International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-02, May 2019

Biometrics based Human Authentication

[*]Chaitra.P, [#]Sudha.H.Thimmaiah

[*]PG Student, [#]Assoc. Prof, Dr. Ambedkar Institute of Technology, Bangalore, India,

[*]chaitrabalu73@gmail.com, [#]sudha.tce.ait@gmail.com

Abstract - In Today's world, the increase in number of digital technology users escalated the need for a better authentication system. In order to provide privacy and confidentiality to the user information in various fields like Bank transactions, Military applications, Medical Fields etc., a well-organized mechanism that provides high security must be implemented. Biometric authentication is one of the efficient methods. In this regard, a double authentication procedure is explained in this paper. Here, at the transmitter end - Thumb Impression is encrypted by Chaos method and the resulting image is hidden in video–object webcam image by DWT Water marking technique. Before transmission, the Stego Video-Object Image is compressed by DCT technique. At the receiving end – the image is decompressed by IDCT and the image is decrypted by IDWT to recover the original message. The above recommended method has the advantage of improved security for various applications.

Keywords — Biometrics Hiding, Chaos Encryption, Discrete Wavelet Transform, Remote Authentication, Steganographic System

I. INTRODUCTION

For frequently exchanging the confidential information, a secured wireless communication with a good remote authentication is required [8]. The process that confirms the identity of the user who requested for access in a lossy communication channel is known as Remote user authentication Remote authentication is a procedure of submitting the encrypted information that also includes other audio and video data. This encrypted information includes inherence factors like (images/video of user face, audio of human voice, thumb impression etc.). Attacks on these communications of confidential information that also includes Remote authentication can create problems. To clear these issues, a double authentication method [14] for providing high security is necessary. In this direction, the proposed method with semantic segmentation, Cryptography (chaotic encryption), and Steganography (DWT watermarking) are proposed.

There are only two ways of authentication:

Positive Authentication: These are authenticating mechanisms that most of the existing system has.

Negative Authentication: These were introduced in the system to reduce the cyber-attacks in many of the communication systems [16].

In this proposed scheme the positive authentication methods and also elements from at least two, and preferably all three, of the following factors should be satisfied.

Possessing factor: Something the user possesses and carries with them (e.g. ID card, security token, cell phone, smart cards etc.)

Awareness factor: Something the user remember or memorizes or aware of (e.g. Password, PIN, (designs/shapes) patterns, secret questions etc.)

Inherence/Fundamental factor: Something the user has (Physical or behavioural characteristics) or Biological features (e.g., DNA sequence, face/iris recognition, thumb impression other biometric identifier etc.)

In reference to [1], in 2012 identity fraud affected about 12.6 million Consumers that created a loss of $4.6 billion ($365/consumer) in U.S. The probability of becoming an identity fraud victim is about 5.3%.Because of all these, remote human authentication is considered as one of the important issues in modern societies [17]. In this regard, many of the experiments and executions have been proposed. Majority of the proposed methods are depending on passwords or smart cards. Biometrics are already been implemented in remote authentication (see [2], [3], [4]) but only as substitution to passwords or PIN numbers in smart cards

II. EXISTING METHODS

One time registration with the central server and accessing many application servers are abundantly available in most of existing systems today, which results in insecurity to the user details and industry. Therefore, unknown user makes use of the leaked data to access the information through authentication (see [2], [3], [4]).

Drawbacks of currently trending systems:-

Authentication through smart cards leads to leakage of information (ID-theft) of the user during transaction over an insecure channel ([1], [5], [7]).If the user losses their smart

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

card, then he/she must w ait for another card to be reissued from the authority. This is more time consuming and transactions are not possible without smart card. Due to its low battery life, smart cards cannot perform difficult manipulations/calculations ([19], [20]). Hence, Biometrics based authentication is necessary to be implemented in these type of applications.

In the proposed method, CPRBG (Chaotic Pseudo-Random Bit Generator) [18] is considered as encrypting technique for a biometric image. This method of encryption creates confusion.

Many other methods are experimented to reduce the loss due to compression in video-object image and biometric signal. When there is a data loss in biometric signal it is not possible authenticate and access the centralized authentication service. The other steganographic methods like DWT are used in some of the existing systems to reduce compression losses [11], [12], [13].

