Optimal Double Layer Secret Sharing Scheme for Biometrics

Elavarasi Gunasekaran* and Vanitha Muthuraman

Department of Computer Applications, Alagappa University, Karaikudi, India
E-mail: drgelavarasi@gmail.com; mvanitharavi@gmail.com
**Corresponding Author*

Received 19 November 2021; Accepted 12 January 2022;
Publication 15 November 2022

Abstract

Visual secret sharing (VSS) method is an encryption method to ensure the Security of secret data, that just performs the partitioning of 'n' shares and distributes among 'n' users in an ideal way so that exposing of less than 'n' shares is of no utilization. However, some dishonest members or hackers team up and tries to cheat other members in the group. Therefore, we have developed a dual layer secret sharing scheme based on universal share based secret sharing scheme. The dual layer is composed of threshold based secret sharing and then followed by the universal share based secret sharing. Here, the universal share is maintained by the trusted party avoids the contribution of dishonest participants. Moreover, to ensure additional security, the proposed approach employs Oppositional Artificial Fish Swarm Optimization (OAFSO) based Stream Cipher encryption technique to encrypt the shares, shows the novelty of the work. Furthermore, the confidentiality is enhanced with Biometric fingerprint authentication step, where the acknowledged users are alone allowed to get the decrypt shares with that the user can retrieve the secret data. The proposed fingerprint authentication method also makes use of Secure Hash Algorithm (SHA 1) to store the fingerprints and the matching is also done with hashed fingerprints only. So that the attackers cannot take and

Journal of Mobile Multimedia, Vol. 19_2, 519–546.
doi: 10.13052/jmm1550-4646.1928

corrupt the stored fingerprints and the misuse of fingerprints is not possible. Finally the performance analysis is made with existing approaches in terms of PSNR and MSE. Maximum PSNR is 58.9802 and minimum MSE value is 0.6232, while the existing methods provide very less PSNR and greater MSE values than the proposed methods.

Keywords: Secret image sharing (SIS), oppositional artificial fish swarm optimization (OAFSO), secure hash algorithm (SHA 1), biometric fingerprint authentication, stream ciphers.

1 Introduction

Advances in information technology are making it beneficial to send digital images via online applications. The growing amount of visually sensitive information such as private clinical reports, highly confidential corporate information, classified military data, and photographs of people has increased interest in security more than ever during this period. Therefore, several solutions and methods have developed to solve the problem of the security of clandestine images. Secret image sharing plans (SIS) are viewed as a significant set of methods among different cryptographic plans in multimedia media security society [1]. Secret sharing is only partitioning of shares so that exposing of a share is of no utilization [7].

Its role is to encode the original picture into n various shares. Utilizing atleast k shares can effectively reproduce the first picture. With not exactly k shares, any data of the first picture can't be gotten too. This exceptional and intriguing capacity permits SIS to be utilized in numerous fields, for example, visual authentication and identification, discrete memoryless network, general access structures, information sharing, etc. It may be generally grouped into two classifications: polynomial-based secret image sharing (PSIS) and visual cryptography (VC) [4].

In 1979, Shamir and Blackley specifically proposed a secret sharing (SS) plan. As an information protection strategy, the program has a quality threshold (k; n) which indicates that confidential information can be recovered from part n and that confidential information can be recovered at least from part k, but specific part k will not recover the data. In 1994, Naor and Shamir shared their first hidden photos. They introduced a visual secret image (VSS) that can be reproduced without counting the secret images. "Shamir's SS grayscale plane was applied by Thien and Lin 2002 to extract latent images from shadowed images. Share secret images, at least back from shadow

images, but not accurate shadow images. Retrieve all data in confidential images [5].

Rather than Shamir's plan, Blakley's strategy can likewise be utilized as the foundation for image sharing. In addition, the Azmuth-Bloom secret exchange scheme based on the Chinese Recovery Theory (CRT) can also be used to exchange secret images. One of the main disadvantages of the Blackley CRT-based method is that its serving size is the same as the size of the secret image. This defect and its high computational complexity make it unsuitable for use in practical situations [8].

Another MSS (Multiple Secret Sharing) technology will be available later this year. This plan can be defined as an MSS (n, n) frame in which n secret images are needed to create a composite image. This frame requires a shared image to reproduce the recovered secret image. Through hidden strategies, this strategy has achieved excellent results in terms of varying levels of similarity and attacks between shared and reconstructed secrets. However, this method is only suitable for n numbers. Although n is a unique number, it has its drawbacks. The restored secret image could not be obtained correctly, and n is a unique number. This problem can be solved with basic methods such as: Add additional random images, use K-image encryption and use two different security modules [6].

To further improve the security of crypto-currencies, biometric testing has become an important area of optical security research. Biometry is a procedure to examine the issue in statistical information in agriculture, biological science and environment. Each individual in this world has distinctive biological configuration which makes each individual diverse in its characteristic, habit, behavior, illness, etc. There are numerous authentication methodology from which one can recognize an individual like face, signature, DNA, finger impression, tongue and so on [2, 10]. Unlike a PIN (Personal Identification Number) or traditional password, biometrics such as fingerprints, face, and irises are unique and appropriate to a person. When used as private keys, they are more difficult to copy or share with others. Thus, biometric data can provide greater security and convenience for personalized testing [9]. The integration of biometrics with secret sharing likewise improves security and protection of verification framework for an individual enrolled in a biometric data set [3].

Therefore, in this paper, we have developed a dual layer secret sharing scheme with biometric authentication. The dual layer is composed of threshold based secret sharing and then followed by the universal share based secret sharing. Here, the universal share is maintained by the trusted party avoids

the contribution of dishonest participants. Moreover, to ensure additional security, the proposed approach employs Oppositional Artificial Fish Swarm Optimization (OAFSO) based Stream Cipher encryption technique to encrypt the shares, shows the novelty of the work. Furthermore, the confidentiality is enhanced with Biometric fingerprint authentication step, where the acknowledged users are alone allowed to get the decrypt shares with that the user can retrieve the secret data. The proposed fingerprint authentication method also makes use of Secure Hash Algorithm (SHA 1) to store the fingerprints and the matching is also done with hashed fingerprints only. So that the attackers cannot take and corrupt the stored fingerprints and the misuse of fingerprints is not possible.

The paper is organized as, Section 1 with various VSS schemes and the use of biometric authentication systems over them. In Section 2, various recent literature works are provided. Section 3 involves the detailed representation of the proposed framework. Atlast Section 4 is provided with various experimental results of the proposed and existing methods and then the conclusion part is provided in Section 5.

2 Literature Review

Harkeerat Kaur and Pritee Khanna [11], focuses on remote web-based/biometric authentication – security issues that simplify multiple server applications. This feature combines the advantages of deleting forged biometric characters with improved security clearance. The random removal method has been used to create secure, invalid, inappropriate, small and small biometric identifiers. Numerous forged identities created with such biometric data prevent crossovers (other database attacks) and allow the client to interact securely with various applications. A universal resource allocation model has been developed for multiple servers. The evaluation protocols correspond to the approval of the general meeting, Customer anonymity and Prevent broadcast attacks like MIMA server, ARM, database replication and forgery

M.A. Murillo-Escobar et al. [12], introduced a fingerprint template protection method dependent on chaotic encryption by utilizing the logistic map and Murillo-Escobar's algorithm. Likewise, they offered a 32 bit microcontroller for secure authentication frameworks to shown its application on embedded expert frameworks.

