Date of publication JUN-30, 2024, date of current version MAY-22, 2024.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.23.2.3541

Smart Recognition and Authentication based on Haar Cascade Classifier and Visual Cryptography

SAIKAT BOSE[1], TRIPTI ARJARIYA[1], ANIRBAN GOSWAMI[2]
[1]Department of Computer Science Engineering, Bhabha University, Bhopal, India
[2]Department of Information Technology, Techno India, Kolkata, India

Corresponding author: Saikat Bose (e-mail: troykol@yahoo.co.in).

ABSTRACT The algorithm with an E-verification method is proposed that combines automated facial recognition technology with digital media and later it combines aspects of secret data exchange and visual cryptography. A face detection technique based on Internet of Things (IoT) selects features using the Principal Component Analysis (PCA) algorithm and the Haar cascade classifier. The selected face serving as a cover follows two level Discrete Haar Wavelet Transform. The shares generated from digital signature and fingerprint are diffused into the converted coefficients. Furthermore, the imperceptibility of the additional noise is increased by a bit-level noise reduction technique. Authenticity is confirmed by regenerating a message digest at the receiving end, and the extraction process operates in complete blindness. The approach is suitable for smart card design and may be used as an automatic recognition system in a real-world setting. Performance comparisons show a notable improvement over other approaches that are comparable. Additionally, the technique is effective against some related attacks.

KEYWORDS IoT; Haar cascade classifier; Machine Learning; Visual cryptography; Daubechies DWT.

I. INTRODUCTION

ELECTRONIC sensitive documents necessitate thorough data validation [1] and comprehensive user authentication. The successful concealment of sensitive data within a digital document serves to establish its authenticity or ownership claims through trusted validations [2]. Further, robust encryption techniques effectively mitigate the risk of unauthorized access to copyrighted content, thereby safeguarding it against a plethora of potential image processing attacks.

Given the current landscape of authentication practices, the proposed concept introduces a novel technique for authenticating Citizen's Passport. This technique not only verifies the authenticity of the passport but also includes a validating test resembling the relevant data [3]. It is imperative to consider the implementation of E-governance-based authentication systems in airports and other international entry and exit points, which would serve as a notable departure from the current methods. This novel approach involves verifying the identity of the individual according to the passport that he or she is carrying. The proposed approach involves multi-watermarking concept [4] based on digital signatures & fingerprint [3] embedding in authorized detected face. By employing an appropriate classifier for Face Recognition, the system is able to achieve multi-phase authentications, thereby validating the citizen's identity initially [5].

A passport is a government-issued identification document of a citizen that encapsulates an individual's identity information and avails consular aid when required [6]. In the realm of passports, it is customary for them to encompass a comprehensive array of data, including but not limited to the complete appellation, visual representation, geographic location and date of birth, personal signature, as well as the expiration date of the person’s passport. Numerous nations engage in the issuance of biometric passports, which encompass an embedded microchip, thereby rendering them amenable to machine interpretation and arduous to replicate [7]. According to the latest data, since January 2019, the number of jurisdictions that have been authorized to issue e-passports exceeds 150 [8]. The validity of non-biometric machine-readable passports that were previously issued typically persists until their individual expiration dates.

The impetus for implementing robust authentication procedure in passport stems from the recognition of confidentiality and validity of citizens' identities, at every international entry/exit points like airports, etc. In this context, it is imperative to specify the paramount security concerns encompassing administrative, physical, and technical safeguards. In light of the necessity to authenticate citizens using passport validation, various advanced data security techniques have emerged. The Passport Seva Kendra (PSK) plays a crucial role in framing of passport [8] utilizing sensitive legal data. The introduction of data hashing, encryption, and concealment techniques can be introduced as a means of safeguarding the personal records of individuals. In light of the aforementioned concerns, the proposed algorithm introduces a novel data security solution aimed at promptly verifying the identity of an individual through a trusted validation process. The motive for the proposed concept is:

1. Proper validation and authentication of citizens based on tri-authentication blind procedure.
2. The system leverages Face Recognition technology to encompass the identification and verification of facial features, utilizing the Haar Cascade technique for machine learning [9].
3. Further, the proposed technique focuses on enhancing the attributes of digital media by combining visual cryptography with secret data (signature) and finger print sharing elements.
4. The work also aims to attain data integrity through hash value-based copyright data hiding techniques.

The below sections as assembled describes the flow of the article.

II. LITERATURE REVIEW

In the realm of face recognition, a machine learning-based approach utilizing the Haar Cascade method has been employed for this specific validation scheme. Additionally, copyright signature watermarking and visual secret sharing techniques have been utilized, alongside the generation of hash values for sensitive data. The subsequent sections will outline some of the prevailing endeavors on the pivotal matters of this realm for improvement.

A. EXISTING APPROACHES

According to T. H. Iwan, H. M. Fahrezy, et al. [10], Microsoft servers incorporate the Face Recognition System using Eigenface face detection method. Aneesa Tankasali et al. [11] demonstrated an IoT-based smart home lighting system with facial recognition. Ushie James et al. [12] suggested using ESP32 CAM instead of Pi Cam for image capture. The system of Ivan Surya et al. [13] includes Blynk IoT and Google Cloud. The Internet-connected Blynk platform for iOS and Android cell phones and other mobile devices controls Arduino, Raspberry Pi, and Node MCU. Elechi et al. [14] installed a smart door system with an automated lock after 30 seconds using Raspberry Pi, camera and sensors.

This widespread use of technology threatens to compromise the confidentiality of secret or copyright material when transmitted wirelessly. Encrypting secret data and fabricating encrypted signals into a digital file for file integrity or fidelity [15] is a standard method for safe transmission [16]. Shamir [17] was the first to propose generating public and private shares from sensitive data and sending the appropriate share. This technique justifies exposing secret information after bonding suitable shares. Reversible data hiding [18] and encrypted information transfer can effectively explain information security.

Sharing and masking-based research is popular [19, 20], and picture redundant information is easy to generate. Existing data masking methods used spatial or transform domain patterns. To improve data concealment and exploit Human Visual Systems (HVS), algorithms started with Spread Spectrum-based approaches [21] and then moved to Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) [22]. Multi-resolution analysis (MRA) and time–frequency resolution problem correction make Discrete Wavelet Transform (DWT) popular for defining data privacy in medical pictures [23]. Bender et al. [24] suggested hiding a message in pixels' least significant bits. According to Lie et al. [25], a traditional bit manufacturing process can be adapted. Changing resolution levels can strengthen secret data attachment to the cover image. Fabricating with all four one-level DWT decomposed coefficients was suggested by L. L Li et al. [26]. Bassam et al. [27] suggested synthesizing secret data in the Least Significant Bit (LSB) positions of all Discrete Wavelet Transform (DWT) coefficients, while Po-Yueh Chen [28] suggested using only the first block, i.e., LL sub-band. Chen et al. [29] showed how to employ HVS after construction by concealing data in the high frequency region and leaving the low frequency region unaltered. Changing wavelet coefficient compression levels increases image quality as stated by Li Long Huang Herman [30].

Chu et al. [31] compressed and encrypted grey secret data before fabricating them in the cover image's Discrete Wavelet Transform (DWT) converted coefficients. X Song and F Liu [32] indulged Gabor Discrete Wavelet Transform (DWT), while Abdelwahab and Hassan [33] developed a data concealing strategy using 1 level Discrete Wavelet Transform (DWT) for both secret and cover images. Bao and Ma [34] proposed concealing secret data in singular value decomposition in the wavelet domain, and Maity and Kundu [35] presented blind watermarking in the LL and HH sub-band of frequency coefficients. Another approach uses a mapping table and the high-frequency sub-band to create a secret message. Chen and Lin [36] integrate human visual system characteristics and complementary data concealing approach to maximize robustness without compromising image quality. Lin and Lin proposed combining cryptography and watermarking to convert secret material to a key based on different features [37]. Ali and Ahn [38] devised a self-adaptive differential evolution approach that embeds the primary component of the watermark into a cover image instead of singular values. Further research was conducted by Al-Haj et al. [39] who used multi-signatures in frequency domain to validate e-documents. Zhang, Li et al. [40] used visual cryptographic and multi-watermarking in frequency domain that embeds multiple signature data using variable encoding. In another concept, Chowdhury et al. [41] focused on multi-signature concealment with authentic hash values and addressed significant data security challenges for e-document validations. Bose et al. [42] validated e-document images using signature sharing, a visual cryptographic concept and data concealing.

Based on the analysis, it becomes apparent that the utilization of transform domain-based data hiding concepts demonstrates higher efficiency. Furthermore, the integration of visual cryptography and watermarking yields improved authentication scenarios, particularly when applied in conjunction with the Internet of Things (IoT). The establishment of a robust data security protocol effectively mitigates all pertinent data security concerns and acts as a dependable means of authenticating or validating the identity of individuals. Therefore, taking into account the efficacy of these methodologies, the present endeavor aims to integrate these concepts in order to establish reliable verification of an individual's identity at airports or other international entry and exit locations. This can be achieved through significant improvements, which will be elaborated upon in the following discussion.

III. INCEPTION OF THE PROPOSED SYSTEM

In the proposed system, the initial step involves capturing photographs of individuals, which are then stored within the primary database residing on the central server of the Passport Seva Kendra. The webcam serves the pu rpose of capturing facial images, which are subsequently utilized for face detection. This detected face is then compared against the pre-existing database, and the resulting recognition outcome is displayed through a live stream. The Python OpenCV library is utilized in order to facilitate face recognition functionality.

The subsequent method conceals the citizen's fingerprint and digital signature by integrating them in the host facial image. Secret embedding is controlled by secure hash values from legitimate test data and Daubechies Discrete Wavelet Transform. The idea also addresses data integrity. Note that this secret data hiding approach uses two hash values. One hash value monitors circular sequencing of the casted signature pieces, while the other identifies the host image sub-block interval for signature data casting. Therefore, the above notion efficiently addresses data security problems including authenticity, integrity, secrecy, and non-repudiation.

