Future work will involve logging real-time metrics for these modules, including success/failure rates, average response time, and performance under common attack scenarios to fully benchmark the system's security and usability. While we did not perform formal adversarial testing like morphing attacks or deepfake simulations, our design assumes resilience by requiring multi-step, cross-modal verification. While the proposed system is designed to enhance security through multi-step, cross-modal biometric verification, this work does not include adversarial evaluations such as biometric morphing attacks or deepfake-based simulations. Future work will focus on comprehensive validation under such adversarial conditions, including simulated attack environments and stress testing against emerging spoofing techniques.

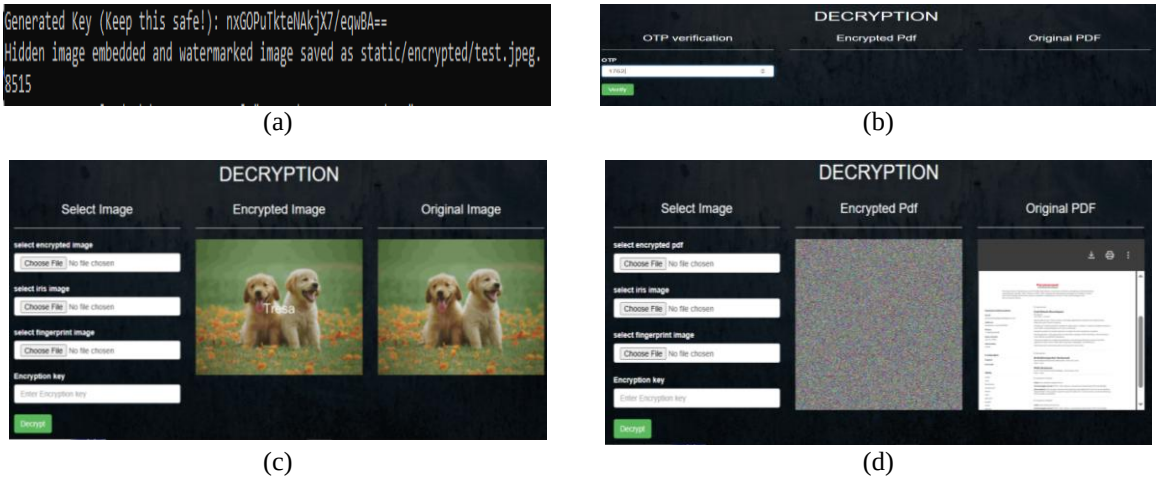


Figure 12. Decryption process; (a) encryption key generation, (b) OTP verification for decryption process, (c) retrieval of original image data after decryption, and (d) retrieval of original pdf document after decryption

5. CONCLUSION

In the face of ever-evolving digital security threats, traditional authentication mechanisms often fall short in preventing unauthorized access and identity fraud. This research presents a multi-layered authentication system to enhance digital document security. The OTP-based re-authentication mechanism adds an additional layer of security, ensuring that only legitimate users can access protected data. Future research can explore AI-driven anomaly detection to identify unusual login behaviors, blockchain-based authentication to enhance transparency, and multi-modal authentication incorporating voice or keystroke dynamics for improved security. Ensuring scalability for large- scale implementations in critical sectors such as finance, healthcare, and government would further extend its practical applicability. This study highlights the importance of MFA in modern cybersecurity. The proposed scalable and secure framework provides a future-ready approach to safeguarding sensitive data, ensuring privacy, and preventing unauthorized access. By combining robustness, adaptability, and user-centric design, the developed framework offers a resilient solution to evolving cybersecurity challenges, laying the groundwork for future innovations in secure document access in the digital world. In addition, resource requirements and scalability considerations have been acknowledged, particularly the need to evaluate computational overhead and system performance when scaled to larger user databases. Usability aspects, including accessibility for users with visual impairments or motor disabilities, will also be a priority for future extensions of the framework to ensure inclusivity in real-world deployments.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Tresa Maria Josylin	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Ganeshayya Shidaganti		✓				✓		✓	✓	✓	✓	✓	✓	
Vishwachetan Dasegowda	✓						✓			✓		✓	✓	
Anasuya Jadagerimath	✓			✓		✓				✓		✓		
Prakash Sheelvanthmath	✓					✓				✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The MMU Iris Dataset and SOCOFing Fingerprint Dataset used in this study are publicly available from their respective sources.