Xiangzhou Liu et al. [13], proposed a multi-level optical identification strategy based on the SVDGI (singular value decomposition ghost imaging)

and Secret Band Orbit (t,n) scheme. SVDGI with SVD provides an effective ghost image (GI) recovery strategy for changing the measurement matrix, allowing the image to be reconstructed to n pixels, which includes fewer N measurements, less time, and more quality. On the other hand, the Threshold Secret Sharing (t, n) algorithm provides a layered identification framework in which the modified measurement matrix is assembled into n keys, "distributed among different partners", and the validation rate is used as the highest, all t ($t \leq n$) or higher level of identification. To restore the image, they can fix the number of authorized members using their exact keys. Although it does not collect accurate data from the $t - 1$ certification image or lower due to its low level of validation, it can still provide remarkable peak performance.

Xiaotian Wu et al. [14], Implement a basic privacy disclosure model for information that may be hidden in encrypted images. An image encryption algorithm was then proposed with Shamir's secret approval. Theoretical studies have been performed to show that the shares generated by the encryption algorithm are suitable for data entry. Finally, some extensions provide two basic methods for using other extensions – a different histogram offset.

Xuehu Yan et al. [15], Thresholds SIS (k, n) charts have been proposed to detect single SIS dependent shadows instead of using data filtering with Visual Secret Sharing (VSS) activities. The scheduler has low output, recognition complexity and no pixel expansion with some shadow recognition strength. In addition, it performs lossless reconstruction without additional encryption.

A. Francis Xavier Devaraj et al. [16], SIARS has introduced in-DL (deep learning) with a variety of shared resources to enable the recovery of large images in the cloud. The SIARS model includes an Adagrad-based convolution neural network (AG-CNN) that relies on a feature-based extractor to achieve a potential set of input image features. At the same time, a SMSC (secure multiple share creation) scheme is implemented to create sharing of multiple incoming photos. The generated inventory attribute vector is added to the cloud database using a unique image ID. Once restored, the client provides a request image and replicates the received public image to access the attached image from the database.

3 The Proposed Scheme

Rising number of sensitive visual information, like confidential clinical reports, highly confidential corporate information, classified military data and private individual pictures, has expanded the interest for security never like

before in the current internet period. Thus, different solutions and methods have been created to solve the problem of the security of secret images. Secret image sharing plans (SIS) are viewed as a significant set of methods among different cryptographic plans in multimedia media security society. Secret sharing scheme is only just the partitioning of 'n' shares and distributed among 'n' users so that exposing of less than 'n' shares is of no utilization. However, there is a chance that if any dishonest member (frauds) present in the group may produce false shares so as to restore fake secret images with an intention to deceive remaining members (victims). Thus, universal share based sharing method is developed, where the universal share is maintained by the coordinator. With the help of universal share, the dishonest member sharing fake shares can be spotted out.

Therefore, we have proposed a secured dual layer universal sharing scheme. Here, the sharing of secret image is done in two layers. At first, the secret image is shared by threshold based method. Then, the universal share based sharing scheme is performed over the thresholded images to ensure added security. After that, again the shared images are encrypted to make them more confidential using proposed stream ciphers whose key is a matrix generated optimally using oppositional Artificial Fish Swarm algorithm. By this way, the shares are secured as encrypted form in the database. Atlast, an authentication phase is provided; through which the authenticated users with acknowledged biometric fingerprints are alone admitted to get the decrypted shares. From the decrypted shares, the authenticated receiver can reconstruct the secret data.

The Overall Block Diagram of proposed Dual Layer Secret image sharing Approach is given by the Figure 1.

Let the secret image be, $I(x, y)$and the four thresholds be, T_1, T_2, T_3 and T_4 respectively. Now, the share creation made using those thresholds be represented as,

$$S_1(x,y) = \begin{cases} Fill\ 1's, & if\ 0 \le pixel < T_1 \\ Fill\ 0's \end{cases};$$

$$S_2(x,y) = \begin{cases} Fill\ 1's, & if\ T_1 \le pixel < T_2 \\ Fill\ 0's, & otherwise \end{cases};$$

$$S_3(x,y) = \begin{cases} Fill\ 1's, & if\ T_2 \le pixel < T_3 \\ Fill\ 0's, & otherwise \end{cases};$$

$$S_4(x,y) = \begin{cases} Fill\ 1's, & if\ T_3 \le pixel < T_4 \\ Fill\ 0's, & otherwise \end{cases} \quad (1)$$

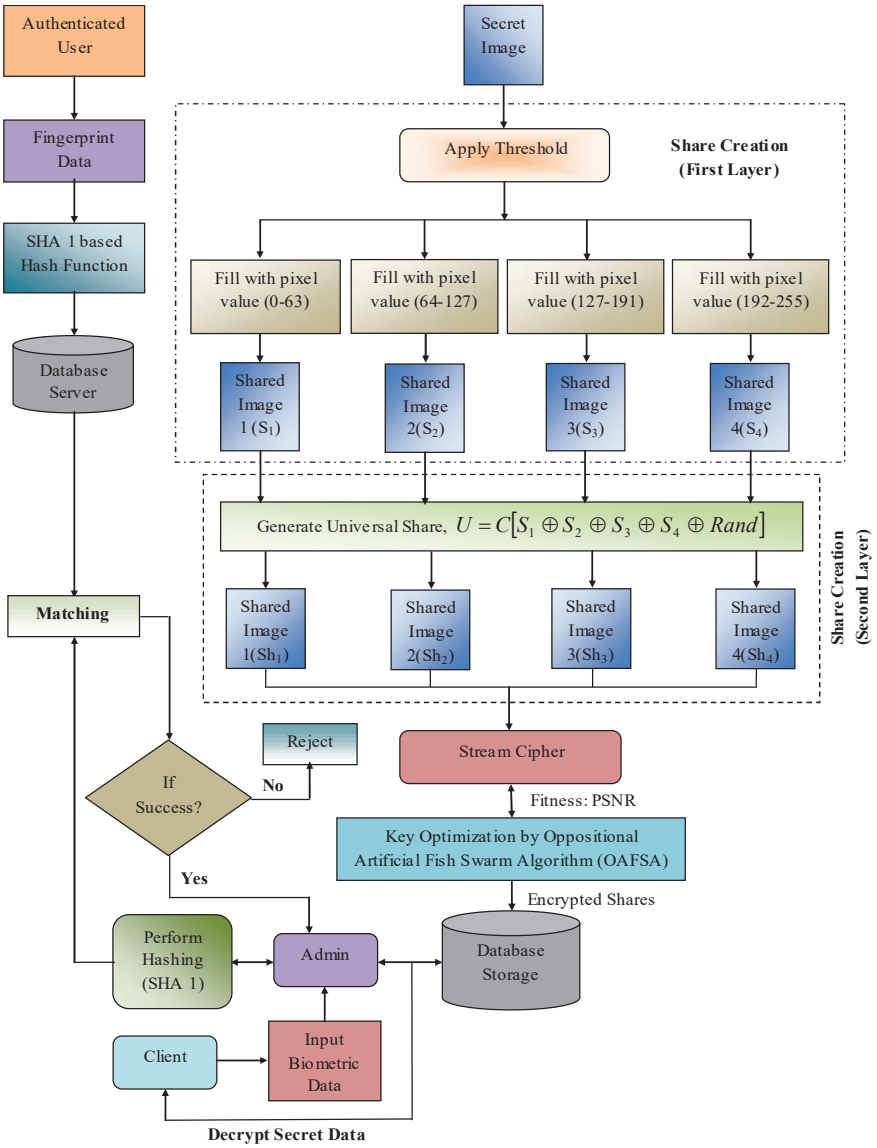


Figure 1 Overall block diagram of proposed dual layer secret image sharing approach.