IV. DISCUSSION ON MULTIRESOLUTION WAVELET

In the realm of wireless communication, it is widely acknowledged that wavelet modulation holds a distinct advantage over Orthogonal Frequency-Division Multiplexing (OFDM) when it comes to mitigating the effects of narrow band interferences.

The Daubechies Wavelet Transform was used to implement the signature and fingerprint embedding technique [43]. Discrete Wavelet Transform (DWT) is effective in compression [44], image analysis [45], and signal classification [46]. High frequency (HH) bands capture delicate details and textures in images. The sensitive data encoded inside this frequency range will be untouched by compression and noise-based attacks. Yue and Chiang [48] proposed a neural network-based visual cryptography technique to address data security concerns such as confidentiality, integrity, authentication, and non-repudiation.

The mathematical idea of Discrete Wavelet Transform (DWT) generates multi-resolution sub-bands from an image [47]. The horizontal and vertical channels of a picture are significantly subsampled to frame different frequencies. The finest scale coefficients LH1, HL1, and HH1 contain higher frequency comprehensive information. LL1 is coarse, low-frequency and divided into LL2, LH2, HL2, and HH2. The goal is to use the altered image redundancy factor and rebuild it properly after decompression. The stages of decomposition are shown in Fig. 1.

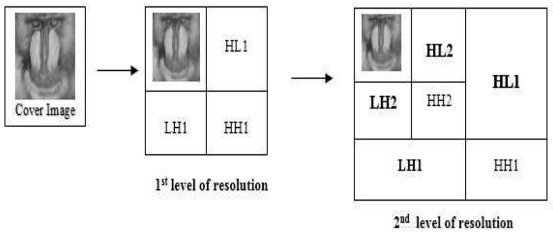


Figure 1. Resolution level in DWT

The input data undergoes a process where it is partitioned into two groups. The even elements are allocated to the first half of a section in an array with N elements, denoted as S_0 to $S_{n/2-1}$. Conversely, the odd elements are assigned to the second half of the same section, specifically $S_{n/2}$ to S_{N-1}. In the forward transform, the element referenced by S [n/2 + n] is odd, while the element referenced by S[n] is even, as stated below in (1).

Update 1: For $n = 0$ to $(n/2 -1)$, $S[n]= S[n] +\sqrt{3}\, S[n/2 + n]$.
Predict: $S[n/2] = S[n/2]-\sqrt{3}/4\, S[0] - ((\sqrt{3}-2)/4\, S[n/2-1])$.
For $n=1$ to $(n/2-1)$: $S[n/2+n] = S[n/2+n]- \sqrt{3}/4\, S[n]- ((\sqrt{3}-2)/4S[n-1])$.
Update 2: For $n = 0$ to $(n/2 -2)$, $S[n]= S[n] -S[(n/2) + n+1]$, $S[n/2-1] = S[n/2-1]- S[n/2]$.
Normalize: for $n=0$ to $(n/2-1)$, $S[n]= ((\sqrt{3}-1)/ \sqrt{2})S[n]$, $S[n + n/2] = ((\sqrt{3}+1)/ \sqrt{2})S[n+n/2]$. (1)

The inverse process is the exact reflection of the forward transformation. The equations pertaining to the reverse technique are explicated in (2).

Update 1: For $n = 0$ to $(n/2 -1)$, $S[n]= S[n] -\sqrt{3}\, S[n/2 + n]$.
Predicate: $S[n/2] = S[n/2] +\sqrt{3}/4\, S[0] + ((\sqrt{3}-2)/4S[n/2-1])$.
For $n=1$ to $(n/2-1)$ $S[n/2+n]= S[n/2+n]+ \sqrt{3}/4S[n]+ ((\sqrt{3}-2)/4S[n-1])$.
Update 2: For $n = 0$ to $(n/2 -2)$, $S[n] = S[n] +S[(n/2) + n+1]$, $S[n/2-1] = S[n/2-1]- S[n/2]$.
Normalize: for $n=0$ to $(n/2-1)$, $S[n]= ((\sqrt{3}+1)/ \sqrt{2})S[n]$, $S[n+n/2]= ((\sqrt{3}-1)/ \sqrt{2})S[n+n/2]$. (2)

V. PROPOSED METHODOLOGY

A. FACE RECOGNITION

The proposed algorithm uses an integrated camera module either using ESP32 or Raspberry pi for detecting the face and then uses a fingerprint sensor to store the fingerprint. When an individual approaches the passport office for making the passport, the image of the face, the fingerprint and digital signature is recorded. A match will be done between the stored image and the image instantly taken. If there is no match the face is stored in the database, otherwise a message will be generated as Duplicate. The Viola-Jones algorithm [60] is one of the most popular and optimized face detection techniques. It uses the Haar cascade classifier using OpenCV for face detection. This detected face is subsequently compared with the pre-existing database, and upon a successful match, the recognition outcome is displayed through a live streaming mechanism. The Python OpenCV library is utilized owing to its strong and effective set of features and provides a comprehensive suite of pre-trained face detection models, which effectively streamline the process of face detection by eliminating the need to develop one from the ground up. This advantageous feature significantly reduces the time and effort required for building a face detection model from scratch.

The whole mechanism of Face Recognition is shown in Fig. 2.

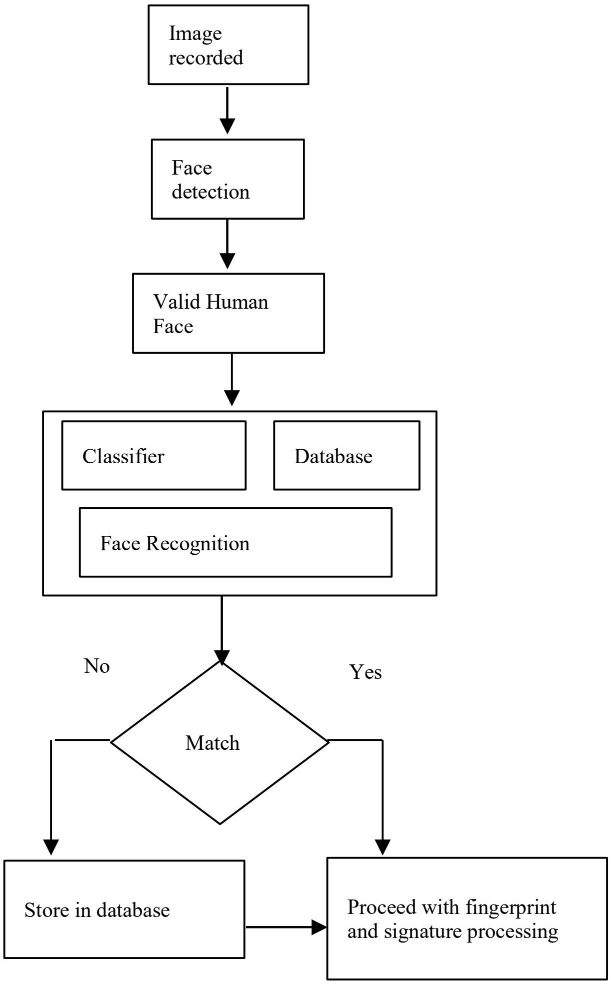


Figure 2. Flowchart for face detection and recognition

B. THE PROCESSING OF DIGITAL SIGNATURE

The complete computational process for encoding a signature protocol for visual authentication has been explained. The initial phase encompasses the proper generation of shares derived from a digitized signature. The subsequent phase elucidates the efficacy of Discrete Wavelet Transform (DWT) and the remarkable fusion of confidential information within the cover image. Lastly, the third phase identifies the concealed data and verifies its authenticity.

Step 1: A born digital or digitized handwritten signature improves entity authentication, data integrity, and non-repudiation [47] in public key (asymmetric) cryptography. The digitized signature of an authentic sender is obtained and each pixel is cleaned to create a binary version with white and black pixels. Also, a threshold-based pixel value categorization improves clarity. Black and white pixels are distinguished and a large quantity of black pixels may be found to recreate the original signature. Yue and Chiang [48] predicted neural network-based visual cryptography creates two sets of shares per pixel, as seen in Fig. 3. The initial share, denoted as Share 1, is encrypted and embedded within a concealment image. The second share, denoted as Share 2, is publicly accessible and has been distributed to the recipient. The issues of data security are handled as:

1. If the identified S1 adequately aligns with S2 to produce a genuine signature, it can serve as the evidence of the authenticity of both the sender and the transmitted document.
2. The non-repudiation characteristic is established when S1 is accurately detected and subsequently overlaid with S2, resulting in the generation of a valid signature.
3. The principle of secrecy is upheld as the disclosure of S1, whether in an encrypted or nonsensical state, cannot expose the sensitive information to an unauthorized individual.
4. The protection of confidential information relies on the accurate generation of the private share and the utilization of the public share for document authentication.

Pixel	Share 1	Share 2	Probability
□	■□	■□	½
	□■	□■	½
■	■□	□■	1/2
	□■	■□	1/2

Figure 3. Mechanism for share generation

Step 2: In the case where the input image does not necessitate blocking and employs basis functions of varying lengths, the utilization of a wavelet-based technique becomes more pertinent and efficient for the progressive transmission of images. Furthermore, the wavelet-based technique facilitates compression of continuous tone and bi-level images, as well as large images. Moreover, it enables progressive transmission with pixel accuracy and resolution, facilitates content security. The cover image non-superimposing 8 × 8 blocks have intensity and resolution. A threshold mechanism eliminates a proportion (p) of the digitized image entries. Self-defined function defines pseudo-random hiding location in the high frequency band of both layers. Alternative blocks can withstand collusion assault.

Step 3: At the recipient's terminal, shares are combined to frame a legitimate document which validates an authorized sender.