REFERENCES

[1] E. Marasco, M. Albanese, V. V. R. Patibandla, A. Vurity, and S. S. Sriram, "Biometric multi-factor authentication: On the usability of the FingerPIN scheme," *Security and Privacy*, vol. 6, no. 1, 2023, doi: 10.1002/spy2.261.

[2] M. Khurana, R. Aggarwal, R. Rani, and V. Khurana, "Understanding password vulnerabilities - A mathematical approach," *AIP Conference Proceedings*, 2022, vol. 2357, p. 100012, doi: 10.1063/5.0080658.

[3] R. Alrawili, A. A. S. A. Qahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Computers and Electrical Engineering*, vol. 119, p. 109485, Oct. 2024, doi: 10.1016/j.compeleceng.2024.109485.

[4] B. Singh and G. Kasana, "A review of digital watermarking techniques: Current trends, challenges and opportunities," *Web Intelligence*, vol. 22, no. 4, pp. 523–553, 2024, doi: 10.3233/WEB-230280.

[5] N. A. Nayak, M. Vijaya, and M Akshitha, "Morse Code Based Secured Authentication System through Machine Learning," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 252–261, May 2023, doi: 10.48175/ijarsct-9687.

[6] F. Wang, A. Hu, Y. Song, W. Zhang, J. Zhu, and M. Liu, "Morse Code Recognition Based on a Flexible Tactile Sensor with Carbon Nanotube/Polyurethane Sponge Material by the Long Short-Term Memory Model," *Micromachines*, vol. 15, no. 7, p. 864, Jun. 2024, doi: 10.3390/mi15070864.

[7] C. S. Pillai, S. A. Shruthi, A. N. Amulya, A. K. Ashitha, D. S. Deekshitha, and K. S. Bhavana, "Morse Code Based Authentication System Using Eye Blink," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 2, pp. 2273–2278, Mar. 2023, doi: 10.56726/IRJMETS33988.

[8] M. Sushmitha, N. Kolkar, S. G. Sra, and K. Kulkarni, "Morse Code Detector and Decoder using Eye Blinks," in *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, Sep. 2021, pp. 651–658, doi: 10.1109/ICIRCA51532.2021.9545039.

[9] H. K. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using Multimodal Biometric Fusion for Watermarking of Multiple Images," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3487–3494, Feb. 2024, doi: 10.1109/TCE.2024.3371458.

[10] R. Deepika, M. Shambhavi, R. Impana, A. P. Shishira, and L. Krishna, "Zero-Bit Watermarking Technique for Generation of Unique ID Using Biometric Images," in *2022 2nd International Conference on Intelligent Technologies, CONIT 2022*, Jun. 2022, pp. 1–4, doi: 10.1109/CONIT55038.2022.9848041.

[11] J. J. Fernandez and P. N Nithyanandam, "Protection of online images against theft using robust multimodal biometric watermarking and T-norms," *Multimedia Tools and Applications*, vol. 83, no. 17, pp. 52405–52431, Nov. 2024, doi: 10.1007/s11042-023-17497-x.

[12] K. N. Singh, O. P. Singh, A. K. Singh, and A. K. Agrawal, "WatMIF: Multimodal Medical Image Fusion-Based Watermarking for Telehealth Applications," *Cognitive Computation*, vol. 16, no. 4, pp. 1947–1963, Jul. 2024, doi: 10.1007/s12559-022-10040-4.

[13] S. Li, L. Fei, B. Zhang, X. Ning, and L. Wu, "Hand-based multimodal biometric fusion: A review," *Information Fusion*, vol. 109, p. 102418, Sep. 2024, doi: 10.1016/j.inffus.2024.102418.