III. PROPOSED METHOD

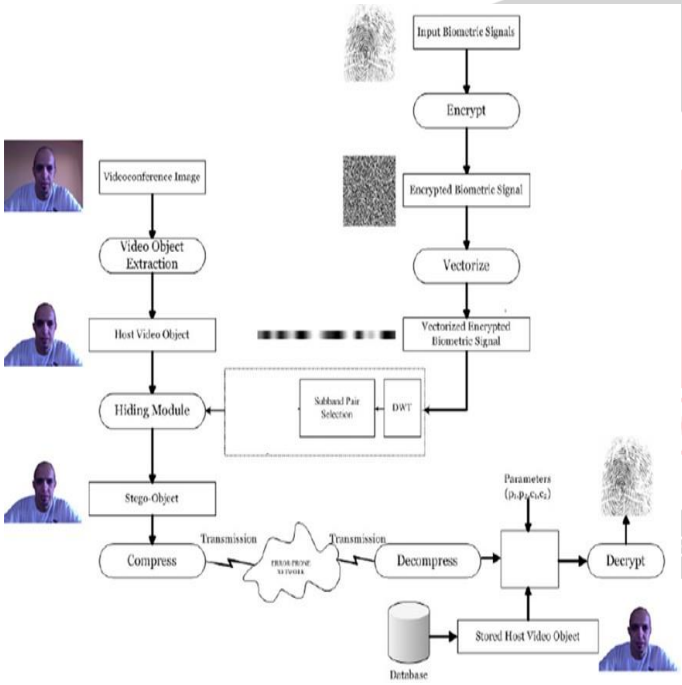

FIGURE 1: Data flow in the proposed scheme.

Image Acquisition: The image Video object (VO)) of the user is captured by a webcam and is considered as cover image.

Automatic Segmentation method: By using this method (head-and-body detector) the host video object is extracted from the captured image.

Cryptographic Technique:

- The biometric image (Secret Image) is encrypted by a cryptographic method called **chaotic encryption** algorithm.

Steganographic Technique:

- DWT (Discrete Wavelet Transform) is applied on chaotic encrypted vectorized image to hide it with in the LL sub-bands of energy efficient pairs of the cover image [14], [15].
- DWT, divides the host video object into two levels and consists of three pairs of sub bands (*HH*2, *HH*1), (*LH*2, *LH*1) and (*HL*2, *HL*1) using 2-D wavelet transform. The sub bands/coefficients below the threshold value are assigned with zero and above are encoded using lossless compression technique.
- The LL sub-bands of energy content and its coefficients are detected and by implementing DWT Watermarking approach encrypted biometric signal should be embedded.
- The stego object and the encrypted biometric image are not visible to human eye even under compression and transmission losses.

A. Algorithm

SENDER SIDE ALGORITHM:

Step1: Input the video and frames separation.

Step2: Video object is extracted from the video.

Step3: Select the secret frame from video object in which data is to be hidden.

Step4: Apply Hiding module

- Take biometric signal
- Encrypt biometric signal using secret key
- Vectorize encrypted biometric signal
- Apply DWT Watermarking and sub band decomposition
- The pair of sub bands with the LL energy content is detected

Step 5: Create video using Stego-object and apply DCT Compression.

RECEIVER SIDE ALGORITHM:

Step 1: Load encrypted video with hidden data and convert it into frames

Step 2: The video is De-compressed using IDCT

Step 3: Apply DWT Watermarking detection module

Step 4: Decrypt biometric signal

Step 5: Extract original biometric signal

Initially the biometric signal is encrypted by incorporating a chaotic pseudo-random bit generator and a chaos driven cipher, based on mixed feedback and time variant S-boxes.

The use of such an encryption mechanism is justified since,

1) Chaos presents sensitivity to initial conditions,

2) A C-PRBG statistically works very well as a one-time pad generation.

IV. DISCRETE WAVELET TRANSFORM

In Discrete Wavelet Transform the wavelets are discretely sampled which are useful in functional and numerical analysis [22].

- The comparative advantage of wavelet transform over other transforms like Fourier transform is that its temporal

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

resolution where the DWT captures both frequency and location information (location in time).

• The application of 2D- DWT in today's technology can be seen in JPEG2000 where the original image is high-pass filtered which results in three large images, where every image describes the variation in brightness (details) in original image.

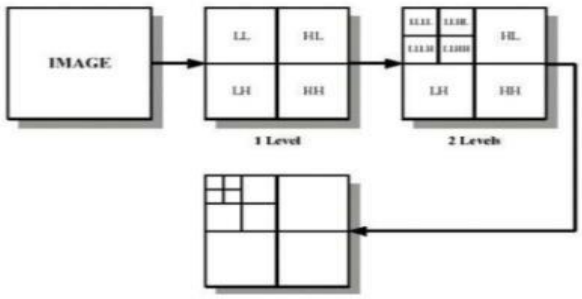

FIGURE 2: Image Compression Levels

The approximated image is obtained by:

• Firstly, the operations like downscaling and low-pass filtering are done then, the image is high pass filtered to retrieve three smaller images of fine resolution.

• Finally, the resulted image of the above process is again low-pass filtered to get the final approximated image in upper left.