C. METHOD FOR FINGERPRINT PROCESSING

The Passport Seva Kendra possesses a biometric authentication system that captures and verifies fingerprints. After obtaining the desired fingerprint images, two cryptographic keys (private and public) are generated from the image. The access to the public share is maintained in an unrestricted manner for all users. Now, this authenticated image is embedded in chip attached in the passport.

D. VERIFICATION PROCESS

On receiving the passport at the Airport, the face of the individual is taken and test for the match. Subsequently, the figure print and signature are taken and matched with the respective fingerprint and signature sensed from the corresponding regions of the facial image. Hence, the validation of the test is done from all aspects and the result authenticates the traveler.

E. WORKFLOW OF THE PROTOCOL FOR AUTHENTICATION

The pictorial representation of the proposed technique is shown in Fig. 4. Initially, the citizen applying for a passport approaches the Passport Seva Kendra with all the credentials. The biometric identity like facial image, retinal image, fingerprints and digital signature are taken. By using private share S1 of signature and F1 of fingerprint are embedded into the cover image. This authenticated image is saved in the chip embedded in the passport.

The image of face is recognized using Haar cascade classifier. On successful recognition, the public shares S2` and F2` from the collected signature and fingerprint are generated and fed to the extraction algorithm to reframe the signature and finger print. These fingerprint and signature are matched with the given ones at all the international entry and exit points such as Airport, International Border Check Posts with the neighboring countries, etc. to prove the authenticity.

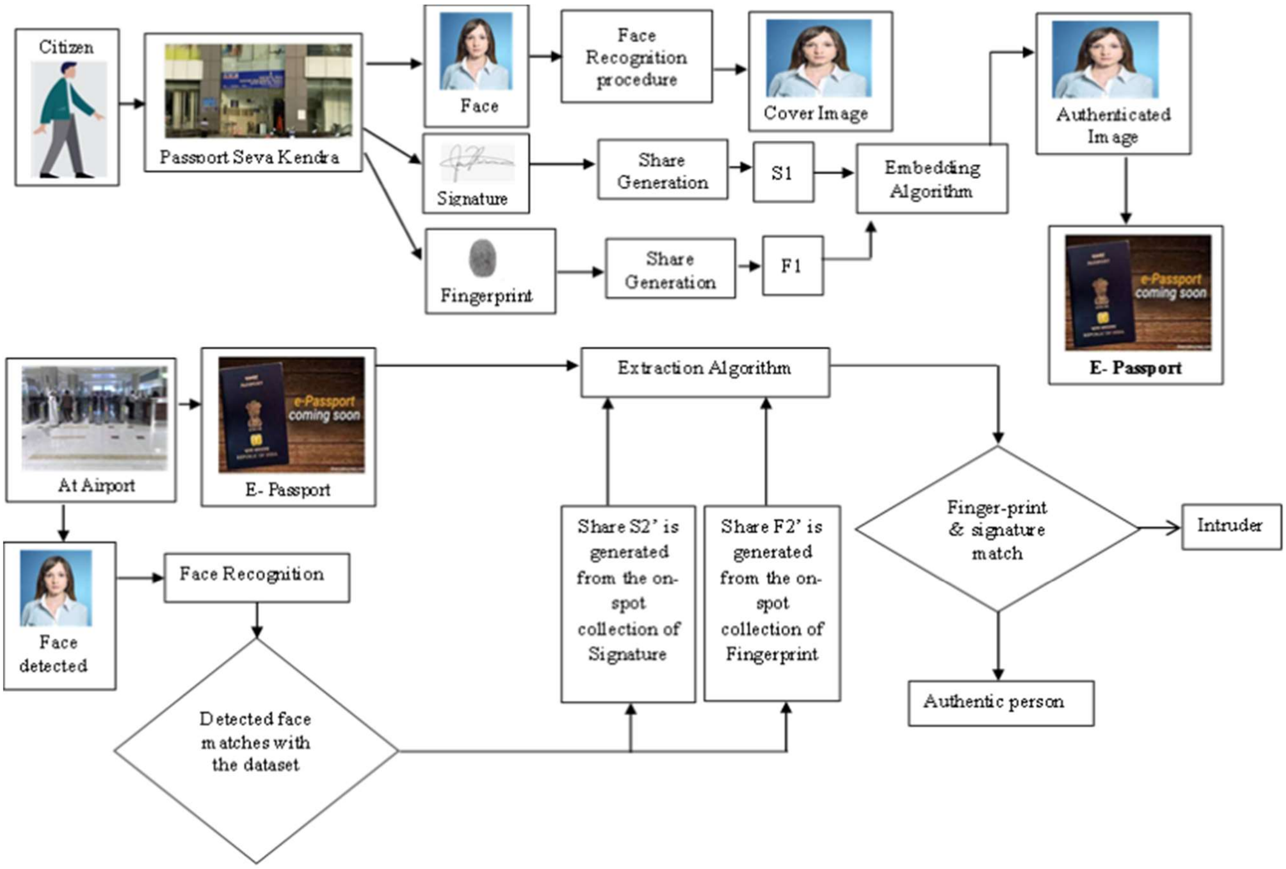


Figure 4. The work flow of the authentication process

VI. THE ALGORITHM

A. HAAR CASCADE CLASSIFIER

Paul Viola and Michael Jones presented Haar cascade classifier [49, 50] (Fig. 5) for object detection. It uses machine learning to train a cascade function from many positive and negative images. First two are edge-detection characteristics. Next two are "Line features" and the last is "four rectangle features" for slanted lines. With .jpg photos, real-time negative image training was done with OpenCV. The database stores positive images separately. Resizing photos during dataset training might cause errors, therefore simplifies the procedure. After training, the classifier can distinguish objects in new photos or videos. The algorithm searches the image with a sliding window at multiple scales and positions, applying the learned classifier to each window to determine if it contains the object of interest.

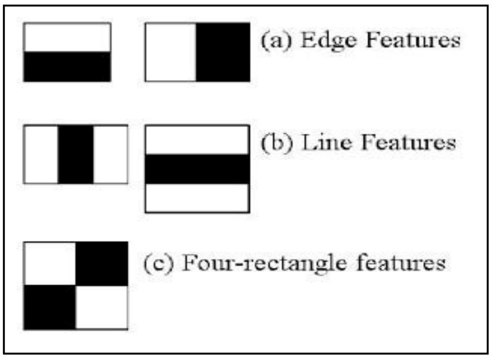


Figure 5. Haar features used for face detection

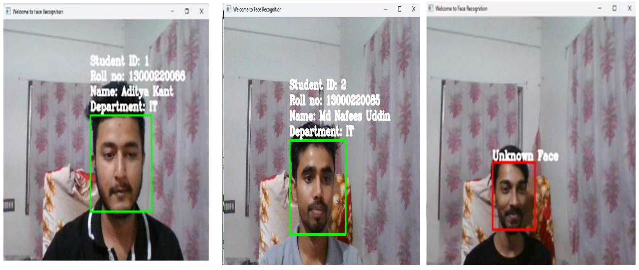
B. CONVOLUTIONAL NEURAL NETWORKS (CNNS)

Therefore, the number of hits is 12/24 for the first two cases but only 8/24 for the third case. So, the system accuracy is 50% for the first two cases and quite less for the third case as in Table 1.

Table 1. Accuracy of Face Recognition.

SN	Person 1	Person 2	Person 3
1	1		1
2	1	1	
3			
4	1	1	
5			1
6	1		
7		1	1
8	1	1	
9			1
10			

In the event that the embeddings are found to be a match, the facial features are successfully identified and subsequently presented alongside the corresponding individual's name. Conversely, if the embeddings fail to align, no visual output is generated. It is given in Fig. 6.


Welcome to Face Recognition
Welcome to Face Recognition
Welcome to Face Recognition

Student ID: 1
Roll no: 13000220066
Name: Aditya Kant
Department: IT

Student ID: 2
Roll no: 13000220085
Name: Md Nafees Uddin
Department: IT

Unknown Face

Figure 6. User interface

C. ILLUSTRATION OF SIGNATURE AND FINGERPRINT PROCESSING

The proposed technique is shown in Fig. 7. The algorithm implementation is elucidated in seven consecutive sub-sections.

C.1 THRESHOLD VALUE DETERMINATION

One of the input payloads, i.e., the digital signature is cleaned using a threshold value T as derived in (3).

$$T_I = \sum Pi \,/\, n,$$

where Pi denotes the intensity of the pixels and n is the number ofpixels of the input image.

$I_1 = \sum Pi$ when $Pi \leq T$, t = t +1 for every true case.
$I_2 = \sum Pi$ when $Pi > T$.
$S_1 = I_1/t, S_2 = I_2/(n\text{-}t)$
$T_N = (S_1 + S_2)/2.$ (3)

C.2 SIGNATURE CLEANING PROCESS

The payload in question refers to a born digital signature and a cleaning mechanism is deployed to ensure its integrity.

$$PI(x, y) < T_N \ ?\ NP_i(x, y) = 0 : NP_i(x, y) = 255 \qquad (4)$$

The signal intensity at the position (x, y) of the payload is denoted as PI(x, y). The function $NP_i(x, y)$ represents the adjusted monochromatic values, i.e., NP_i specifies black and white values only.