Substituting the threshold values into variables T_1, T_2, T_3 and T_4, the created shares be like,

$$S_1(x,y) = \begin{cases} Fill\ 1's, & if\ 0 \leq pixel \leq 63 \\ Fill\ 0's, & otherwise \end{cases};$$

$$S_2(x,y) = \begin{cases} Fill\ 1's, & if\ 64 \leq pixel \leq 127 \\ Fill\ 0's, & otherwise \end{cases};$$

$$S_3(x,y) = \begin{cases} Fill\ 1's, & if\ 128 \leq pixel \leq 191 \\ Fill\ 0's, & otherwise \end{cases};$$

$$S_4(x,y) = \begin{cases} Fill\ 1's, & if\ 192 \leq pixel \leq 255 \\ Fill\ 0's, & otherwise \end{cases} \quad (2)$$

From the above representation, it is given that if a pixel value at position $(1,1)$ of $I(x,y)$ is less than 64, then the position $(1,1)$ of share $S_1(x,y)$ is filled with 1 and the remaining shares are filled with 0's. Here, the filling with 1's represent the filling of corresponding pixel value presented at position $(1,1)$ of $I(x,y)$. Likewise, if the pixel value at position $(1,1)$ of $I(x,y)$ is between 64 and 127, filling of 1 takes place at the $(1,1)$ position of share $S_2(x,y)$. Also, the values between 128 and 191 correspond to the shares $S_3(x,y)$ and the values greater than 191 belong to the share $S_4(x,y)$ respectively.

Once, the shares are created by threshold method, universal share based secret sharing method is followed. Universal share based sharing schemes are practiced when the presence of dishonesty shareholders are found in a group. In many cases, some users presenting in the group may tries to cheat other members by providing fake shares during retrieval; as the reconstruction of the secret is done by the gathering of all the shares provided by every members presenting in the group. Additionally, if the number of secret images is more, the share management turns out to be step by step more troublesome. To skip from these kinds of issues, the universal share based schemes are developed. The proposed universal share based scheme is designed securely to be processed over the threshold based shared images.

Let the input images be the threshold based shared images represented as, $S = \{S_1, S_2, S_3, S_4\}$. The first main step involved in the proposed universal share based scheme is to generate the universal share 'U'. Here, the universal share is created from the encrypted combination of the shares created at the first layer and a random matrix '$Rand$'. Thus the universal share can be

represented as,

$$U = E[S_1 \oplus S_2 \oplus S_3 \oplus S_4 \oplus Rand] \tag{3}$$

Where, $Rand$ denotes the random matrix of size equal to the shares S. E represents the block cipher based encryption and symbol $\oplus$ stands for EX-OR operation.

After creating the universal share, the final shared images $Sh = \{Sh_1, Sh_2, Sh_3, Sh_4\}$ are created with the help of the universal share as,

$$\textbf{\textit{Share 1:}}\ Sh_1 = S_1 \oplus U \tag{4}$$

$$\textbf{\textit{Share 2:}}\ Sh_2 = S_2 \oplus Sh_1 \oplus U \tag{5}$$

$$\textbf{\textit{Share 3:}}\ Sh_3 = S_3 \oplus Sh_1 \oplus Sh_2 \oplus U \tag{6}$$

$$\textbf{\textit{Share 4:}}\ Sh_4 = S_4 \oplus Sh_1 \oplus Sh_2 \oplus Sh_3 \oplus U \tag{7}$$

3.1 Share Encryption by Proposed Stream Cipher

Stream ciphers are generated using pseudo-random keystrokes, after which the display is associated with the source text via an exclusive operator. Here, encrypted hard data is represented by a series of binary digits with an arbitrary sequence of binary digits keys. In addition, the continuous encryption structure indicates high or reasonable performance in terms of speed and errors in voice transmission. Stream-specific encryption generates a series of random keys using the Oppositional Artificial Fish Swarm Optimization (OAFSO) algorithm.

3.2 Oppositional Artificial Fish Swarm Optimization (OAFSO) and Key Matrix Generation

In universal, fish can find the most nutritious area by searching or catching other fish one at a time. An area with more fish is usually more nutritious. AFSO's basic idea is to copy fishing practices such as hunting, farming and locating local fish for general optimization. In the improvement of the FSOA, the accompanying characteristics are thought of: (i) each fish addresses a candidate solution of the optimization problem; (ii) food density is connected to an objective function to be optimized; and (iii) the aquarium is the solution space where the fish can be found. Here, the key sequence of stream ciphers is generated using the OAFSO algorithm. Steps involved in OAFSO is given beneath,

Initialization

The algorithm first starts with a series of solutions (keystroke) that are generated randomly, and then iteratively searches for the optimal solution. In AFSO, every fish moves to a visual position based on their visual distance D_v in order to find the newer states. Let the initial set of solution and its visual position at some moment be represented as,

$$Y = (y_1, y_2, \ldots y_x) \tag{8}$$

$$Y_p = (y_1^p, y_2^p, \ldots, y_x^p) \tag{9}$$

Where, x represents the total variables; Y and Y_p are the current state and the visual position at some moment of an Artificial Fish respectively.

The state at the visual position is given as,

$$y_j^p = y_j + D_v \cdot R \tag{10}$$

In above equation, R denotes the random number within 0 and 1; D_v represents the visual distance. Now, the next state Y_{new} is computed using,

$$Y_{new} = Y + \frac{Y_p - Y}{\|Y_p - Y\|} S \cdot R \tag{11}$$

Where, S represents the step length. Also, the Flowchart of proposed Oppositional Artificial Fish Swarm Optimization algorithm is given in Figure 2.

Evaluate Fitness

At this point in time, the appropriateness of the current state Y and the state y_j^p to the visual position is evaluated. If the state y_j^p at the visual position is greater than the current state Y, it advances in the direction Y_p and reaches the next state Y_{new}; Otherwise, a remote visual inspection visit D_v will still find the overall optimum. The suitability is calculated using the following representation:

$$F(Y) = \sum_{x,y}^{X,Y} Sh^2(x, y) \tag{12}$$

Where, $Sh^2(x, y)$ represents each pixel value of the created secret shares.