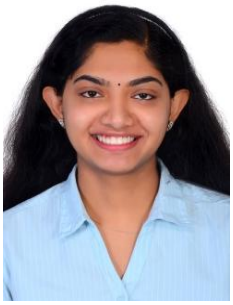
[14] N. Alay and H. H. Al-Baity, "Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits," *Sensors*, vol. 20, no. 19, pp. 1–17, Sep. 2020, doi: 10.3390/s20195523.

[15] P. Terhörst, D. Fährmann, N. Damer, F. Kirchbuchner, and A. Kuijper, "On Soft-Biometric Information Stored in Biometric Face Embeddings," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 519–534, Oct. 2021, doi: 10.1109/TBIOM.2021.3093920.

[16] N. Nnamoko, J. Barrowclough, M. Liptrott, and I. Korkontzelos, "A behaviour biometrics dataset for user identification and authentication," *Data in Brief*, vol. 45, p. 108728, Dec. 2022, doi: 10.1016/j.dib.2022.108728.

[17] M. Khudzaifah, S. H. Ma'rifah, and H. Fahmi, "Implementation of Rubik's Cube Algorithm and Rivest-Shamir-Adleman (RSA) Algorithm on Iris Digital Image Security," in *Proceedings of the 12th International Conference on Green Technology (ICGT)*, 2023, pp. 312–323, doi: 10.2991/978-94-6463-148-7_31.
[18] S. Durgaraju, D. Vishal, T. Vel, H. Madathala, and B. Barmavat, "AI-Driven Adaptive Authentication for Multi-Modal Biometric Systems," *Journal of Electrical Systems*, vol. 17, no. 1, pp. 75–88, Jan. 2024, doi: 10.52783/jes.6643.
[19] S. H. Choudhury, A. Kumar, and S. H. Laskar, "Adaptive Management of Multimodal Biometrics—A Deep Learning and Metaheuristic Approach," *Applied Soft Computing*, vol. 106, 2021, doi: 10.1016/j.asoc.2021.107344.
[20] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Information Fusion*, vol. 52, pp. 187–205, 2019, doi: 10.1016/j.inffus.2018.12.003.
[21] S. Serengil and A. Özpınar, "A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules," *Bilişim Teknolojileri Dergisi*, vol. 17, no. 2, pp. 95–107, Apr. 2024, doi: 10.17671/gazibtd.1399077.
[22] H. T. Cethana, T. C. Nagavi, P. Mahesa, V. Ravi, and H. Gururaj, "FaceNet – A Framework for Age Variation Facial Digital Images," *ICST Transactions on Scalable Information Systems*, vol. 11, Jul. 2024, doi: 10.4108/eetsis.5198.
[23] C. Gundler, M. Temmen, A. Gulberti, M. P.-Nerger, and F. Ückert, "Improving Eye-Tracking Data Quality: A Framework for Reproducible Evaluation of Detection Algorithms," *Sensors*, vol. 24, no. 9, 2024, doi: 10.3390/s24092688.
[24] M. Krichen, "Convolutional Neural Networks: A Survey," *Computers*, vol. 12, no. 8, p. 151, Jul. 2023, doi: 10.3390/computers12080151.
[25] J. Zhao, T. Zhang, J. Jiang, T. Fang, and H. Ma, "Color image encryption scheme based on alternate quantum walk and controlled Rubik's Cube," *Scientific Reports*, vol. 12, no. 1, p. 14253, Aug. 2022, doi: 10.1038/s41598-022-18079-x.
[26] Madduluri, R. Varma, A. Golla, S. Raghava, and T. J. Sai, "Advanced Image Encryption & Decryption using Rubik's Cube Technology," *International Journal of Engineering and Advanced Technology*, pp. 24–27, Feb. 2022, doi: 10.35940/ijeat.c3331.0211322.
[27] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, and C. Valli, "Integration of Biometrics and Steganography: A Comprehensive Review," *Technologies*, vol. 7, no. 2, p. 34, Apr. 2019, doi: 10.3390/technologies7020034.