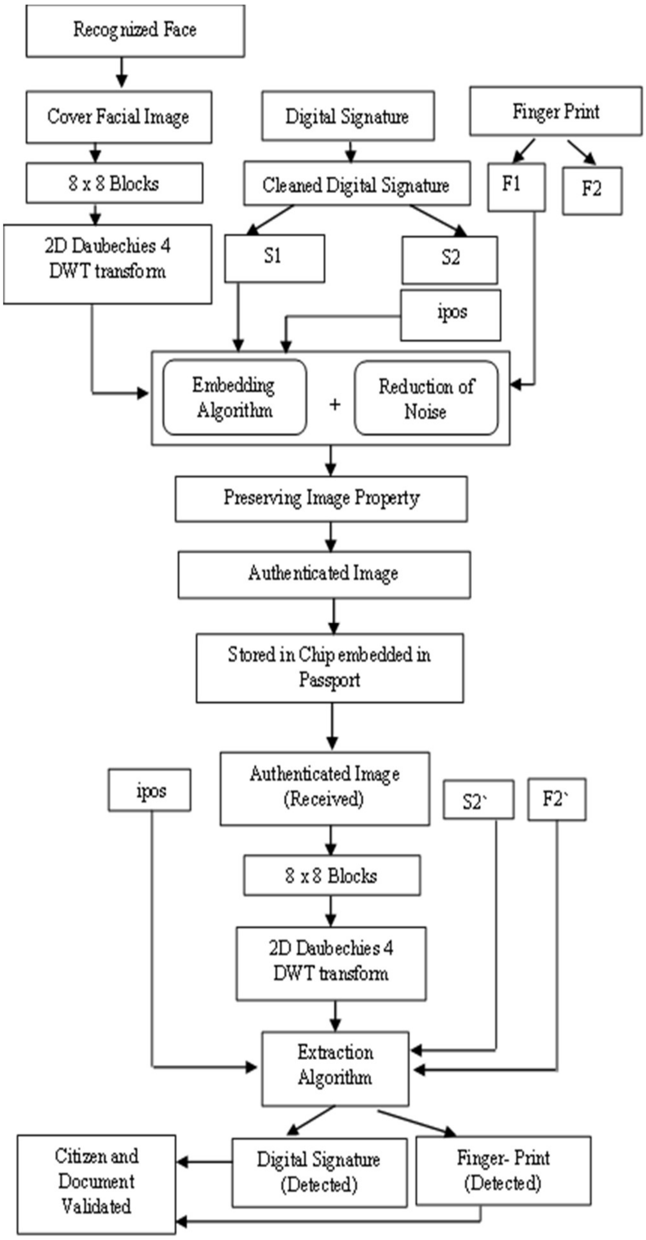

Recognized Face
Cover Facial Image
Digital Signature
Finger Print
8 x 8 Blocks
Cleaned Digital Signature
F1
F2
2D Daubechies 4 DWT transform
S1
S2
ipos
Embedding Algorithm
+
Reduction of Noise
Preserving Image Property
Authenticated Image
Stored in Chip embedded in Passport
ipos
Authenticated Image (Received)
S2`
F2`
8 x 8 Blocks
2D Daubechies 4 DWT transform
Extraction Algorithm
Citizen and Document Validated
Digital Signature (Detected)
Finger- Print (Detected)

Figure 7. The algorithm

C.3 SHARE CREATION

The method of share creation is shown in Fig. 8. The intensity value, i.e., PI(x, y) governs the generation of the shares from digital signature and fingerprint. The mathematical expression for generating S1 and S2 from digital signature can be represented by the following formula:

(NPi (x, y) = 0)? S1(x, 2 x (y - 1)) = 255;
S1(x, 2 x y) = 0,
S2(x, 2 x (n — 1)) = S1(x, 2 x y),
S2(x, 2 x y) = S1(x, 2 x (y - 1)) :
(mod(random ([x, y]); 2) == 0) ? S1(x; 2 x (y-1))= 255,

S1(x, 2 x y)= 0, S2(x , 2 x (y -1)) = S1(x, 2 x (y - 1)) , S2(x, 2 x y)= S1(x, 2 x y) : S1(x, 2 x (y-1)) = 0;
S1(x, 2 x y) = 255; S2(x, 2 x (y - 1)) = S1(x, 2 x (y-1)), S2(x, 2 x y)) = S1(x, 2 x y); (5)

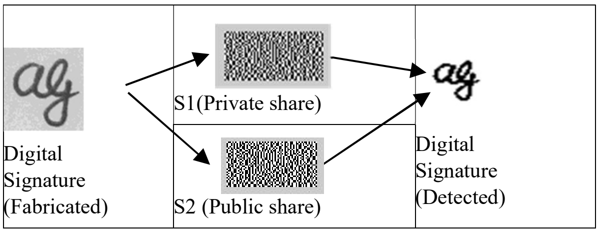


Figure 8. Share generated from a digital signature

The mathematical expression for generating F1 and F2 from the fingerprint can be derived as follows. The shares are computed using an 8 digit passport number (PN) and a 15 digit serial number (SN) in the following way:

F1 = [∑(PN + SN) + ∑(Digits of PN) + ∑(Digits of SN)] Mod 4 + 1
F2 = [|(RN - SN)| |(rev(RN) – rev(SN))|] Mod 4
(F1 > T_N)? (F1 = 0): (F1 = 255)
(F2 > T_N)? (F2 = 0): (F2 = 255) (6)

C.4 PSEUDO-RANDOM POSITION FOR INSERTION

The embedding of S1 and F1 in the cover image can be achieved at positions derived pseudo-randomly. The positions can be generated using this algorithm:
At first a pseudo-random variable is denoted with value 0.

1. The variable B denotes the current block number and is represented as a set of 8 bits.
2. B` denotes the reverse order of B.
3. The variable "ipos" represents a pseudorandom variable and will store the computed value of the pseudorandom position for each block:

I_i = Binary of B`; i varies from 1 to 8:
a = $I_4I_3I_2I_1$, b = $I_8I_7I_6I_5$.
$X_1 = (I_4I_3I_2I_1) \oplus (I_8I_7I_6I_5) = X_{11}X_{12} X_{13}X_{14}$ (7)
$P_1P_2 = (X_{11}X_{12}) \oplus (X_{13}X_{14})$
ipos = Dec(P_1P_2).

C.5 GENERATION PROCEDURE

Input: The cover is an image represented as a set of non-overlapping sub-blocks each size 8x8 and the secret data is the shares generated from signature and fingerprint.

Output: An authenticated image.

The following steps are repeated for the generation of full payload.

1. The sub-blocks are subjected to a two-level D4/db2 wavelet in a sliding window pattern. The generation process exclusively employs the integer component of the HH1 coefficient and four coefficients of HH1 from a selected block.
2. The individual bits of the shares are sequentially scanned and subsequently synthesized.

(Iv == 0) && (ipos == I)? The bit value at position ipos of P(x, y) is replaced by 0: continue.
(Iv == 255) && (ipos == I)? The bit value at position ipos of P(x, y)is replaced by 1: continue. (8)

Mathematically, this change in intensity level is expressed as: P`(x, y) = P(x, y) + α × (0/1), where P(x, y) is the host signal, P`(x, y) is the modified signal. α is the scaling factor measuring the strength of Iv. The possible value of (x, y) is ((1, 1), (2, 2), (2, 3), (3, 2), (3, 3)).

3. By adjusting parameter α, it is possible to dampen the variation of signal intensity. Toggling the bits in the frequency component located to the right of ipos to their opposite values—from 1 to 0 or from 0 to 1 - modifies the binary stream. Mathematically speaking, it can be expressed as follows:

P`(x, y) == (h($I_v$, ipos)) ? (α = |(P`(x, y)— I_v)|): 0;
If (α ≤ 0) ? No change: Alteration is done as mentioned. (9)

4. The block is retransformed into an authenticated form in the spatial domain using the Inverse Daubechies Discrete Wavelet Transform (D4/db2 wavelet). In order to preserve the integrity of the image properties, specific adjustments are made to the adverse blocks.
5. The authenticated block is repositioned to its initial coordinates within the output image.

C.6 RETENTION OF IMAGE PROPERTY

The present block has had the hiding technique applied again, and the adverse authenticated pixel value has been corrected if needed. One way to make the procedure easier is to use a threshold variable T.

It is observed that the generated authorized pixels comprise values between 0 and 255 given the range of spatial values [0, 255]. The difference between zero and the highest negative pixel value can be used to compute the offset Q1. To calculate Q2, deduct 255 from the maximum value of a pixel that has been observed. The logical OR operation between Q1 and Q2 can be used to represent the variable D. The following guidelines are followed while adjusting the spatial values: (1) A reduction of 2 D is applied to values lying within the range [(255-T), 255)], (2) A D increase is applied to values falling within the range [0, T], and (3) A D increase is applied to values falling within the mid-range of [(T, 1), ((255-T)].

C.7 DETECTION PROCEDURE

Input: An authenticated image.
Output: Digital Signature and Fingerprint.

The input image is divided into a set of 8x8 non-overlapping blocks, which may then be accessed using a sliding window mechanism. Until the complete share is successfully recognized, the iterative procedure is continued. The D4/db2 wavelet is performed on the current sub-block.

We only choose the integer portion of the cell frequency components ((1, 1), (2, 2), (2, 3), (3, 2), and (3, 3)) in order to detect generated bits. The pseudo-random position generation follows the same rule as described in the generated process. The generated bits are converted into binary representations of (0 - 0) and (1 - 255) and correctly identified inside the respective cellular contexts.

The detection process can be represented as follows:
(ipos==I) && (PI'(x, y))==0)?(Iv'(w)=0):continue. (10)
(ipos==I) && (PI'(x ,y))==1)?(Iv'(w)=255):continue.

The expression Iv'(w) can be represented as

$$(PI'(x, y) - PI(x, y))/(\alpha \times PI(x, y)). \tag{11}$$

Once all the values have been fully detected, the variables are converted into a two-dimensional format. Internally, the receiver's share S2 and F2 are combined with S11 and F11 to produce a valid signature and fingerprint at the receiver's end.

The established signature and fingerprint have been officially validated, thereby endorsing the principle of visual cryptography.

VII. EXPERIMENTAL RESULTS

The overall system is divided into three tier approach. First, the process of facial recognition is performed. On approval, the second and third authentication methods are justified with fingerprint and digital signature. Here the first subsection A illustrates facial recognition results and the subsequent section B depicts the fingerprint and signature-oriented result is achieved.