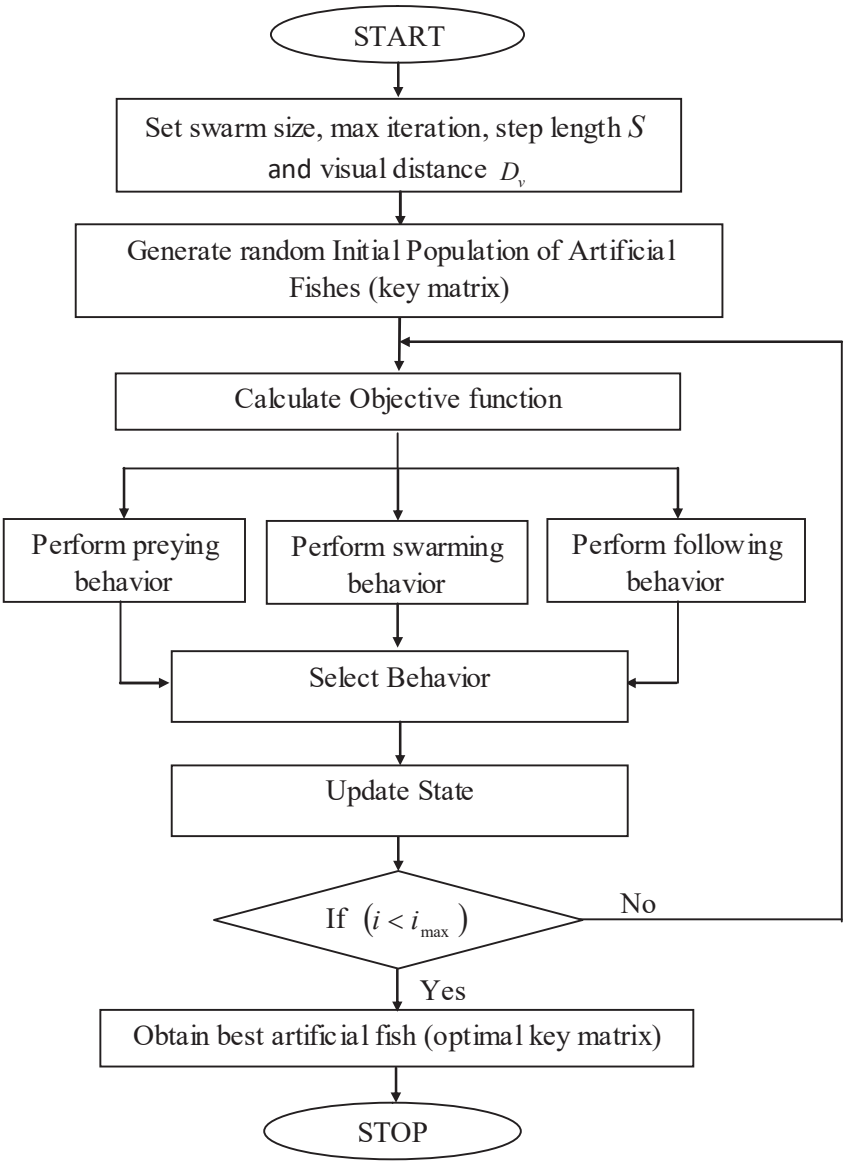


Figure 2 Flowchart of proposed oppositional AFSO algorithm.

Select Behavior and Update State

The AFSO follows three main functions particularly, preying behavior, swarming behavior and following behavior. Among these behaviors the default behavior is preying behavior, which is followed when the remaining functions fails to produce the optimal results.

Function 1: Preying Behavior

During this behavior, the moving process of artificial fishes tends to find their food based on the objective function (i.e. food concentration) within their vision. Let the current state of artificial fish is Y_j, and a randomly selected state Y_i within its visual range ($D_{ji} \leq D_v$) is given by,

$$Y_i = Y_j + D_v \cdot R \tag{13}$$

If the fitness of a randomly selected state exceeds the fitness of the current state ($F_j < F_i$), the artificial fish moves one step in the direction in which it Y_i is presented:

$$Y_j^{(k+1)} = Y_j^{(k)} + \frac{Y_i - Y_j^{(k)}}{\|Y_i - Y_j^{(k)}\|} S \cdot R \tag{14}$$

Further, the state Y_i is randomly reselected again and again in order to check whether the state Y_i (after reselection) produces better fitness. If, after repeated tests, the forward condition is not met, the artificial fish is moved randomly by one step in the following illustration:

$$Y_j^{(k+1)} = Y_j^{(k)} + D_v \cdot R \tag{15}$$

Function 2: Swarming Behavior

Fish usually move in groups to avoid danger. Based on this swarm behavior, let γ represents the crowd factor ($0 < \gamma < 1$). Y_M and x_N be the centerpiece or number of its companions in the current zone ($D_{ji} \leq D_v$). If the physical form Y_M is better than the current state physical form Y_j (i.e. $F_M > F_i$) and there are not many people ($\frac{x_N}{x} < \gamma$), take a step towards the partner center; Otherwise, the victim's behavior is applied. The behavior of the swarm is shown here as follows:

$$Y_j^{(k+1)} = Y_j^{(k)} + \frac{Y_M - Y_j^{(k)}}{\|Y_M - Y_j^{(k)}\|} S \cdot R \tag{16}$$

Function 3: Following Behavior

When one or more fish find food, neighboring partners will follow them to get food faster. Either Y_j and $Y_{\max}$ the current state of the artificial fish and the optimal partner in its visual range. If the fitness of $Y_{\max}$ and Y_j be $(F_{\max} > F_j)$ and encountered $(\frac{x_N}{x} < \gamma)$, the artificial fish takes a step to $Y_{\max}$ position itself, otherwise it affects the behavior of the prey. Therefore, it $Y_{\max}$ is defined in the following way based on the following behavior:

$$Y_j^{(k+1)} = Y_j^{(k)} + \frac{Y_{\max} - Y_j^{(k)}}{\|Y_{\max} - Y_j^{(k)}\|} S \cdot R \tag{17}$$

At last, the state update is done based on any of the above three moving behavior of fishes.

Stopping Criterion

Stopping criterion is attained, when there is no room for the solution improvement (i.e same or small difference in the fitness value) during the reach of maximum iterations.

At this time, the optimal key sequence is obtained. Now, each value of the key sequence is represented in 8-bit binary format and then right circular shift operation is performed to the sequence. Afterwards, the key sequence is transformed to regular decimal values and then EX-OR'ed individually with each shares of 'Sh' in order to form the encrypted shares.

3.3 Biometric Fingerprint Authentication with SHA-1

To additionally improve the security of visual cryptosystem, biometric validation is performed. Each individual in this world has distinctive biological configuration which makes each individual diverse in its characteristic, habit, behavior, illness, etc. There are numerous biometric authentication methodologies from which one can recognize an individual like face, signature, DNA, finger impression, tongue and so on. Among these, fingerprint based biometric authentication methods are successfully deployed in many applications. Here, the proposed approach makes use of fingerprint based biometric data for user authentication. Admin (trusted party) collects the fingerprints of authenticated users and then SHA-1 based hashing is performed on the fingerprints individually.

3.3.1 Secure Hash Algorithm (SHA) 1

Secure Hash Algorithm (SHA) was created and standardized by the National Institute of Standards and Technology (NIST) [18]. SHA was initially intended for compression purpose, where a large sized message is compressed to a hash of fixed length. However, SHA is the most famous tool to guarantee trustworthiness properties like authentication and verification due to its significant cryptographic primitives. SHA-1 is the cryptographic hash function of 1, which is basically the same as standard SHA, but fixes a bug that used SHA-1 until 1995 in the construction of the original SHA hash, causing a fatal bug that is now the most common widely used SHA hash function. Here, the input message of SHA must be lesser than 2^{64} bits is processed to produce a 160 bit message abstract. The proposed biometric authentication method based on SHA transforms the fingerprint of every individual to generate hashed output.

Algorithm processing includes the following steps:

Padding

The main function of message padding is to make the overall length of the enlightened message longer. Rebel keeps its own 1-bit, which changes from an individual number to a 0-bit, with the number of padding bits between 1 and 512.