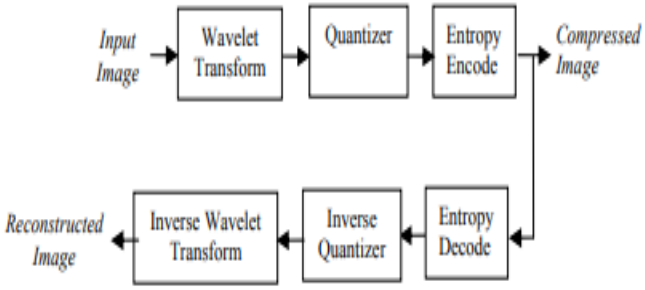

FIGURE 3: Flow of Discrete Wavelet Transform

- The DWT decomposes a digital signal into different sub-bands so that the lower frequency sub-bands have finer frequency resolution and coarser time resolution compared to the higher frequency sub-bands.
- DWT technique is usually applied in signal and image processing, especially for lossless image compression where an image is separated into a pixel. Lossy compressed images can also be obtained in DWT.
- The Lossless image compression is mostly used in applications where a good quality and good compression ratio of the image are required.
- For a Lossless image compression the PSNR (Peak Signal to Noise Ratio) of the image will also be a good value.
- Firstly, the image under consideration is decomposed into sub-bands (LL, LH, HH.HL coefficients) and is compared with the threshold.
- If (Coefficients < threshold value) then, they are assigned with "0"
- If (Coefficients > threshold value) then, they are encoded with lossless compression technique. After these procedures the image is processed with DWT quantization and then moved onto DPCM encoder. (Differential Pulse Code Modulation).

A. HAAR - Discrete Wavelet Transform

Haar wavelet function, denoted by ψ(t), is given by:

$$\psi(t) = \begin{cases} 1, & 0 \le t \le 1/2 \\ -1, & 1/2 \le t \le 1 \\ 0, & elsewhere \end{cases} \quad (1)$$

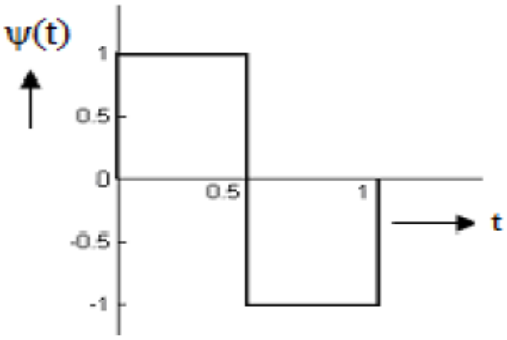

FIGURE 4: Wavelet function

- Due to its low computing requirements, the Haar transform has been mainly used for image processing and pattern recognition.
- From this reason two dimensional signal processing is an area of efficient applications of Haar transforms due to their wavelet– like structure.
- Modern cameras are capable of producing images with the range of tens of megapixels resolution. These images need to be compressed before storage and transfer.
- The Haar transform is used for image compression. The basic idea is the transfer of the image into a matrix in which each element of the matrix represents a pixel of the image. For example, a 256×256 matrix is saved in place of 256×256 image. JPEG image compression involves dividing the original image into 8×8 sub-images. Each sub-image is an 8×8 matrix.
- The 2-D Haar transform is required. The equation of the Haar transform is

$$B_n = H_n A_n H_n^T$$

Where $\mathbf{A_n}$ is a $n \times n$ matrix and $\mathbf{H_n}$ is n-point Haar transform. The inverse Haar transform is

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

$$B_n = H_n A_n H_n^T$$

V. CHAOTIC ENCRYPTION

Chaotic Pseudo-Random Bit Generator (C-PRBG) to create the keys that trigger the whole encryption to increase security.

• The generated key has size equal to the size of each biometric signal. **Chaotic cryptology** includes two integral opposite parts:

Chaotic cryptography and chaotic **cryptanalysis**.

One of the application of the mathematical chaos theory is the Chaotic Encryption in the field of cryptography, which is the study or techniques used to privately and securely transmit information with the presence of a third party or adversary.

Chaotic systems and cryptographic primitives share unique characteristics that allow the chaotic systems to be applied to cryptography.

If a system is implemented with Chaotic Encryption and Cryptographic keys to obtain symmetrically mapped acceptable functional outputs, it will be impossible for an adversary to find the outputs without any knowledge of the initial values.

In the proposed image encryption algorithm chaos-based image encryption method is used where another encrypted image / any matrix of random values larger / of the same size of the plain-image is considered as a key. The operations needed in encryption and decryption processes are reduced, with high level of security and less computational time.

In this algorithm, we explained the pseudo-code of the proposed scheme.