A. SIMULATION RESULTS RELATED TO FACE RECOGNITION

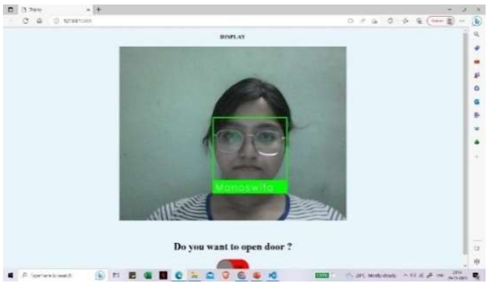
The process of facial recognition is applied to each individual's facial image that is acquired via the camera. The database contains a collection of verified images belonging to authorized individuals who have been granted access privileges. In the context of real-time image recognition, upon successful matching of an image from the database, the identified individual's facial features are promptly displayed alongside their corresponding name through a live streaming mechanism integrated within the webpage.

Table 2. Comparison for Face Recognition

Sl No	Tuli(Canditate)	Richa(Candidate)	Unknown
1	1		
2	1		
3	1		
4		1	
5	1		
6	1		
7	1		
8		1	
9	1		
10			1
11	1		
12	1		
13			1
14	1		
15			1
16	1		
17		1	
18	1		
19	1		
20	1		
21		1	
22	1		
23	1		
24		1	
25	1		
26	1		
27	1		
28		1	

Face recognition

A comprehensive evaluation is conducted to assess the efficacy of the face recognition system. In our dataset, we have a limited sample size consisting of two individuals namely Tuli and Richa. The accuracy test was conducted exclusively with the presence of Tuli within the camera frame for duration of 30 seconds. The tabular data in Table 2 shows the accuracy metrics of the face recognition system implemented utilizing OpenCV.



Do you want to open door ?

Figure 9. User interface

Therefore, the number of hits for Tuli is 19/28 and the number of misses is 8/28. The System Accuracy is 68%. The system operates at a frame rate of 1 frame per second, and the resulting output is displayed in real-time on the designated display page, as depicted in Fig. 9.

The observed decrease in accuracy can be attributed to a multitude of factors, including but not limited to:

- The laptop camera exhibits a limited field of view, resulting in significant pixelation for faces positioned at a certain distance.
- Insufficient lighting conditions may impede accurate facial detection, thereby giving rise to erroneous positive identifications.
- The functionality of the prototype is impaired during nocturnal hours. In order to achieve enhanced performance and superior image resolution, the utilization of infrared cameras of higher cost and superior quality becomes imperative.

For this reason, the system should not depend only on face recognition, but when the accuracy rate is more than 60% the additional confirmation is required through fingerprint and signature verification. To assure, the proposed prototype is secure enough to be applied as it cannot be easily broken by brute force.

B. EXPERIMENTAL RESULTS RELATED TO SIGNATURE AND FINGERPRINT AUTHENTICATION

The proposed scheme guarantees a heightened level of security. The generated shares exhibit no discernible resemblance to the underlying secured data, nor can one share be reliably predicted based on another.

Based on the visual representation provided, it is apparent that neither of the distributions of shares bears resemblance to the original source signature in terms of pixel distribution. Furthermore, it is exceedingly challenging for an observer to anticipate the correlation between two images based on their pixel distribution. Furthermore, the inherent dual randomness in the allocation of pixels for shares derived from a pristine digital signature effectively diminishes the likelihood of generating duplicate pairs of shares. According to the proposed methodology, the magnitude of a share is precisely twice the magnitude of a processed digital signature. Given the dimensions of a sensitive image (signature or fingerprint), M and N, it follows that the total number of potential combinations for prediction is 2(M*N). While this can be computed mathematically, it is not feasible to achieve in practice within a reasonable time frame.

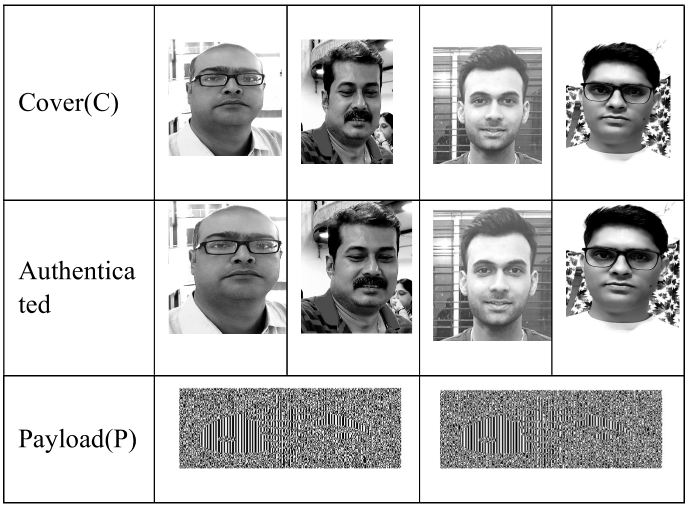


Figure 10. Visual interpretation

The following section elucidates the visual interpretation subsequent to conducting experiments on the cover images, namely Saikat, Shamboo, Partha, Shubham, Yasraj, Tuli, Jitendra, etc., using the proposed algorithm and the assessment of the algorithm performance utilizing the image quality metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Information Fidelity (IF), and Correlation Coefficient (CC). Figure 10 shows the visual representation of certain cover and authenticated images. The cover image (C) has dimensions of 512x512, while payload (share of signature and fingerprint) has dimensions of 70x70 & 70x70, respectively. As part of the payload (P), each of the shares is represented as 2S.

Based on the visual representation, it is evident that disparity between the source and authenticated image in terms of the Human Visual System (HVS) is minimal. This similarity is maintained even though the concurrent concealment process is applied to the high frequency regions of the resolution levels at two levels.

Furthermore, implementing appropriate and essential modifications to the cover image subsequent to the generation of the share facilitates the achievement of lossless reconstruction of the authenticating image. The process of experimentation involves manipulating the intensity of adjustments in the concealing formula and subsequently evaluating the resulting authenticating signals. This will help to modulate the level of white noise in order to optimize imperceptibility while maintaining robustness.

Fig. 11 shows the signal strengths of the shares belonging to signature and fingerprint formed and reformed. Series 1 – 4 depict the shares from the signature and series 5 – 8 depict the scenario for fingerprint. It is noticeable that the effects before and after are not distinguishably different.

Further, in Fig. 12 we have illustrated the impact of intensity adjustment after the generation procedure. The optimal scenario is evaluated at i and 2i time, while for all other time points, the graphical disparity is notably pronounced.

