ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.1, 443–451
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.44

MULTIPLE SECRET SHARE CREATION SCHEME WITH ELEPHANT HERD OPTIMIZATION ALGORITHM FOR BIOMETRIC IMAGE SECURITY

Elavarasi Gunasekaran[1] and Vanitha Muthuraman

ABSTRACT. Due to advanced development in information technologies, cybersecurity and biometric approaches becomes significantly increased. A new multiple secret share creation scheme for biometric images is proposed. To enhance the shares security, each shares are encrypted by using stream cipher of lightweight cryptography (LWC). For increasing the effectiveness of the stream cipher, here the optimal key selection process takes place by elephant herd optimization (EHO) algorithm. The performance of the projected technique of by elephant herd optimization based stream cipher (SC-EHO) is assessed and the results are examined under diverse aspects on iris images. The experimental results depicted that the projected technique has reached to maximum security compared to other methods. The experimental values ensured that the SC-EHO algorithm has obtained a higher PSNR of 56.30dB and throughput of 31MB.

1. INTRODUCTION

In recent days, biometric mechanism is applied extensively for the purpose of identifying legal authority and user, so that the user identity will be protected from any kind of fraudulent activities. Regardless, the better analyzing methods are more vulnerable which are easily hacked and biometric owner might

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 68P25.

Key words and phrases. Biometrics, encryption, security, share creation, light weight cryptography.

Submitted: 20.12.2020; *Accepted:* 06.01.2021; *Published:* 21.01.2021.

be endangered. In secured accessing system, the fraud identification is a major challenging issue. In order to overcome these limitations, an effective and efficient secure accessing module has to be designed according to biometric owners. Methods like SHA-1, MD5, 3DES, RC5, AES, and IDEA are considered to be traditional approaches for preserving the data like images and confidential files, at the time of transmitting information through inconsistent communication stations. Besides, it is not applicable for massive encrypted data like images and texts. Then, a progressive deployment for developing non-traditional encryption models like chaotic as well as hyper-chaotic encryption, as chaotic systems are based on cryptographic features in confusion as well as diffusion operations. In [1–3], chaotic encryption models are presented for conserving the properties such as text, grey images, color images, fingerprints and so on. Followed by, currently developed chaotic encryption methods are relevant to biometric details conservation with the help of chaos.

Nedjah et al. [4] developed an effective execution of iris texture validation on smart cards. For this purpose, a perfect matching is performed on a card. Hence, biometric properties are saved in the card to ensure the complete security and integrity. Initially, using circular translations of harmonizing iris codes, False Acceptance Rate (FAR) as well as False Rejection Rate (FRR) has been enhanced. Regardless, once the simulation outcome is obtained, the newly developed model is highly recommended to have optimal computation. For reducing the impact, the application presented model is improved along with confirmed threshold test to be reduced and to accomplish least FAR and FRR.Khelifi [5], it models the noisy systems in which the security and privacy is retained, the service provider, named as data hider, could not view the actual content of hosted information. Mostly, the recently introduced methods are applied in this study to execute a bit-wise encryption technology, also called as stream cipher. Also, saving the data by applying models like encryption might be compromised as the spatial consistency simplifies original images. This study is implemented a reversible data hiding mechanism from a security perception. As a result, Ciphertext-Only Attack (COA) and the weakening of previous state-of-the-art method, legalized data hiding schemes.

2. The Proposed SC-EHO Model

At first, the MSC process gets executed to split the image into a set of multiple shares. Next, the generated shares are encrypted using LWC technique where the optimal keys are chosen by EHO algorithm.