Algorithm:

Input: (1) Plain image A of *K*× *M* size. (2) Key image of K × *M* size.

Output: Encrypted image of *K*× *M* size.

Begin

1. The plain image (A) of K × *M* size is considered.

2. The secret key image (B) of K× *M* size is considered.

3. For every pixel in A consider RGB components (Ar,Ag,Ab).

4. For every pixel in B consider RGB components (Br,Bg,Bb).

5. For every RGB components of pixels in A & B apply diffusion process i.e..

F(A(r,g,b) , B (r,g,b)) = C(r,g,b).

6. The binary represented 8 bits of each pixel in every layer is concatenated with RGB layers in C. The concatenation follows RGB order.

7. A 1D array of size (24 elements) is selected and a confusion process called permutations is performed.

8. The three RGB layers of C is the representation of three subdivision of confusion process.

9. Repeat step (3-8) to all pixels in "A" and the corresponding pixels in B to obtain pixels in C.

End

The Encryption and Decryption steps are as follows:

Step1: The plain image (A) with *K* × *M* size and the key image (B) with same size of (A) i.e *K x M* is considered.

Step 2: For each pixel of A and B corresponding RGB components are considered.

Step 3: For every corresponding RGB components of A and B any logistic map is applied to obtain new RGB components

Step 4: To have a 24 bit value new RGB component is concatenated.

Step 5: A 1 Dimensional array of size 24 elements are considered and permutation is applied.

Step 6: A gray value is constructed for new pixel from the permuted new RGB component.

Step 7: Perform steps 1 to 6 for all pixels in A.

Step 8: For Each corresponding Data compression in A&B apply diffusion process using (Bit XOR)

Proposed chaos-based Decryption scheme:

Step 1: Data A with K X M Size.

Step 2: Key Image with K X M Size

Step 3: Apply each key on each bit of data to get decrypted data.

VI. HIDING THE ENCRYPTED BIOMETRIC SIGNAL

The encrypted biometric signal is robustly hidden in the host video object. Towards this direction we aim at producing a stego-video object that could protect its hidden message even in cases of compression or lossy transmission [9], [10].

A head-and-body image of the biometric signal's owner is analyzed and the host video object is automatically extracted next a DWT Watermark-based algorithm is proposed [21] for hiding the encrypted biometric signal to the host video object. The proposed algorithm hides the encrypted information into the LL energy-efficient pairs of sub-bands.

• Initially the extracted host object is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of sub bands (*HL*2, *HL*1), (*LH*2, *LH*1) and (*HH*2, *HH*1).

• Afterwards, the pair of sub bands with the LL energy content is detected and the coefficients are selected where the encrypted biometric signal should be casted. Finally, the

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

signal is redundantly embedded to both sub bands of the selected pair, using a non-linear energy adaptable insertion procedure.

VII. DISCRETE COSINE TRANSFORM

Discrete cosine transform represents the image under consideration as a sum of sinusoids that varies in magnitude and frequencies. This compression technique can be implemented in MATLAB by using dct2 function that computes two dimensional DCT for an image.

• This compression technique can be easily implemented in MATLAB by (dct2) function on an image.

• In DCT, only the visually significant pixels of an image are retained and is concentrated in just few coefficients hence, there will be reduction in image size and requires less memory space for storage.

• Because of these advantages, this method is considered as an efficient one in compression.

VIII. MESSAGE RECOVERY

The stego object (or a distorted image) is considered, once it has reached its receiver. The encrypted biometric signal is initially extracted by following a reverse (to the embedding method) process.

To achieve this let us assume that the recipient of the stego-object has also received the size of the encrypted *2-D* biometric signal (*a* x *b*), the scaling constants

(c_1, c_2) and possesses the original host video object (or he/she has the algorithm to segment it from the initial head-and shoulder image).

At the receiver end, these steps are executed to retrieve the secret message.

Step 1: Firstly, the received stego-object $\hat{X}$ and original video object *X* are decomposed into two levels with seven sub-bands using the DWT,

$$Y = DWT(X) \quad \hat{Y} = DWT(\hat{X}) \tag{2}$$

Step 2: The size *a* X *b* is considered, the embedded positions are detected by following the hiding process. Then the coefficients of sub-band *LH*2 (*LH*1) of *Y* are subtracted from the coefficients of sub-band *LH*2 (*LH*1) of $\hat{Y}$, and the result is scaled down by the value of coefficient of *LH*2 (*LH*1) of Y, multiplied by *c*2 (*c*1):

For *i* =1 to *a* x *b*:

$$w_i^{(2)} = \frac{x_i'^{(2)} - x_i^{(2)}}{x_i^{(2)} \cdot c_2} \qquad w_i^{(1)} = \frac{x_i'^{(1)} - x_i^{(1)}}{x_i^{(1)} \cdot c_1} \tag{3}$$

Step 3: The resulting hidden message coefficients $w(2)^i$ and $w(1)^i$ are averaged and rearranged to provide the encrypted biometric signal.