BIOGRAPHIES OF AUTHORS



Tresa Maria Josylin is currently working as Assistant Professor in the Department of Computer Science and Engineering at BMS Institute of Technology and Management, Bangalore. She holds a Master of Technology M.Tech. degree in Computer Science and Engineering from M.S. Ramaiah Institute of Technology, Bangalore, and a Bachelor of Engineering B.E. degree in Computer Science and Engineering from Atria Institute of Technology, Bangalore. Her academic interests are focused on artificial intelligence, deep learning, and natural language processing. She has actively participated in research activities, and her work has been presented at national and international conferences. She can be contacted at email: tresamjosylin@bmsit.in.

Ganeshayya Shidaganti is currently working as an Associate Professor in Computer Science Department at Ramaiah Institute of Technology. He has received a Ph.D. degree in faculty of Computer and Information Sciences at Visvesvaraya Technological University (VTU), Belagavi. He has completed his B.E. (CSE) from B.V.B. College of Engineering and Technology, Hubli and M.Tech. (CSE) from Ramaiah Institute of Technology, Bangalore. With over a decade of teaching experience, he has published 40+ research papers in International Conferences/Book Chapters and Journals, indexed in Scopus and authored the book "Confluence of Teaching and Learning through Digital Pedagogy" by Cambridge Scholars. He has received the 2024 UiPath Academic Alliance "Educator of the Year" award under Research and Publication and recognition for leadership at UiPath DevCon 2020. He has participated in and delivered multiple guest lectures throughout his teaching journey. He is also a member of professional societies IEEE, ACM, and CSI. He can be contacted at email: ganeshayyashidaganti@msrit.edu or ganeshayyais@gmail.com.

Vishwachetan Dasegowda is currently serving as an Assistant Professor in the Department of Computer Science at Ramaiah Institute of Technology. He is actively pursuing a Ph.D. in the field of Natural Language Processing, with a specific focus on phishing email detection. His research interests span across a diverse range of areas, including natural language processing, cybersecurity, computer networks, internet of things, operating systems, and web technologies. His research contributions include publications in high-impact journals and international conferences. He is a member of the Association for Computing Machinery (ACM), demonstrating his dedication to professional growth and engagement with the latest advancements in computer science. He can be contacted at email: vishwachetan@msrit.edu.

Anasuya Jadagerimath currently serving as Professor in CSE (AI and ML) at DBIT, Bengaluru, she has held multiple leadership roles including HoD positions. She holds a Ph.D. from Tumkur University, an M.Tech. from M.S.R.I.T (VTU), and a B.E. from B.E.C Bagalkot (K.U.D). A VTU-recognized research supervisor, she has guided numerous projects, published extensively in Scopus-indexed journals, and presented at global conferences. She is a recipient of the Jyeshta Acharya Bharat Education Excellence Award (2024) and holds patents in IoT and intelligent systems. Her contributions span NPTEL certifications, AICTE-funded initiatives, and collaborations with industry programs like Infosys and AWS Educate. She is passionate about bridging academic theory with practical innovation through workshops, seminars, and student mentorship. She can be contacted at email: anasuyanj556@gmail.com.

Prakash Sheelvanthmath is currently Pro Vice Chancellor at Dayananda Sagar University and he was the Senior Vice President at East Point Group of Institutions, Bengaluru, where he oversees all educational operations. With extensive expertise in the education sector, he has held significant leadership roles at top institutions. Previously, he served as Vice President at Mohan Babu University, managing critical academic responsibilities, and as the Executive Director at Chandigarh University, contributing to strategic advancements. His role as Dean and Professor at Dayananda Sagar University further enhanced his academic and administrative impact. Earlier in his career, he played a pivotal role at NIIT Ltd, supporting the growth of the education and IT sector. His comprehensive background across renowned universities and organizations has established him as a leader committed to driving institutional growth, academic innovation, and operational excellence. He can be contacted at email: prakash.hospet@gmail.com.