2.1. **Multiple Secret Share Creation Scheme.** Certainly, a natural image is composed of directly overlapping shares, where the human optical system could find the confidential image with no traditional devices. Finally, counts of shares are distributed frequently. The homogenous models contain sensor hubs that are identical since it is far away from measurements such as battery power and the devices are highly complicated to build. Then, an image produces "N" shares for security method. For Iris image sharing task, threshold to produce shares has to be allocated and shares developed. The numbers of imaginary images are represented as:

$$Shares = \int_{1}^{k} lim_{m?1tnp} P_{ij}. \tag{2.1}$$

Eq. (2.1) represented $ij?$place in a grid, $Shares?$defines the share of an image and $P_{ij}?$ implies the portions of image pixel. In case of generated shares, the input images is considered as,

If the "T" as 1 Generate Share 1
Else "T" as 0 Generate Share 2

Produce inconsistent systems and such models are applied for making many counts of shares. Initialize$n-1$ arbitrary matrices with size $i \times j$ for units. Shadows are generated on the basis of threshold measures. As pixels are fixed to similar measures in triangular portion, initial share is not changed completely. Only small amount of initial share is random, along with a remainder which is an accurate copy of initial triangular region. Hence, the essential randomness has to be produced and it is highly challenging in secret sharing models.

2.2. **General Key Matrix Formation.** A seed measure's' has been applied for generating the key matrix, which is selected by an individual. The permutation of column on concealed image might be obtained in prior to reach the basic matrices which enhance the data security. It is performed using main generation technology. A matrix is classified as 4 portions of $m * n$ matrix on the basis of size of $m * n$ matrix. The functions have exhibited the formation of a block. A

key matrix in conjunction with a single block size matrix produces n seed value which has been initialized by user in key generation model. The given function is a sample main matrix:

$$Keymatrix = \begin{bmatrix} 53 & 132 & 254 & 83 \\ 161 & 134 & 108 & 209 \\ 191 & 105 & 248 & 89 \\ 128 & 32 & 224 & 73 \end{bmatrix}. \tag{2.2}$$

2.3. **EHO algorithm.** EHO algorithm depends upon the key matrix which is developed for enduring the security of biometric shares. Hence, when key matrix is not invertible, then it is not suitable for decryption and actual data cannot be obtained. As the key matrix generation is random, in a single execution it is highly difficult to obtain a key matrix. A evaluation model should be developed for generating the key matrix. The EHO method is described using applied characterized procedures and performance is defined below.

Consider an elephant clan is c_i. Then, future position of an elephant is j in a clan that is updated using Eq. (2.2):

$$x_{new,ci,j} = x_{ci,j} + \alpha \times (x_{best,\ ci} - x_{ci,j}) \times r, \tag{2.3}$$

where $x_{new,ci,j}$ illustrates the extended place, and $x_{ci,j}$depicts latest place of an elephant j in clan ci. $x_{best,\ ci}$ implies a matriarch of clan c_i; where female in optimal elephant in a clan. A scale factor $\alpha \in [0, 1]$ determines the efficiency of a leader of c_i on $x_{ci,j}$. $r \in [0,\ 1]$, where it is defined as a stochastic distribution which provides an enhanced objective in population diversity. In recent times, a uniform distribution is applied. It is clear that $x_{ci,j} = x_{best,\ ci}$, means that a matriarch in a clan cannot be updated by applying (2.3). It can be eliminated by extending the optimal elephant using the provided equation:

$$x_{new,ci,j} = \beta \times x_{center,ci},$$

where the power of $x_{center,ci}$ on $x_{new,ci}$, is normalized by $\beta \in [0, 1]$.The data from an individual in clan c_i was used to develop new individual $x_{new,ci,j}$. The intermediate of clan ci, $x_{center,ci}$, is calculated for d-th dimension by D calculations, in which Drefers entire dimension, as provided below:

$$x_{center,ci,d} = \frac{1}{n_{ci}} \times \sum_{j=1}^{n_{ci}} x_{ci,j,d}.$$

Here, $1 \leq d \leq D$ indicates d-th dimension, n_{ci} denotes number of individuals in ci, and $x_{ci,j,d}$ signifies dth dimension of an individual $x_{ci,j}$.In all clans, male elephants move away from their family and live solely once it is grown as adult. The isolation is named as a separating operator so that optimization problems are solved. In order to improve the exploring ability of EHO method, assume that an elephant with poor fitness will implement a separating operator for each generation as shown in Eq. (2.4):

$$x_{worst,ci} = x_{min} + (x_{max} - x_{min} + 1) \times rand, \tag{2.4}$$

where x_{max} and x_{min} refers the upper as well as lower bound, respectively. $x_{worst,ci}$ defines the inferior individual elephant in clan ci. $rand \in [0,\ 1]$ denotes the class of stochastic distribution, and uniform distribution from [0,1] as employed in recent times.For EHO, as same as meta-heuristic approaches, a type of elitism strategy is utilized for protecting the best elephant individuals by terminating the clan extension as well as separating operators. At the initial stage, a fittest elephants are protected, while inferior individuals are exchanged by protective elephants consequently. The elitism ensures that, the secondary elephant population is effective than former one.