Step4: The original biometric signal is recovered by decrypting the enciphered signal. Here it should be mentioned that if the same video object *X* is used for every authentication attempt, the scheme may become vulnerable to attacks [23], [24]. In order to confront this problem the sender and receiver may share multiple video objects (poses) for each user.

In each authentication session, the sender may select one pose and inform the receiver of the selected pose's ID. This is a more resistant to attacks methodology, which can become even more coefficient if new poses of the users are periodically collected.

IX. SECURITY ANALYSIS OF THE PROPOSED METHOD

The main purpose of this method is to identify the possibility of remote authentication over wireless channels under lossy protocols. Hence, the steganographic methods play a major role in achieving (compression, losses during transmission etc.)

In cryptography, the system is said to be interrupted when an attacker can retrieve the secret [6]. Similarly, a steganographic system is broken in three ways; *firstly*, the attacker must detect that steganography has been used. *Secondly*, the embedded message must be extracted from the host and *finally* the attacker should read the embedded message.

Relating to security issues of the proposed Steganographic scheme there are few notes that should be observed by a steganographer:

- If the secret image is embedded in the image available on the internet devotee might notice and utilize them to decode the stego-image. In our scheme images are created by the user under authentication and destroyed immediately after use
- In order to reduce any Human Visual Perceptual attack, the generated stego-image must not have any visual artifacts. To achieve this, the proposed scheme adapts the wavelet coefficient of cover image, thus visual artifacts are avoided.

In our case:

(a) To resist the collusion attacks.

The embedding locations are dynamically identified based on thresholds and the image itself. Even if the same thresholds are used in a different image, the embedding locations will be different. Additionally if different thresholds are used for the same image, the embedding locations will also be different.

Thus statistical analysis performed during collusion attacks may not be as useful in our scheme as for schemes which use fixed locations.

(b) The scheme also appears to be resistant against middleman attacks. (In middleman attacks the attacker injects counterfeit images into the transmission channel by jamming the communication link.)

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

The attacker copies the bits from locations he/she assumes they contain the embedded information and embeds them to the same locations of a counterfeit image. At the same time, the attacker sends a forged acknowledgement to the trusted transmitter.

As a result, the transmitter assumes that his/her stego-image transmission is successful. The attacker then transmits the counterfeit image to the authentication authority, which upon reception, extracts the hidden information and authenticates the transmitter.

However, for the proposed steganographic scheme, the embedding locations are based on the image itself and vary with each image and with different thresholds.

Therefore, even with strong statistical analysis, it is particularly hard to pinpoint embedding locations since they always change. Furthermore even if the embedding locations have been identified by the attacker for a specific session, and a counterfeited image has been injected, the detection algorithm will still not be able to authenticate the user because the authentication information is encrypted. Thus the receiver will reject the counterfeit image.

X. RESULT ANALYSIS

In this section, the explanation of the complete results obtained with the implementations of the above mentioned methods are mentioned.

Here, the parameters Correlation, MSE, PSNR, BER, and Memory usage Efficiency are considered to analyse the efficiency of the proposed method.

- Initially, a cover image is taken from the webcam which has background other than head and shoulder of the user.
- A Video Host Image is obtained by semantic segmentation method (where the unwanted background pixels are removed.)
- **Due to segmentation of the image, memory/data usage efficiency of transmission increases.**

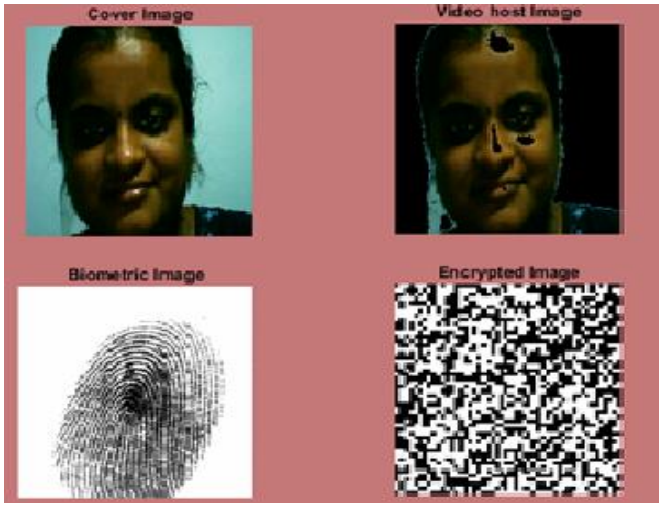

FIGURE 5: Cover Image: A webcam captured Image

Video host Image: Automatically extracted video object

Biometric Image: biometric signal

Encrypted Image: Chaotic encrypted image

Vectorized Image: Vectorized image of biometric Image

The above figure shows the results obtained after each process of encryption.