Also, If (message) $<2^{64}$ bit, padded with zeros;

Otherwise ($>2^{64}$ bit), separate message into several groups of 2^{64} bit and process separately.

Append Length

Now, the length of message comprised of 64-bits binary representation is appended to the last part of the message.

Initialize SHA-1 Buffer

After increasing the length, SHA-I generates a series of five four-word buffers (A, B, C, D, E) and starting with sixteen values. The algorithm converts the message groups inserted into the message summary, from which the intermediate or final results of the summary message are buffered.

Procedure communication in 16-word blocks:

The processing of SHA1 algorithm is accompanied by four rounds, where each round consists of 20 steps. The total number of steps 's' involved in

each rounds $(s = 4 * 20)$ utilizes a diverse primitive logical function which are represented as:

Round 1: $L(B, C, D, s \in 0 \leq s \leq 19) = (B \,\&\, C) \| (\bar{B} \,\&\, D)$ (18)

Round 2: $L(B, C, D, s \in 20 \leq s \leq 39) = B \oplus C \oplus D$ (19)

Round 3: $L(B, C, D, s \in 40 \leq s \leq 59) = (B \,\&\, C) \| (B \,\&\, D) \| (C \,\&\, D)$ (20)

Round 4: $L(B, C, D, s \in 60 \leq s \leq 79) = B \oplus C \oplus D$ (21)

After performing above four rounds, the values of 160-bits barrier (A, B, C, D, E) is updated to form a final 160 bit message abstract.

Once performing hash function over the biometric fingerprints, every individual hashed fingerprint is enrolled in a fingerprint template data set. If the true client requests for secret data, the admin performs hash function and matches with the hashed fingerprints stored in the fingerprint template data set. Once matching succeeds, the admin provides the decrypted shares to the user. Moreover, the block diagram of Proposed Biometric Fingerprint Authentication scheme with SHA-1 is given in Figure 3.

The integration of biometrics with secret sharing likewise improves security and protection of verification framework.

3.4 Secret Image Reconstruction

During the reconstruction process of secret image data, the authenticated users receiving decrypted shares $Sh = \{Sh_1, Sh_2, Sh_3, Sh_4\}$, is also provided with the universal share. User can just perform simple Ex-OR operations with the universal share to generate the original secret as,

***Share 1*:** $S_1 = Sh_1 \oplus U$ (22)

***Share 2*:** $S_2 = Sh_2 \oplus S_1 \oplus U$ (23)

***Share 3*:** $S_3 = Sh_3 \oplus S_1 \oplus S_2 \oplus U$ (24)

***Share 4*:** $S_4 = Sh_8 \oplus S_1 \oplus S_2 \oplus S_3 \oplus U$ (25)

Now, the set of shares $S = \{S_1, S_2, S_3, S_4\}$ *is created* (i.e. shares at second layer). Now the original secret image 'I' is found by just combining the obtained shares as, $I = S_1 \oplus S_2 \oplus S_3 \oplus S_4$. The main benefit of proposed scheme is that the reconstruction step is very simpler than that of the sharing scheme.

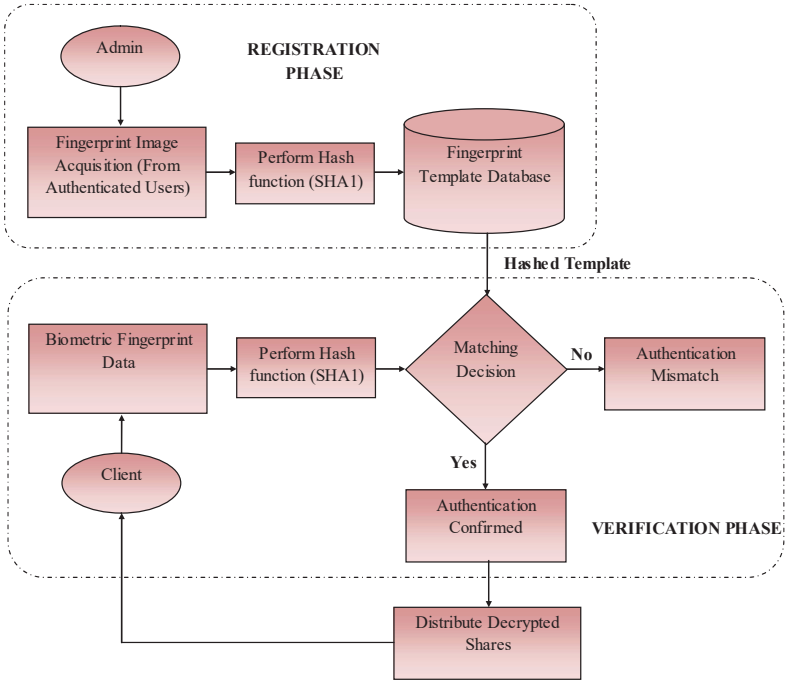


Figure 3 Proposed biometric fingerprint authentication scheme with SHA-1.

4 Result and Discussion

4.1 Experimental Setup

The results provided in this segment were acquired from the proposed Dual Layer Secret image sharing Approach implemented in a PC with the associated details: CPU Intel§Pentium 1.9 GHz, 64-bit operating system, Microsoft® Windows 10, 4 GB of RAM, and Math Works MATLAB R2014b stage. Here, all experiments were done utilizing secret and biometric databases, while each containing 200 test images. Few of the secret medical images and the fingerprint images used for biometric fingerprint authentication scheme are given by Figures 4 and 5 respectively.

4.2 Experimental Results

In this section, the intermediate results obtained for the proposed dual layer share creation method is provided. As the secret image is shared in two layers, the second column in Table 1 gives the results obtained with threshold

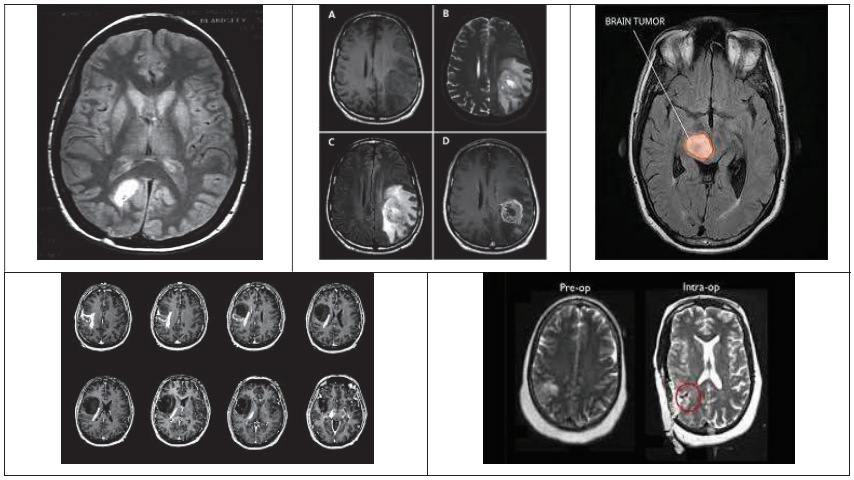


Figure 4 Secret image database.