2.4. **Left Shift Operator (LSO) for Optimal Key Matrix.** It reads and records the pixels on encrypted biometric image. The data present in a package can be applied in binary to a decimal key matrix for unique images with the help of LSO method. The sequences of bits are scanned. Values from 0 to infinity of ith character of hidden key minus 1 are listed in the table. Hence, it is necessary to assign the characters for all rows of matrix. Then, variable present in a column of matrix M could not be evaluated by an adversary without hidden key.

2.5. **Stream Cipher for Shares.** A stream cipher is a type of a symmetric-key method which is operated on single bits or bytes. The structure and security of a stream cipher depends upon pseudorandom generator which generates the key streams. Block ciphers does not require storage space, whereas stream cipher needs storage for recording the advanced operational state. For this purpose, the similar bit undergoes encryption in diverse state for stream ciphers if it is enciphered repeatedly; however it is in the block ciphers. Also, stream ciphers are required while zero error propagation is desired such as radio communication, because of non error propagation for Synchronous stream ciphers.

Stream ciphers are based on hypothetical cipher, named as One Time Pad. In OTP, a secret key should be a length of generated shares$share\ 1$ and $share\ 2$. The encryption ability is simplified as $E(k,s) = s \bigoplus key$ and decryption work $E(k,c) = c \bigoplus key$. For off chance where k is inconsistent, OTP contains an ideal secret key for the purpose of protection. At this point, it is peculiar for an intruder for capturing the cipher images and to infer a data with ideal keys in an encryption process. The encrypted binary image is obtained using XOR operator using ideal key abilities and plain image measures. Followed by, the ideal cipher method by approving the objective function is defined as:

$$Function\ (key_i, S) = (((S^* U_{k1}) \bigoplus U_{k2}) + U_{k3}) \bigoplus U_{k4}). \tag{2.5}$$

From (2.5), a key is 128-bit as well as $key = \{U_{k1}, \ldots, U_{k4}\}$& S implies a 32-bit string, image $\bigoplus$ implies the bit-wise exclusive-or, extension as duplication. The ideal keys are modified with the aim of not enabling rehashed and it offers some insight to the cracker for breaking the cipher image.

2.6. **Encryption and Decryption process.** The measures are determined under the application of function where the length of plain images denotes the encoded binary images are effective when compared to key-stream length. (2.5). As a result, 3 encryption models were developed namely procedures are based on best open keys as well as key-stream esteems:

$$\left\{ \begin{array}{l} P1 : S_i = Functior\,(U_{ki}, cipher_{i-1} \bigoplus Plain_{i-1}) \\ P2 : W_i = Functior\,(U_{ki}, S_j \bigoplus Plain_{i-2}) \end{array} \right\}.$$

In order to get the recipient, image undergoes encoding and computed within the device. The length of plain content shows the encoded pairing image which can be partially enough. The decoding model decrypts an encoded shared image along with a typical encryption keys. The material applied for encoding in converted character code table is secured and base position of a table is sustained in the memory. It is presented by

$$Plainshare_i = Cipher \bigoplus S_i.$$

From the recipient, a key output undergoes optimization for encrypted binary image which expands the time limit of a system with the application of key-stream depiction and actual values. Hence, a receiver knows key qualities applied for encryption.

3. Performance Validation

In order to examine the performance of the presented model, a set of simulations take place on iris images. Fig. 1 investigates the fitness analysis of the EHO algorithm with particle swarm optimization (PSO) algorithm under varying number of iterations. The figure depicted that the PSO algorithm has exhibited worse performance by attaining minimum fitness whereas the EHO algorithm is found to be superior by offering a maximum fitness.