- A Biometric Image is considered as a secret image and is encrypted using Chaos Encryption.
- The Correlation of the Original Biometric Image and Encrypted Image is considered to understand the similarity between original and encrypted image.
- Additionally, to quantify and compare the correlations of adjacent pixels, the correlation coefficient *rxy* of all selected adjacent pairs (x,y) is calculated for the plain and encrypted images using the following formulas, where *xi* and *yi* are the gray values of two adjacent pixels in the image.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)) \cdot (y_i - E(y))$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (4)$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \qquad E(y) = \frac{1}{N}\sum_{i=1}^{N}y_i \qquad (5)$$

Generally,
Correlation Coefficient = (covariance between the two variables) / (product of their standard deviations).

- The units of covariance (x, y) are same as the product of the units of (x) and the units of (y).
- From the above formula we can infer that the units of D(x) are units of (x) and for D(y) are units of (y).
- Since the numerator and denominator of the correlation coefficient are the product of (x) and (y) units, the "r_{xy}" has no units.
- The maximum value for the correlation coefficient is ± 1.00.Correlation coefficient has fixed extremes and it is a unit less measure.
- For the analysis purpose this measure is usually represented in percentage.

- The **correlation** result reaches a maximum at the time when the two signals match best. Here we consider, the **Correlation Coefficient** to analyze

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

the similarity between the original and encrypted image.

- For the above mentioned biometric image, the similarity between encrypted and original images is **3.581%** which means, the encrypted Secret image is difficult to retrieve by the intruders or attackers.

FIGURE 6: Compressed Stego Image

- In the Fig 6, the Stego Image is obtained by DWT Watermarking Steganographic technique and the Vectorized Encrypted Biometric Image is hidden in the Cover Image obtained by webcam.

- Before transmission the Stego Image is compressed by DCT Compression to efficiently utilize the Bandwidth.

- For the Above Image in the Fig 6, the MSE (Mean Squared Error), PSNR (Peak Signal to Noise Ratio) and BER (Bit Error Rate) are calculated.

TABLE 1: Parameters that analyse the quality of transmitted Image

Paramters	Values
MSE	0.82806
BER	-1.425 x10^{-4}

- **MSE** measures the average of the squares of the errors, that is, the average squared difference between the estimated values and what is estimated.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (6)$$

- **MSE** is the mean of the squares of errors in two images $\mathbf{I_1}$, $\mathbf{I_2}$ Where M and N represents the dimensions of two images of same size.

- In the result obtained, the value of the MSE is 0.82806 which is small value and hence, this image is

CORRELATION COEFFICIENT
0.030581

better for transmission.

- **PSNR** is used to measure the quality of reconstruction of lossy and lossless compression.

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (7)$$

- In the formula for PSNR, the value of R is decided by the format of the image. If the format of the image is 8 bit, R = 255. If the format of the image is expressed using floating point numbers then, R = 1.

  Acceptable values for the **PSNR** in lossy image and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better. For 16-bit data **values** the **PSNR** range from 60 and 80 dB. Usually the Acceptable **values** for wireless transmission quality loss are considered to be about 20 dB to 25 dB.

- **BER** is the ratio of (number of **bit errors**) to (total number of transferred **bits)** during a studied time interval. BER is expressed in negative power.

- In the above result obtained, the BER is (-14250.00000) where BER is 10 to the minus 4, this means that out of (around 10,000) bits transmitted, 1 had an error. This value is good for transmitting the information with less error.

Same parameters are considered, at receiving end and compared for the analysis of proposed method.

FIGURE 7: Retrieved biometric Image at the receiving end

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

TABLE 2: Parameters that analyse the quality of Retrieved Image

Paramters	Values
MSE	10.0949
PSNR	38.0557 dB
BER	-1.9823 x 10^{-4}

At the receiving end, the values of the parameters are much better compared to the transmitting end.