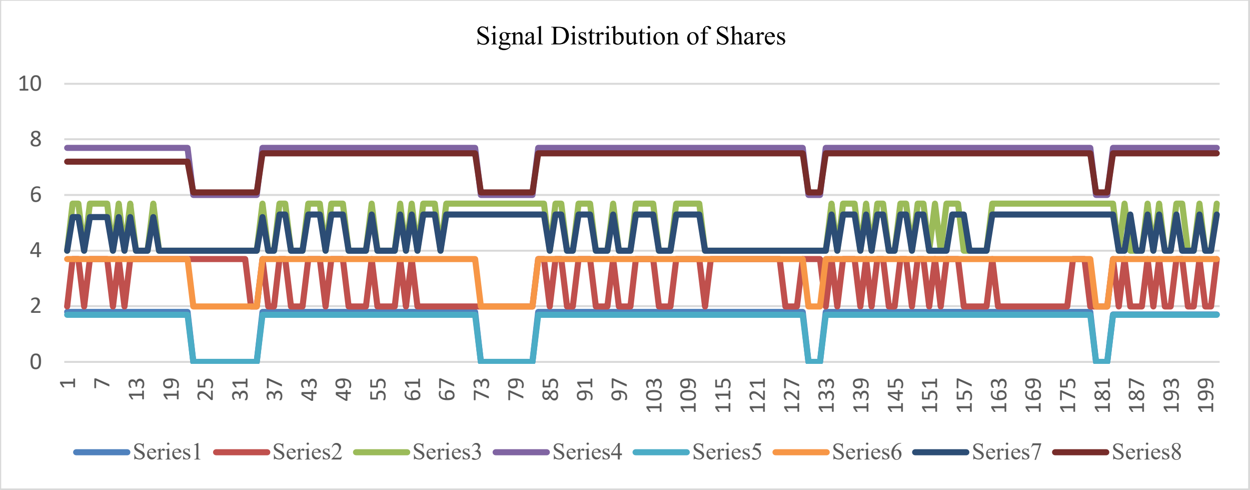


Figure 11. Signal Strength

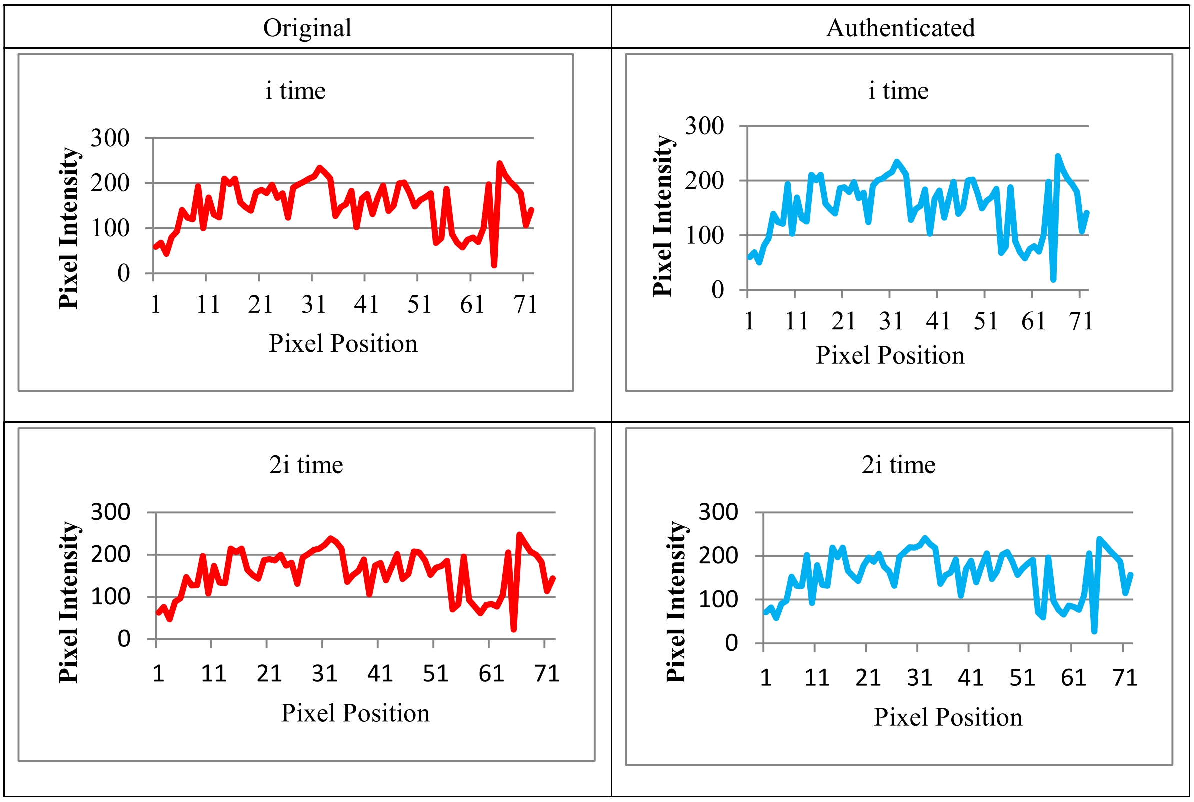


Figure 12. Comparison of generation intensity at time *i* and 2*i*

The final section delineates the algorithmic efficiency pertaining to the quality metrics, namely Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Information Fidelity (IF), Structural Similarity Index (SSIM) and Cross-Correlation (CC), as illustrated in Table 3.

Table 3. Analysis using Quality Metrics

Source Image	Capacity (in bytes)	MSE	PSNR	IF	SSIM	CC
SAIKAT	10240	6.2211	39.14	0.9911	0.9946	0.9979
SHAMBO		7.5246	38.42	0.9818	0.9874	0.9983
PARTHA		6.2531	39.01	0.9901	0.9849	0.9989
SHUBHAM		7.5017	38.01	0.9934	0.9979	0.9964
YASRAJ		8.4260	37.24	0.9845	0.9960	0.9950
TULI		8.0015	37.90	0.9919	0.9976	0.9914
JITENDRA		8.2357	37.63	0.9952	0.9932	0.9971
RAJA		7.6214	38.13	0.9892	0.9917	0.9926
RANA		8.3016	37.54	0.9927	0.9969	0.9962
SANJAY		8.3798	37.19	0.9890	0.9968	0.9981
PANNA	10.6814	35.18	0.9896	0.9980	0.9968	10.6814
SHAMI	9.9812	35.87	0.9949	0.9887	0.9934	9.9812
POOJA	7.7651	38.03	0.9910	0.9817	0.9910	7.7651
RICHA	9.0871	36.76	0.9856	0.9956	0.9954	9.0871
GHIZALA	8.0011	37.98	0.9918	0.9964	0.9918	8.0011
ASMIK	8.1322	37.61	0.9901	0.9932	0.9954	8.1322

Under typical conditions, a Peak Signal-to-Noise Ratio (PSNR) exceeding 35 dB is generally regarded as satisfactory. The algorithm is designed in a manner that effectively achieves a satisfactory average Peak Signal-to-Noise Ratio (PSNR) value of 37.61 dB. This is despite the fact that a substantial amount of data concealment is performed at two different levels simultaneously.

Furthermore, the Mean Square Error (MSE), Image Fidelity (IF), Structural Similarity Index Matrix (SSIM), and Correlation Coefficient (CC) exhibit average values of 8.1322, 0.9901, 0.9932, and 0.9954, respectively. The present analysis provides a rationale for incorporating techniques that reduce noise and minimize distortion in order to ensure the successful restoration of signature and fingerprint, thereby validating visual authentication.

The proposed approach entails the integration of visual cryptography with data authentication. The reconstructed image exhibits an augmented pixel expansion, thereby amplifying the quantity of black sub-pixels corresponding to the white pixel. This alteration illustrates a decrease in image resolution and an increase in file size. The algorithm under consideration facilitates the generation of time-varying shares derived from a meticulously processed signature and fingerprint, thereby guaranteeing optimal contrast and randomization.

In the event of an unidentified facial recognition, unmatched fingerprint and signature of the user retains the option to refrain from initiating entry access.

In this experiment, we successfully integrated an SG 90 Micro servo motor with an ESP 8266 microcontroller, as depicted in Fig. 13. The button serves as a mechanism for regulating the locking and unlocking functionalities. A solenoid lock, resembling a physical lock, can be employed to operate in a comparable manner. Table 4 shows the hardware connection of SG 90 motor.

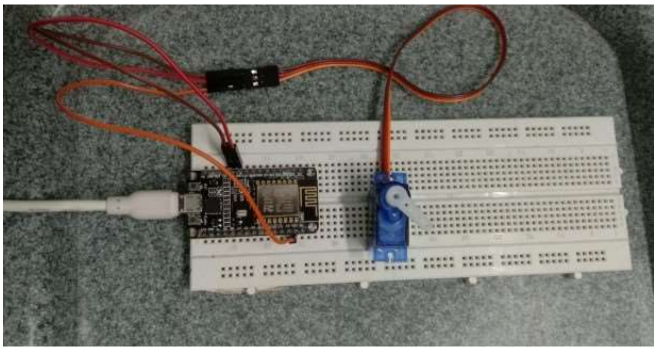


Figure 13. Hardware connection

Table 4. Hardware pin connection

ESP8266	**SG 90 Micro Servo Motor**
3v3	VCC
GND	GND
D3	Signal

VIII. COMPARISON WITH SOME OF THE EXISTING TECHNIQUES

Aneesa Tankasali et all. in their work [11] used a Raspberry Pi camera instead of a normal Webcam. However, using Raspberry Pi leads to several problems and can be overcome by using a normal Webcam. In the algorithm by Ivan Surya Hutomo et al. [13], Google Assistant integration used Dialog flow and Firebase for the Integration of face recognition and the smart gate.

A concerted endeavor is also undertaken to bolster the efficacy of the proposed algorithm through a comparative analysis with the selected analogous algorithms that currently exist. The comparative analysis is conducted with respect to the mean Peak Signal-to-Noise Ratio (PSNR) value, as depicted in Table 5. Upon observation, it is noted that the algorithm under consideration exhibits enhanced performance when employing a 2-level resolution, in contrast to algorithms A, B, and C which only utilize a 1-level resolution. Furthermore, the concealment capacity of the proposed algorithm is found to be approximately equivalent to that of algorithms A, B and C. When comparing algorithm D to G, it is observed that there is an improvement even with a 2-level resolution. The DWT exhibits notable efficacy when juxtaposed with a comparable methodology employing the Haar DWT, as elucidated in H. A histogram analysis is shown in Fig. 14.

Table 5. Comparative Study with Similar Techniques

SL NO	**ALGORITHM**	**LEVEL OF RESOLUTION**	**AVG. PSNR (in dB)**
A	[26]	1	34.60
B	[36]	1	39.42
C	[51]	1	38.52
D	[38]	2	36.14
E	[52]	2	26.30
F	[53]	2	33.08
G	[54]	2	36.04
H	[55]	2	36.14
I	Proposed Algorithm	2	37.61

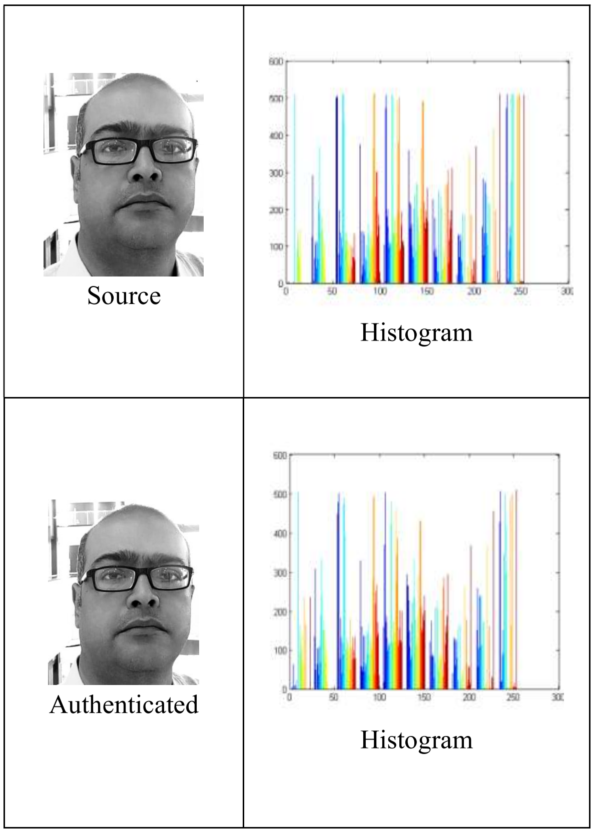


Figure 14. Histogram Analysis

IX. PERFORMANCE AGAINST VARIOUS ATTACKS

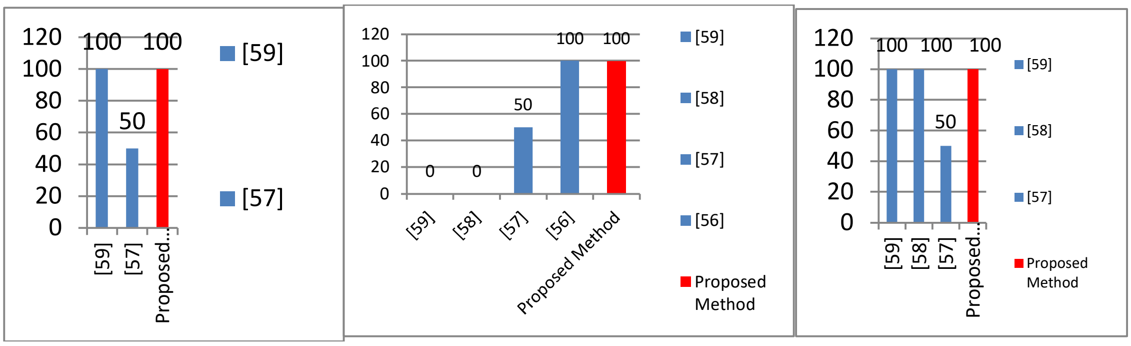
The algorithm under consideration exhibits notable resilience against various associated attacks and demonstrates efficacy in the realm of legal copyright technology, as will be elaborated below. For evaluating the robustness of this scheme various attacks are applied on the signature generated e-Passport and the quality of the four best extracted signatures are examined to assess the attack impact. Since attacks normally alters the pixel byte values of the signature coded e-