Fig. 2 analyses the results of the SC-EHO algorithm with existing methods interms of PSNR, execution time and throughput. On determining the performance interms of PSNR, the ECC technique has obtained least performance with the minimum PSNR of 37.54dB whereas the PRESENT model has offered slightly higher PSNR of 44.76dB. On continuing with, the SC technique has reached to a reasonable PSNR of 54.89dB. But the proposed SC-EHO algorithm has demonstrated better performance with the maximum PSNR of 56.30dB. Similarly, on assessing the results interms of execution time, the SC-EHO technique has gotten the higher execution time of 9.45s whereas the SC model has offered somewhat lower execution time of 7.21s. On continuing with, the ECC and PRESENT techniques have reached to a reasonable execution time of 6.14s and 5.23s. On determining the performance interms of throughput, the ECC technique has obtained least performance with the minimum throughput of 22MB whereas the PRESENT model has offered slightly higher throughput of 24MB. On continuing with, the SC technique has reached to a reasonable throughput of 28MB. But the proposed SC-EHO algorithm has demonstrated better performance with the maximum throughput of 31MB.

4. Conclusion

This paper has proposed an effective MSC with LWC technique with EHO algorithm to achieve security for biometric images. In order to examine the performance of the presented model, a set of simulations take place on iris images. Originally, MSC process is applied to produce a multiple set of shares for every applied image. Afterwards, the shares are encrypted by LWC technique. For raising the effectiveness of the LWC, stream cipher is applied and the optimal key selection process takes place by EHO algorithm. The experimental values