XI. PERFORMANCE ANALYSIS

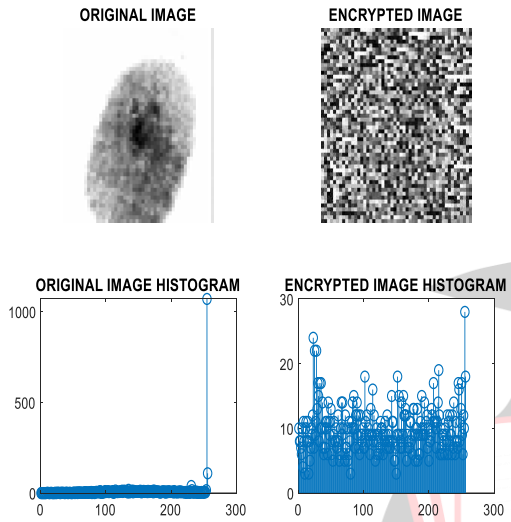

FIGURE 8: Histograms of original and Encrypted Images

- In Fig 8, the **variations in the intensities** of the pixels of the Original and Encrypted Biometric Image are analysed through this histogram plots.
- The Encrypted Image is again vectorized to provide another level of Security which is shown in the Fig 5.
- **Histograms** are useful in enhancing the quality of the image. The x axis in a histogram represents the values and y axis represents the number of elements in that particular range.
- In the histogram plot of encrypted image, the intensities of the original image are distributed within the range of 0 to 300 values.
- From this we can infer that, in encrypted histogram: The chaos encrypting method enhances the imperceptibility of the biometric image by distributing the number of elements in a particular range of values when compared to original image histogram.
- Histogram of the Chaotic Encrypted image is noticeably different and flat from that of the original image. Hence, successful attacks are impossible.

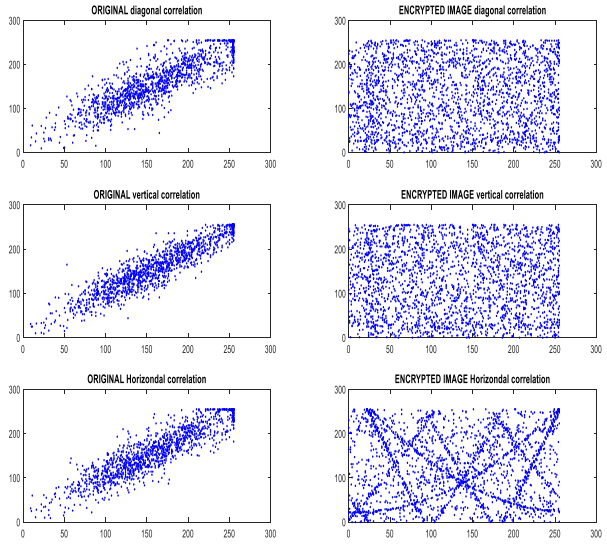

FIGURE 9: Diagonal, Vertical and Horizontal Correlation distributions of adjacent pixels selected from Original-image and Encrypted Image

- The plot of Correlation distributions in Diagonal, Vertical and Horizontal directions are considered to analyse the similarity of two images in various directions.
- Generally, for any image there will be more correlation between a pixel and its adjacent pixel which means that, there will be small distinction in the gray value over a larger area.
- The main aim of encryption is to diminish the correlation or similarity between a pixel and its adjacent pixel.
- As the similarity between the two plots decreases, a better encryption effect with high security can be obtained.
- Here, 3000 adjacent pixels in diagonal, vertical and horizontal directions in both of the original and encrypted image are randomly selected.
- Three plots of correlation distribution maps in these directions are drawn as shown in the fig 9.
- It is easily visible in the plots that, **correlation of the adjacent pixels of original image is high and exhibits a linear relationship whereas in encrypted image correlation is weakened and it exhibits strong randomness.**
- This nature of plots in three directions indicates that, **the image encryption is good and security is high.**
- Here, **MSE** value is closer to 0 in transmitter, whereas in receiver we can see slight increase in

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

the value, due to processing (storing and retrieving of the image) from the device.

- As the MSE value increases the **PSNR** value decreases at the receiving end.
- The PSNR value of 38.0557dB obtained at the receiver, is in the acceptable range of lossy image compression.
- As the image **BER** is always measured in negative powers we can infer that, as the BER value increases the quality of the image also increases.
- In the above case, the numeric value of error rate is slightly increased from ($1.4*10^{-4}$(14250.00) to $1.9*10^{-4}$(19283.00)), but these are negative values and hence the efficiency of the image is increased.

- **DATA / MEMORY USAGE EFFICIENCY**

The most existing schemes do not consider semantically meaningful video objects as hosts, but whole images. On the other hand the proposed scheme considers semantically meaningful video objects, offering possible advantages such as:

(a) A Two level authentication mechanism by capturing with a camera the person under authentication,

(b) Efficient data / memory usage, since most of the used bandwidth transmits information relevant to the authentication process, and

(c) This method provides well organized rate limiting by discarding the unwanted blocks that does not contain the hidden information and retaining the required face blocks. This way of segmentation utilizes less memory space and provides high efficiency to the authentication system.