Passport image so possible alteration of hidden data bits on the concern pixel byte values. Hence, significant amount of destruction is possible for extracted signatures and in this aspect the best copy of each extracted signature is identified by judging the similarity between the extracted signature and its original form. This signature quality evaluation is first reflected in Table 6, which clearly shows better extraction of signatures under different image processing attacks. In this aspect the CC value of the four best extracted signatures are reflected in Table 6 for each attack and they are compared with the existing works reflecting better signature extraction. It is important to note that all the metrics of the attacks shown in Table 6 generally demonstrate good signature recovery with higher CC values of four extracted signatures.

Vitally, this superior signature extraction is mainly possible due to variable threshold range driven signature bit encoding on different pixel bytes resulting in variable attack impact on different pixel bytes. Hence, this scheme clearly promotes good signature recovery through Table 6. Apart from this the bar chart shown in Fig. 15 definitely reflects excellent recovery of the number of signatures under various attacks based on the threshold CC value > 0.7. Here Fig 15 highlights a comparison of the number of signature recoveries in contrast to the existing approaches on the basis of extracted signature CC values >0.7 against specific attacks. The percentage recovery for three different attacks, namely Salt & Pepper Noise, Cropping and Translation is shown in Fig 15 in graphical form. W_x with CC Values greater than 0.7 are taken into consideration.

Table 6. Result Analysis after Attacks

Attack	Attack %	Works	CC value			
			W_1	W_2	W_3	W_4
Salt & Pepper Noise (D is Noise Density)	D = 15%	[59]	0.8213	0.8458	-	-
	D = 10%	[57]	0.81	0.41	-	-
	D = 5%	Proposed Method	**0.9431**	**0.9512**	**0.9612**	**0.9449**
Cropping (Row * Column)	-	[59]	0.6981	0.4780	-	-
	-	[58]	0.3264	0.3650	-	-
	-	[57]	0.64	0.84	-	-
	-	[56]	0.9794	0.9810	0.9726	-
	(60 * 60)	Proposed Method	**0.95**	**0.92**	**0.93**	**0.97**
Translation	-	[59]	0.7265	0.8361	-	-
	-	[58]	0.9496	0.9679	-	-
	-	[57]	0.38	0.98	-	-
	[0.4,0.4]	Proposed Method	**0.94**	**0.95**	**0.97**	**0.91**
Row - Column Manipulation (Row * Column)	-	[59]	0.6760	0.6389	-	-
	-	[58]	0.6716	0.6665	-	-
	(20 * 20)	[56]	0.9478	0.9676	0.7412	
	(60 *60)	Proposed Method	**0.9761**	**0.9179**	**0.9476**	**0.9868**
Sharpen	-	[58]	0.9128	0.9565	-	-
	-	[57]	0.93	0.95	-	-
	5 %	Proposed Method	**0.9294**	**0.8127**	**0.8941**	**0.8239**
Smooth	-	[58]	1	1	-	-
	-	[57]	0.96	1	-	-
	30 %	Proposed Method	**0.9686**	**0.9482**	**0.9792**	**0.9815**



Salt & Pepper Noise **Cropping** **Translation**

Figure 15. Comparison of Signature Recovery based on CC Threshold Value>0.7 Under Different Attacks

X. CONCLUSION

The primary goal of the proposed methodology is to guarantee and strengthen data security through a streamlined approach, involving facial recognition through machine learning technique. The efficacy of the algorithm is predicated upon its ability to enhance the feature of losslessness while simultaneously exhibiting heightened robustness and minimal visual artifacts. The statistical detection of the secret share is highly challenging due to the presence of a pseudo-random generation position. In the event that the secret share is detectable, its utility is rendered null unless it is combined with the complementary component, which is only obtained from the authorized person. The payload exhibits a considerable magnitude, while the cover image remains minimally affected, enabling accurate payload detection at the recipient's end in the absence of the original image. The impact of the control technique on optimization in noise reduction is a critical consideration. Additionally, the implementation of an encryption technique plays a pivotal role in ensuring robust security against potential brute force attacks. Therefore, this algorithm exhibits potential applicability in the domains of copyright protection and human authentication.

References

[1] T. Tsui, X.-P. Zhang, D. Androutsos, “Color image watermarking using multidimensional Fourier transformation,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16-28, 2008, https://doi.org/10.1109/TIFS.2007.916275.

[2] S. Behnia, M. Teshnehlab, P. Ayubi, “Multiple watermarking scheme based on improved chaotic maps,” *Communication in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2469-2478, 2010. https://doi.org/10.1016/j.cnsns.2009.09.042.

[3] J. Liu, J. Li, J. Ma, N. Sadiq, U. A. Bhatti, Y. Ai, “A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map,” *Applied Sciences*, vol. 9, no.700, pp. 1-23, 2019, https://doi.org/10.3390/app9040700.

[4] I. J. Cox, M. L. Miller, J. A. Bloom, Digital Watermarking, Morgan Kaufmann, 1999.

[5] H. Dehgan, S. E. Safavi, “Robust image watermarking in the wavelet domain for copyright protection,” ICEE 2010, https://doi.org/10.48550/arXiv.1001.0282.

[6] Definition of PASSPORT. [Online]. Available at: www.merriam-webster.com.

[7] P. Cane, J. Conaghan, The New Oxford Companion to Law, London: Oxford University Press, 2008. https://doi.org/10.1093/acref/9780199290543.001.0001.

[8] The electronic passport in 2021 and beyond, Thales Group, 2021.

[9] C. Li, Z. Qi, N. Jia, J. Wu, “Human face detection algorithm via Haar cascade classifier combined with three additional classifiers,” *Proceedings of the 2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)*, 2017, pp. 483-487, https://doi.org/10.1109/ICEMI.2017.8265863.

[10] T. H. Iwan, H. M. Fahrezy, R. P. Merliasari, “The design and the implementation of security system office door using Raspberry Pi face detection,” *Proceedings of the 1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019), Advances in Social Science, Education and Humanities Research*, vol. 410, pp. 307-311, 2020. https://doi.org/10.2991/assehr.k.200303.074.

[11] K. Gupta, N. Jiwani, Md H. U. Sharif, M. A. Mohammad, N. Afreen, “Smart door locking system using IOT”, *Proceedings of the 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2022, pp. 1-4. https://doi.org/10.1109/ICACCM56405.2022.10009534.

[12] P. Elachi, E. Okowa, U. Ekwueme, “Facial recognition based smart door lock system,” Journal of Scientific and Industrial Research, vol. 6, issue 2, pp. 95-105, 2022.

[13] I. S. Hutomo, H. Wicaksono, “A smart door prototype with a face recognition capability,” *IAES International Journal of Robotics and Automation (IJRA)*, vol. 11, no. 1, pp. 1-9, 2022. https://doi.org/10.11591/ijra.v11i1.pp1-9.

[14] P. Elechi, E. Okowa, U. Ekwueme, “Facial recognition based smart door lock system,” *FUPRE Journal of Scientific and Industrial Research*, vol. 6, no. 2, pp. 95-105, 2022.

[15] C.-S. Lu and H.-Y. M. Liao, “Multipurpose watermarking for image authentication and protection,” *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579-1592, 2001, https://doi.org/10.1109/83.951542.

[16] M. Borda, I. Nafornita, “Digital watermarking – Principles and applications,” Proceedings of the International Conference on Communications, 2004, pp. 41–54, 2004.

[17] A. Shamir, “How to share a secret,” *Communication of the ACM*, vol. 22, no. 11, pp. 612–613, 1979. https://doi.org/10.1145/359168.359176ю

[18] D. R. D. Brabin, J. R. P. Perinbam, D. Meganathan, “A block based reversible data hiding scheme for digital images using optimal value computation,” *Wireless Pers Commun*, vol. 94, pp. 2583–2596, 2017. https://doi.org/10.1007/s11277-016-3817-4.

[19] C. W. Lee, W. H. Tsai, “A secret-sharing-based method for authentication of grayscale document images via the use of the PNG image with a data repair capability,” *IEEE Transactions on Image Processing*, vol 22, no. 1, pp. 207–218, 2012, https://doi.org/10.1109/TIP.2011.2159984.

[20] X. Gao, X. Li, D. Tao, C. Deng, J. Li, “Robust reversible watermarking via clustering and enhanced pixel-wise masking,” *IEEE Transactions on Image Processing*, vol. 21, no. 8, pp. 3598–3611, 2012. https://doi.org/10.1109/TIP.2012.2191564.

[21] J. J. K. O. Ruanaidh, T. Pun, “Rotation, scale and translation invariant spread spectrum digital image watermarking,” *Signal Processing*, vol. 66, no. 3, pp. 303–317, 1998, https://doi.org/10.1016/S0165-1684(98)00012-7.

[22] M. A. Suhail, M. S. Obaidat, “Digital watermarking-based DCT and JPEG model,” *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640–1647, 2003. https://doi.org/10.1109/TIM.2003.817155.