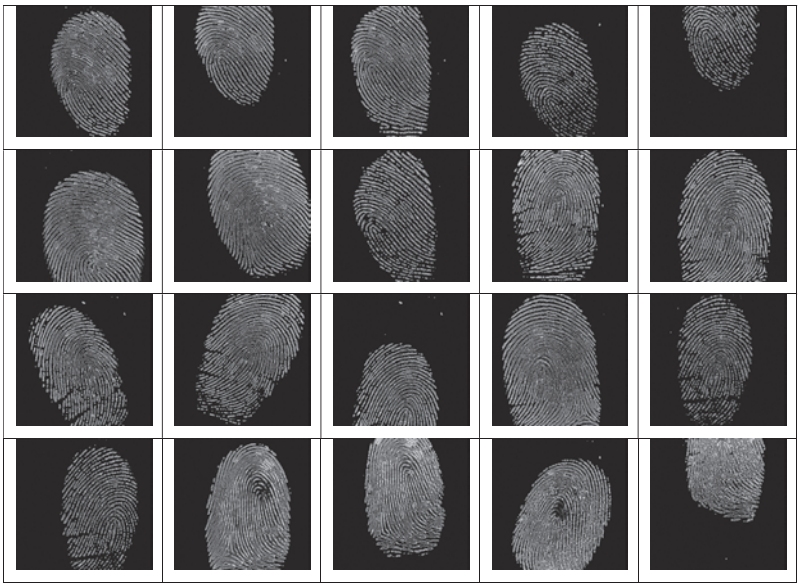
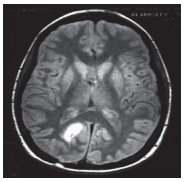
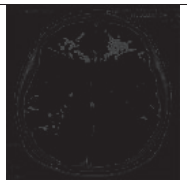
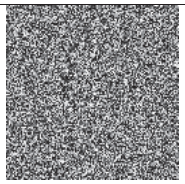
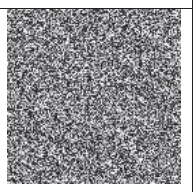
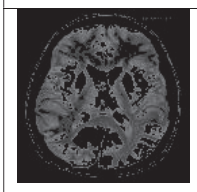
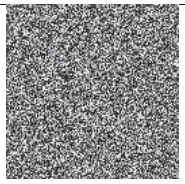
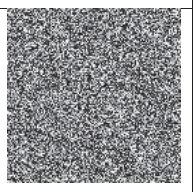
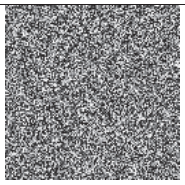
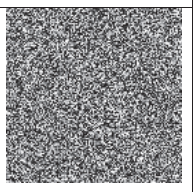
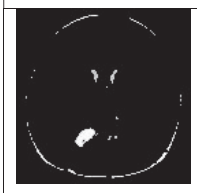
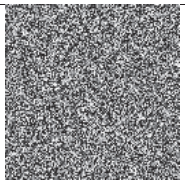
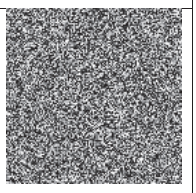


Figure 5 Biometric fingerprint image database.

based sharing. Moreover, the third column represents the shares obtained with proposed universal share based share creation method. Finally, the shares are encrypted using the OAFSO algorithm based stream cipher is shown in column 4 of Table 1.

Table 1 Secret image sharing results

Secret Image	Shares - Layer 1	Shares - Layer 2	Shares - Encrypted
			
			
			
			

Once the genuine client wants to obtain the secret data, he/she enters the proposed biometric Fingerprint Authentication system, where the finger prints of authenticated users are already enrolled in the finger print template database in hashed format. Based on the matching decision, genuine clients are confirmed and the trusted party decrypts and provides the decrypted shares to them. Here the intermediate results obtained for the proposed Biometric Fingerprint Authentication system is provided in Table 2.

In Table 2, the first row represents the genuine fingerprint provided by authenticated user receiving decrypted shares. Second row, fake fingerprint is provided and the system giving some random image is given.

In above Table 3, the intermediate results obtained with the proposed Secret image Reconstruction method is provided. The Encrypted shares maintained by the trusted party are given in first column. Next column gives the

Table 2 Biometric fingerprint authentication results

Genuine				
Fake				

Table 3 Secret image reconstruction results

Shares - Encrypted	**Shares – Decrypted (Shares- Layer 2)**	**Retrieved Shares- Layer 1**	**Retrieved Secret Image**

decrypted shares (representing the shares produced at second layer), which is shared with the authenticated clients. Third column represents the retrieved shares from first layer and finally the reconstructed secret image is provided in fourth column.

4.3 Performance Analysis

This section provides an overview of the proposed co-creation method based on the proposed universal dual layer partition. Here, the performance is analyzed through metrics like PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and CC (Cross Correlation). The values obtained for the PSNR, MSE and CC for the proposed dual layer universal share based share creation model with five test secret image data and their reconstructed results are shown in Table 4.

Table 4 PSNR and MSE values between original and the reconstructed images

Image	PSNR	MSE	CC
1.jfif	56.2376	0.97571	1
2.jfif	56.5487	0.90826	1
3.jfif	56.7325	0.90758	1
4.jfif	56.2834	0.9582	1
5.jfif	56.8372	0.90269	1

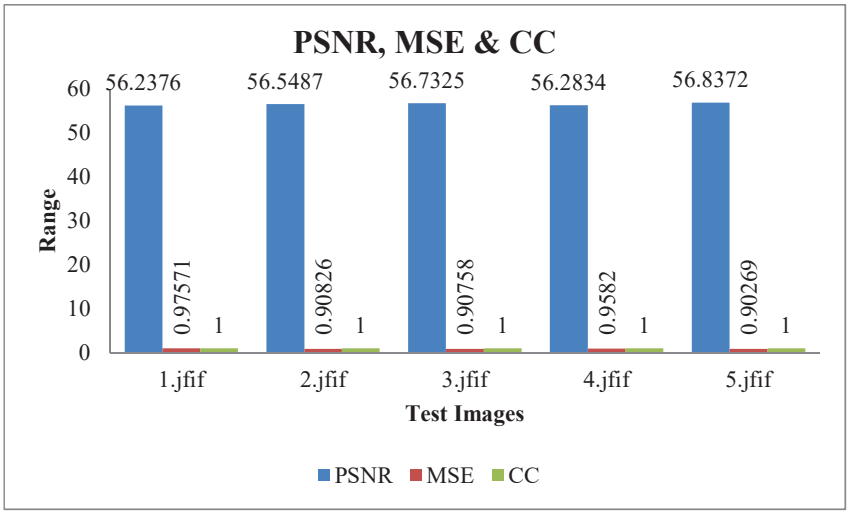


Figure 6 PSNR results of the proposed scheme.

Here, The PSNR values' showing around 48 represents the better image quality after reconstruction.

4.4 Comparison

Here, to analyze the performance of proposed dual layer universal share based share creation model, we have made a comparative analysis with other existing methods. For analysis, we have considered 5 test images and the analysis is made with existing methods like Rectangle Block cipher and SIMON ciphers. Also the values obtained for the proposed and the existing schemes are given in Table 5. Comparison graphs for PSNR and MSE values between proposed and the existing schemes are also provided in Figures 6 and 7 respectively. From the above table, the proposed PSNR values are 56.2376, 56.5487, 56.7325, 56.2834 and 56.8372 and MSE values are 0.97571, 0.90826, 0.90758, 0.9582 and 0.90269 are obtained for the proposed approach. On the other hand, the existing methods provide lower PSNR values and higher MSE values, when compared to that of proposed outcomes. This clearly shows the efficiency of the proposed approach producing quality outputs at the reconstruction stage.