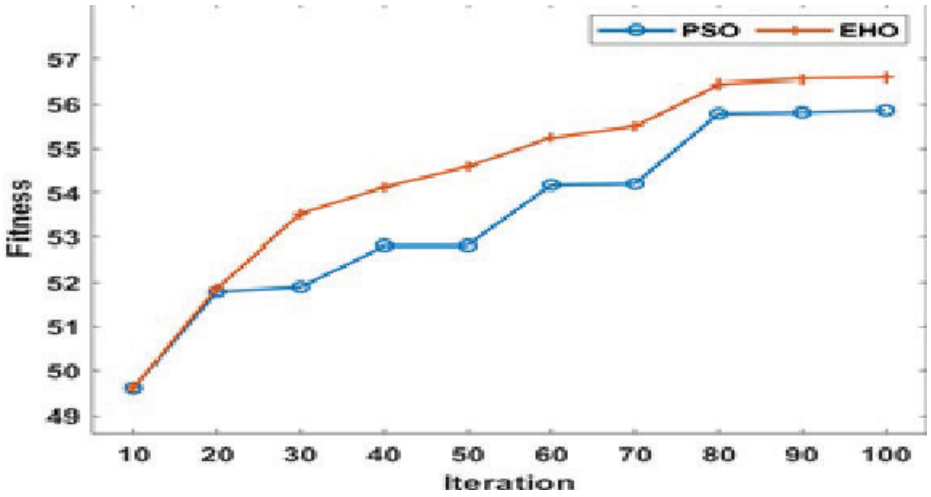

FIGURE 1. Fitness Analysis of EHO algorithm

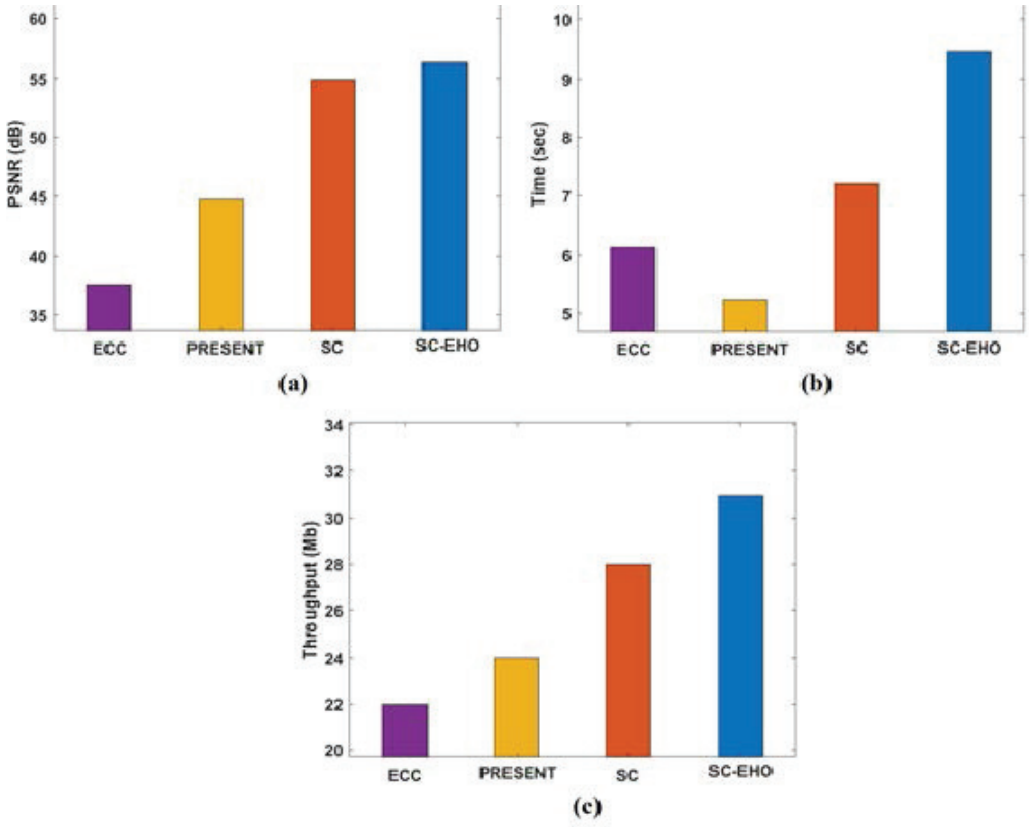

FIGURE 2. Results analysis of SC-EHO algorithm with existing methods

ensured that the SC-EHO algorithm has obtained a higher PSNR of 56.30dB and throughput of 31MB. The experimental results depicted that the projected technique has reached to maximum security compared to other methods.

ACKNOWLEDGEMENT

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

REFERENCES

[1] M.A. MURILLO-ESCOBAR, C. CRUZ-HERNANDEZ, F. ABUNDIZ-PEREZ, R.M. LOPEZ-GUTIERREZ, O.R. ACOSTA DEL CAMPO: *A RGB image encryption algorithm based on total plain image characteristics and chaos*, Signal Processing, **109** (2015), 119–131.

[2] M.A. MURILLO-ESCOBAR, C. CRUZ-HERNANDEZ, F. ABUNDIZ-PEREZ, R. M. LOPEZ-GUTIERREZ: *A robust embedded biometric authentication system based on fingerprint and chaotic encryption*, Expert Systems with Applications, **42**(21) (2015), 8198– 8211.

[3] A. AGUILAR-BUSTOS, C. CRUZ-HERNANDEZ, R. LOPEZ-GUTIERREZ, E. TLELO-CUAUTLE, C. POSADAS-CASTILLO: *Hyperchaotic encryption for secure e-mail communication*, Emergent Web Intelligence: Advanced Information Retrieval, Springer, London, (2010), 471–486.

[4] N. NEDJAH, R.S. WYANT, L.M. MOURELLE, B.B. GUPTA: *Efficient yet robust biometric iris matching on smart cards for data high security and privacy*, Future Generation Computer Systems, **76** (2017), 18-32.

[5] F. KHELIFI: *On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain*, Signal Processing, **143** (2018), 336-345.

DEPARTMENT OF COMPUTER APPLICATIONS, ALAGAPPA UNIVERSITY, KARAIKUDI, INDIA.
Email address: drgelavarasi@gmail.com

DEPARTMENT OF COMPUTER APPLICATIONS, ALAGAPPA UNIVERSITY, KARAIKUDI, INDIA.
Email address: mvanitharavi@gmail.com