XII. CONCLUSION AND FUTURE WORK

Even though many experiments have been conducted to meet the demand of a better authentication system, the proposed method has few issues, which should be investigated in the future work. In particular,

- In this method the, recipient must have the original host video object, hence implementation is non-blind and this feature may not be required in some specific applications.
- Chaotic encryption is the new field of research in cryptography study, and it will take some more time to improvise its security analysis.
- These methods relatively provide lossy transmission, which can be considered as the future work for improvement.

Result analysis and its detailed theoretical explanation describe "how well the proposed method provides security?" The system is also able to recover the hidden encrypted biometric signal under different losses and also make use of less memory space.

• The application of DWT Watermarking with DCT Compression provides high security and also these systems are easy to maintain [25]. These methods have good compatibility with both Image and video compressions.

Even with the presence of added noise and losses in data transmission, this proposed methodology provides a good authentication system with efficient memory and data usage.

REFERENCES

[1] A. Pascual and S. Miller, "Identity fraud report: Data breaches becoming a treasure trove for fraudsters," Javelin Strategy Res., Pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.

[2] E.-J. Yoon and K.-Y. Yoo, ``Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235_255, Jan. 2013.

[3] H. Kim,W. Jeon, K. Lee,Y. Lee, and D.Won,"Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in *Computational Science and Its Applications* (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer-Verlag, 2012, pp. 391_406.

[4] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1411_1418, Mar. 2014.

[5] L. Lamport, "Password authentication with insecure communication,"*Commun. ACM*, vol. 24, no. 11, pp. 770_772, Nov. 1981.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

[7] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4,pp. 727_740, Jun. 2006.

[8] M. Jakobsson and M. Dhiman, "The benefits of understanding passwords," in *Mobile Authentication* (Springer Briefs in Computer Science).New York, NY, USA: Springer-Verlag, 2013, pp. 5_24.

[9] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 162_175.

[10] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hiding in compressed images," *IEEE Trans. Image Process.*, vol. 10, no. 8,pp. 1252_1263, Aug. 2001.

[11] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 1, no. 3, pp. 32_44, May/Jun. 2003.

[12] P.Y. Chen and H.-J. Lin, "A DWT based approach for image steganography,"*Int. J. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 275_290, 2006.

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.

[13] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, "Steganography for a low bit-rate wavelet based image coder," in *Proc. IEEE Int. Conf. Image Process.*, vol. 1. Sep. 2000, pp. 597_600.

[14] D. Kundur, Y. Zhao, and P. Campisi, "A stenographic framework for dual authentication and compression of high resolution imagery," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 2. May 2004, pp. 1_4.

[15] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure color image steganography in transform domain," *Int. J. Cryptography Inf. Secur.*, vol. 3, no. 1, pp. 17_24, Mar. 2013.

[16]A. Madero, "Password secured systems and negative authentication,"Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Technol.,Cambridge, MA, USA, 2013. [Online]. Available: http://hdl.handle.net/1721.1/90691

[17] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Comput. Commun.*, vol. 32, no. 4, pp. 583_585, Mar. 2009.

[18] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme," *Comput. Commun.*, vol. 34, no. 3, pp. 305_309, Mar. 2011.

[19] E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, "A security enhanced remote user authentication scheme using smart cards," *Int. J. Innovative Comput., Inf. Control*, vol. 8, no. 5(B), pp. 3661_3675, May 2012.

[20] R. Madhusudhan and R. C. Mittal "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *Intell. Algorithms Data-Centric Sensor Netw.*, vol. 35, no. 4, pp. 1235_1248. Jul.2012.

[21] K. Zebbiche, L. Ghouti, F. Kheli_, and A. Bouridane, "Protecting fingerprint data using watermarking," in *Proc. 1st NASA/ESA Conf. Adapt. Hardw. Syst.*,Jun. 2006, pp. 451_456.

[22] K. Zebbiche and F. Kheli_, "Region-based watermarking of biometric images: Case study in fingerprint images,"*Int. J. Cryptography Inf. Secur.*,vol. 2008, Jun.2008, Art. ID 492942.

[23] T. Hoang, D. Tran, and D. Sharma, "Remote multimodal biometric authentication using bit priority-based fragile watermarking" , in *Proc. 19th Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1_4.

[24] Klimis Ntalianis, and Nicolas Tsapatsoulis, "Remote authentication via Biometrics: A robust Video-object steganographic mechanism over wireless Networks," *IEEE transactions on emerging topics*. vol. 4, no. 1, pp. 156_174, 2016.

[25] P.Campisi, "Object-oriented stereo-image digital watermarking,"*J. Electron. Imag.*, vol. 17, no. 4, p. 043024, Oct. 2008.

 DOI : 10.35291/2454-9150.2019.0104 © 2019, IJREAM All Rights Reserved.