Moreover, the proposed approach is also compared without and with other existing optimization methods through a set of five test images. For comparison, we have considered few optimization methods like AFSO (Artificial Fish Swarm Optimization), OWOA (Oppositional Whale Optimization Algorithm). Here, the comparison is made with PSNR and MSE metrics and the values gotten are provided in Table 6. The comparison plots for PSNR and MSE is also given in Figures 8 and 9 respectively.

From above Table 6, it is noted that the PSNR values attained with the proposed using OAFSO are 0.97571, 0.90826, 0.90758, 0.9582 and 0.90269

Table 5 Comparison between proposed and the existing schemes

	Proposed Scheme (With Stream Cipher)		Existing Scheme (With Rectangle Block Cipher)		Existing Scheme (With SIMON Ciphers)	
Images	PSNR	MSE	PSNR	MSE	PSNR	MSE
1.jfif	56.2376	0.97571	55.2146	1	50.3455	0.88789
2.jfif	56.5487	0.90826	55.1745	1	52.8943	0.89783
3.jfif	56.7325	0.90758	55.0533	1	51.7893	0.87456
4.jfif	56.2834	0.9582	55.1745	1	51.87934	0.85546
5.jfif	56.8372	0.90269	55.8723	1	50.5623	0.81421

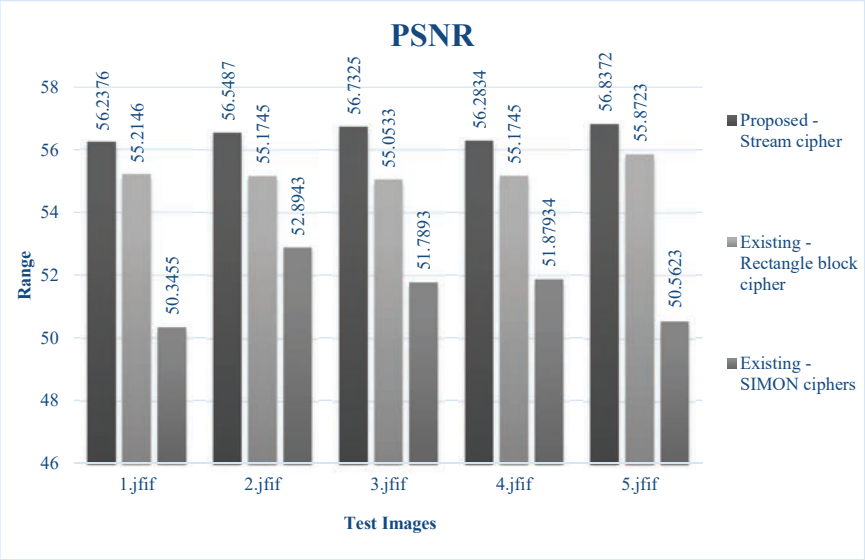


Figure 7 PSNR comparison between proposed and the existing schemes.

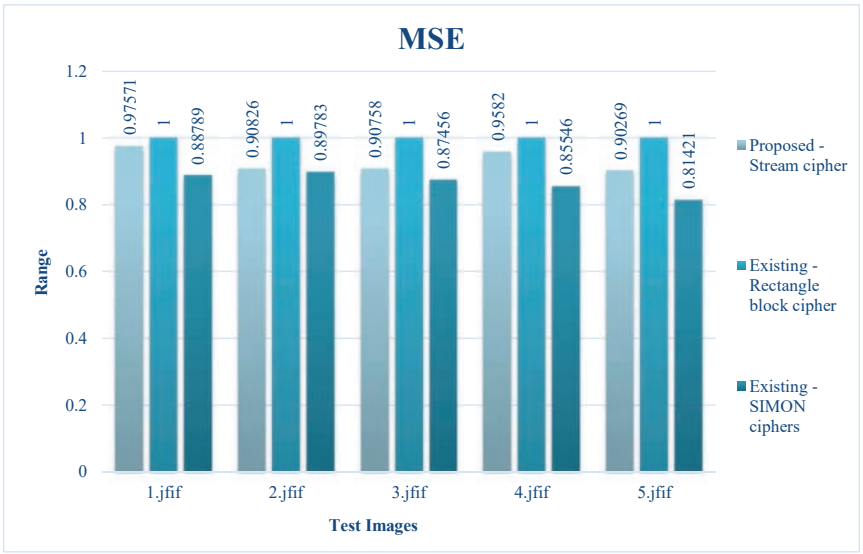


Figure 8 MSE comparison between proposed and the existing schemes.

Table 6 PSNR and MSE comparison of the proposed method without and with other optimization method

	Proposed Scheme (OAFSO)		Proposed Scheme (With AFSO)		Proposed Scheme (OWOA)		Proposed Scheme (Without Optimization)	
Images	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
1.jfif	0.97571	1	1.1746	0.8943	56.2376	55.2146	53.0176	46.8642
2.jfif	0.90826	1	1.2012	0.8503	56.5487	55.1745	53.4761	46.7947
3.jfif	0.90758	1	1	0.8253	56.7325	55.0533	54.0071	46.7047
4.jfif	0.9582	1	1.0545	0.8153	56.2834	55.1745	53.8147	46.7147
5.jfif	0.90269	1	1	0.8123	56.8372	55.8723	53.2783	46.8712

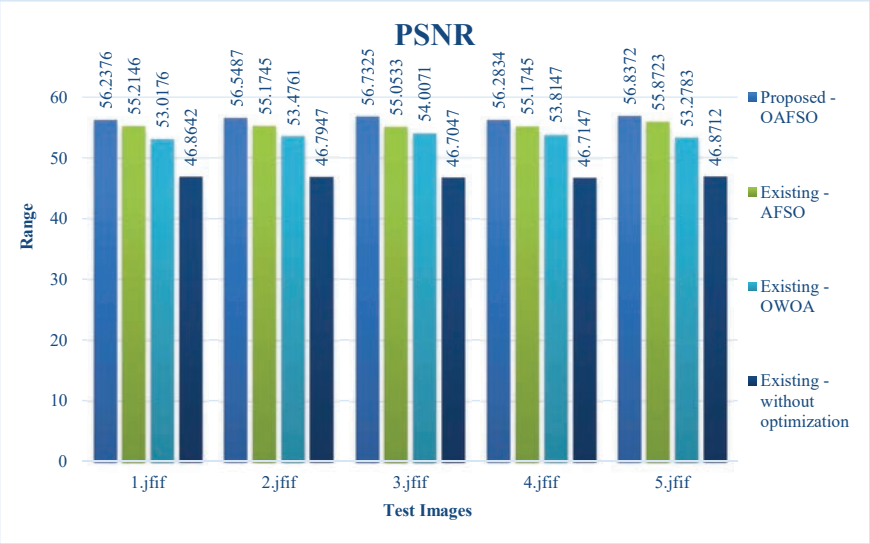


Figure 9 PSNR comparison among the proposed and existing schemes with and without optimization.s

and the proposed MSE values are 1,1,1,1 and 1 respectively. Also, the PSNR of existing methods be, 1.1746, 1.2012, 1, 1.0545 and 1 for AFSO; 56.2376, 56.5487, 56.7325, 56.2834, 56.8372 for OWOA and 53.0176, 53.4761, 54.0071, 53.8147 and 53.2783 for existing method without optimization. Here, also the PSNR values of existing methods provide very lower PSNR, showing that the better quality image retrieval by the proposed approach than the existing methods. Similarly, the MSE values of the existing methods are also greater than the proposed MSE values. This shows the increased error faced by the existing methods during the reconstruction of shares.