[23] G. Coatrieux, L. Lecornu, Ch. Roux, & B. Sankur, “A review of image watermarking applications in healthcare,” *Proceedings of the 28th IEEE Annual International Conference on Engineering in Medicine and Biology Society, EMBS'06*, 2006, pp. 4691–4694. https://doi.org/10.1109/IEMBS.2006.259305.

[24] W. Bender, D. Gruhl, N. Morimoto, A. Lu, “Techniques for data hiding,” *IBM Systems Journal*, vol. 35, no. 3–4, pp. 313–336, 1996, https://doi.org/10.1147/sj.353.0313.

[25] W. N. Lie, L. C. Chang, “Spatial domain image watermarking by data embedding at adaptive bit Position,” *Proceedings of the IPPR Conference on Computer Vision, Graphics and Image Processing*, 1999, pp. 16–21.

[26] L. Li, H. H. Xu, C. C. Chang and Y. Y. Ma, “A novel image watermarking in redistributed invariant wavelet domain,” *The Journal of Systems and Software*, vol. 84, no. 6, pp. 923–929, 2011. https://doi.org/10.1016/j.jss.2011.01.025.

[27] B. J. Mohd, S. Abed, T. Al-Hayajneh, S. Alounch, “FPGA hardware of the LSB steganography method,” *IEEE Transaction on Consumer Electronics*, 978-1-4673-1550-0/12

[28] P.-Y. Chen, H.-J. Lin, “A DWT based approach for image steganography,” *International Journal of Applied Science and Engineering*, vol. 4, issue 3, pp. 275-290, 2006. https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275

[29] P. Y. Chen, H. J. Lin, “A DWT based approach for image steganography,” *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.

[30] L. H. H. Herman, Image Compression using the haar wavelet transform. Plenum Press, 2001.

[31] Y. P. Chu, S. W. Guo, Y. K. Chan, H. C. Wu, “Image hiding based on a hybrid technique of VQ compression and discrete wavelet transform,” *Proceedings of the International Computer Symposium*, 2004, pp. 313–317.

[32] X. Song, F. Liu, C. Yang, X. Luo, Y. Zhang, “Steganalysis of adaptive JPEG steganography using 2D Gabor filters,” *Proceeding of 3rd ACM Workshop on Information Hiding and Multimedia Security*, USA, 2015, pp. 15-23. https://doi.org/10.1145/2756601.2756608.

[33] A. A. Abdelwahab, L. A. Hassan, “A discrete wavelet transform based technique for image data hiding,” Proceedings of the National Radio

Science Conference, NRSC 2008, Tanta, Egypt, 2008, pp. 1-9, https://doi.org/10.1109/NRSC.2008.4542319.

[34] P. Bao, X. Ma, "Image adaptive watermarking using wavelet domain singular value Decom-position," *IEEE Transaction on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96–102, 2005. https://doi.org/10.1109/TCSVT.2004.836745.

[35] S. P. Maity, M. K. Kundu, "A blind CDMA image watermarking scheme in wavelet domain," *Proceedings of the 2004 International Conference on Image Processing, 2004. ICIP'04.*, Singapore, 2004, pp. 2633-2636, https://doi.org/10.1109/ICIP.2004.1421644..

[36] L. H. Che, J. J. Lin, "Mean quantization-based image watermarking," *Image and Vision Computing*, vol 21, no. 8, pp. 717–727, 2003, https://doi.org/10.1016/S0262-8856(03)00067-2.

[37] T. C. Lin, C. M. Lin, "Wavelet-based copyright-protection scheme for digital images based on local features," *Information Sciences*, vol. 179, no. 19, pp. 3349–3358, 2009, https://doi.org/10.1016/j.ins.2009.05.022.

[38] M. Ali, C. W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWTSVD transform domain," *Signal Processing*, vol. 94, pp. 545–556, 2014, https://doi.org/10.1016/j.sigpro.2013.07.024.

[39] A. Al-Ha, M. Farfoura, "Providing security for e-government document images using digital watermarking in the frequency domain," Proceedings of the IEEE ICIM, 2019, pp. 77–81. https://doi.org/10.1109/INFOMAN.2019.8714674.

[40] L. Zhang, X. Yan, H. Li, & M. Chen, "A dynamic multiple watermarking algorithm based on DWT and HVS," *International Journal of Communications, Network & System Sciences*, vol. 5, pp. 490–495, 2012. https://doi.org/10.4236/ijcns.2012.58059.

[41] S. Chowdhury, S. Mistry, N. Ghoshal, "Multi phase digital authentication of e-certificate with Secure concealment of multiple secret copyright signatures," *Int. J. of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, 2019, pp. 3365–3380. https://doi.org/10.35940/ijitee.J1231.0881019.

[42] S. Bose, T. Arjariya, A. Goswami, S. Chowdhury, "Multi-layer digital validation of candidate service appointment with digital signature and bio-metric authentication approach," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 14, no. 5, pp. 81-100, 2022, https://doi.org/10.5121/ijcnc.2022.14506.

[43] I. Daubechies, *Ten Lectures on Wavelets*, Philadelphia: SIAM, 1992, https://doi.org/10.1137/1.9781611970104.

[44] G. R. Kuduvalli, R. M. Rangayyan, "Performance analysis of reversible image compression techniques for high resolution digital teleradiology," *IEEE Transactions on Medical Imaging*, vol. 11, no. 3, pp. 430–445, 1992. https://doi.org/10.1109/42.158947.

[45] J. M. Lina, "Image processing with complex Daubechies wavelets," *Journal of Mathematical Imaging and Vision*, vol. 7, no. 3, pp. 211–223, 1997, https://doi.org/10.1023/A:1008274210946.

[46] L. M. Patnaik, "Daubechies 4 wavelet with a support vector machine as an efficient method for classification of brain image," *Journal of Electronic Imaging*, vol. 14, issue 1, article ID 013018, 2005. https://doi.org/10.1117/1.1868003.

[47] M. Vetterli, J. Kovacevic, "Wavelets and sub-band coding," Englewood Cliffs, 1995, NJ: Prentice Hall PTR.

[48] T. W. Yue and S. Chiang, "A neural network approach for visual cryptography," *Proceedings of the IEEE International Conference on Neural Networks*, vol. 15, pp. 494–499, 2000, https://doi.org/10.1109/IJCNN.2000.861518.

[49] V. Bhutra, H. Kumar, S. Jangid, L. Solanki, "Door security using face detection and Raspberry Pi," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 331, no. 012011, 2018. https://doi.org/10.1088/1757-899X/331/1/012011.

[50] S. Roy, Md N. Uddin, Md Z. Haque, Md J. Kabir, "Design and implementation of the smart door lock system with face recognition method using the Linux platform Raspberry Pi," *JCSN – International Journal of Computer Science and Network*, vol. 7, issue 6, 2018.

[51] P. Patil, D. S. Bormane, "DWT based invisible watermarking technique for digital images," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 2, no. 4, pp. 603–605, 2013.

[52] Y. Dinesh, A. P. Ramesh, "Efficient capacity image steganography by using wavelets," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, no. 1, pp. 251–259, 2012.

[53] A. Chawla, P. Shukla, "A modified secure digital image steganography based on DWT using matrix rotation method," *International Journal of Computer Science and Communication Engineering*, vol. 2, no. 1, pp. 20–25, 2013.

[54] L. Li, H. H. Xu, C. C. Chang, Y. Y. Ma, "A novel image watermarking in redistributed invariant wavelet domain," *Journal of Systems and Software*, vol. 84, no. 6, pp. 923–929, 2011, https://doi.org/10.1016/j.jss.2011.01.025.

[55] A. Goswami, N. Ghoshal, "Imperceptible image authentication using wavelets," *International Journal of Network Security*, vol. 18, no. 5, pp. 861–873, 2016.

[56] I. Nasir, Y. Weng, J. Jiang, S. P. Ipson, "Multiple spatial watermarking technique in color images," Springer-Verlag London Limited, 2010, *Signal Image and Video Processing*, vol. 4, issue 2, pp. 145-154, 2010. https://doi.org/10.1007/s11760-009-0106-7.

[57] N. Mohananthini, G. Yamuna, "Performance comparison of single and multiple watermarking techniques," *I. J. Computer Network and Information Security (IJCNIS)*, vol. 7, pp. 28–34, 2014, https://doi.org/10.5815/ijcnis.2014.07.04.

[58] N. Mohananthini, G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," *Journal of Electrical Systems and Information Technology*, vol. 3, pp. 68-80, 2016.

[59] N. Mohananthini, G. Yamuna "Image fusion process for multiple watermarking schemes against attacks," *Journal of Network Communications and Emerging Technologies (JNCET)*, vol. 1, issue 2, pp. 1-8, 2015.

[60] M. Tyagi, Viola Jones Algorithm and Haar Cascade Classifier, Towards Data Science, July 13, 2021. [Online]. Available at: https://towardsdatascience.com/viola-jones-algorithm-and-haar-cascade-classifier-ee3bfb19f7d8

MR. SAIKAT BOSE is Masters in Computer Science (Embedded System) from MAKAUT in the year 2006. He had worked as Assistant Professor in Techno India for 12 years. Currently he is working as Controller of Examination in Techno Global University, Sironj. He is persuading his Research in computer Science Department, Bhabha university, Bhopal.

DR. TRIPTI ARJARIYA had done Ph.D (Computer Science) and has a teaching experience of 16 years. She has 59 Research Papers. Currently she is working as professor in Bhabha University, Bhopal. Her research area is about application of artificial Intelligence. She is also working as guide to many Research Scholars in University.

DR. ANIRBAN GOSWAMI is currently working as Asst. Professor and Asst. Registrar in Techno Main Salt Lake (An Engineering College under Maulana Abul Kalam Azad University of Technology), Kolkata, West Bengal, India. He has more than 22 years of teaching experience. He had contributed in more than 10 graduate level projects and has 15 international conference and 8 international journal publications. His area of research is Steganography, AI and Machine Learning.