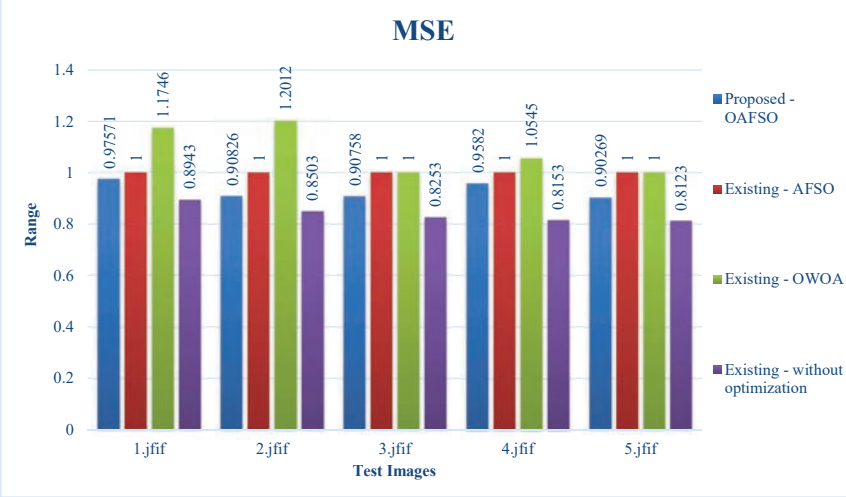


Figure 10 MSE comparison among the proposed and existing schemes with and without optimization.

5 Conclusion

In this paper, we have introduced a dual layer secret share creation model with OAFSO based Stream ciphers. Moreover, we have presented a biometric authentication scheme where the SHA1 based hashing is performed to securely store and maintain the fingerprints (templates of authenticated users) used for verification. Further the performance of the proposed scheme is analyzed through metrics like PSNR and MSE and contrasted with the existing methods. Experimental results show that the proposed dual layer secret share creation model outperforms the existing methods. Moreover, the Maximum PSNR value is reached upto 58.9802. Thus, it is proven that the proposed approach produces better quality retrieval images and thus the approach can also be used for high sensitive secret data. In future, hybrid deep learning based classification models can be included.

Acknowledgement

This research work has been supported by RUSA PHASE 2.0, Alagappa University, Karaikudi, India.

Conflict of Interest

The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated during the current study.

Ethics Approval

This article does not contain any studies with human participants performed by any of the authors.

References

[1] Charoghchi, Sara, and Samaneh Mashhadi. "Three (t, n)-secret image sharing schemes based on homogeneous linear recursion." Information Sciences 552 (2021): 220–243.

[2] Gupta, Himanshu, and Nupur Sharma. "A model for biometric security using visual cryptography." In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 328–332. IEEE, 2016.

[3] Patil, Sonali, Kapil Tajane, and Janhavi Sirdeshpande. "Enhancing security and privacy in biometrics based authentication system using multiple secret sharing." In 2015 International Conference on Computing Communication Control and Automation, pp. 190–194. IEEE, 2015.

[4] Bao, Long, Shuang Yi, and Yicong Zhou. "Combination of Sharing Matrix and Image Encryption for Lossless (k, n)-Secret Image Sharing." IEEE Transactions on Image Processing 26, no. 12 (2017): 5618–5631.

[5] Gong, Qinghong, Yongjie Wang, Xuehu Yan, and Lintao Liu. "Efficient and Lossless Polynomial-Based Secret Image Sharing for Color Images." IEEE Access 7 (2019): 113216–113222.

[6] Guo, Jing-Ming, Dwi Riyono, and Heri Prasetyo. "Improved beta chaotic image encryption for multiple secret sharing." IEEE Access 6 (2018): 46297–46321.

[7] Miss, Hinal M. Mudia, and Pallavi V. Chavan Miss. "Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme." Procedia Computer Science 78 (2016): 632–639.
[8] Ahmadian, Amir M., and Maryam Amirmazlaghani. "A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms." Signal Processing: Image Communication 74 (2019): 78–88.
[9] Yan, Aimin, Yang Wei, and Jingtao Zhang. "Security enhancement of optical encryption based on biometric array keys." Optics Communications 419 (2018): 134–140.
[10] Ali, Zulfiqar, Muhammad Imran, Sally McClean, Naveed Khan, and Muhammad Shoaib. "Protection of records and data authentication based on secret shares and watermarking." Future Generation Computer Systems 98 (2019): 331–341.
[11] Kaur, Harkeerat, and Pritee Khanna. "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing." Future Generation Computer Systems 102 (2020): 30–41.
[12] Murillo-Escobar, Miguel Angel, César Cruz-Hernández, Fausto Abundiz-Pérez, and Rosa Martha López-Gutiérrez. "A robust embedded biometric authentication system based on fingerprint and chaotic encryption." Expert Systems with Applications 42, no. 21 (2015): 8198–8211.
[13] Liu, Xiangru, Xiangfeng Meng, Yurong Wang, Huazheng Wu, Xiulun Yang, Wenqi He, and Hongyi Chen. "Optical multilevel authentication based on singular value decomposition ghost imaging and secret sharing cryptography." Optics and Lasers in Engineering 137 (2021): 106370.
[14] Wu, Xiaotian, Jian Weng, and WeiQi Yan. "Adopting secret sharing for reversible data hiding in encrypted images." Signal Processing 143 (2018): 269–281.
[15] Yan, Xuehu, Qinghong Gong, Longlong Li, Guozheng Yang, Yuliang Lu, and Jingju Liu. "Secret image sharing with separate shadow authentication ability." Signal Processing: Image Communication 82 (2020): 115721.
[16] Devaraj, A. Francis Saviour, G. Murugaboopathi, Mohamed Elhoseny, K. Shankar, Kyungbok Min, Hyeonjoon Moon, and Gyanendra Prasad Joshi. "An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme." IEEE Access 8 (2020): 144310–144320.

[17] Neshat, Mehdi, Ali Adeli, Ghodrat Sepidnam, Mehdi Sargolzaei, and Adel Najaran Toosi. "A review of artificial fish swarm optimization methods and applications." International Journal on Smart Sensing and Intelligent Systems 5, no. 1 (2017).

[18] Ibraheem, Raaed K., Roula A. J. Kadhim, and Ali S. H. Alkhalid. "Anti-collision enhancement of a SHA-1 digest using AES encryption by LABVIEW." In 2015 World Congress on Information Technology and Computer Applications (WCITCA), pp. 1–6. IEEE, 2015.

Biographies

Elavarasi Gunasekaran is currently pursuing the Ph.D. degree with the Department of Computer Applications, Alagappa University, Karaikudi, India. Her research interests include secret sharing scheme, cryptography and biometrics security.

Vanitha Muthuraman, M.Sc (OR & CA)., M.Sc., M.Phil., Ph.D(CS). Presently working as a Assistant professor in the Department of Computer Applications, Alagappa University, Karaikudi. She has more than 10 years of experience in Research and nearly 10 years of experience in teaching. She has published more than 50 papers in international journals and acted as session Chairperson and reviewer.