Vol.7 No.1 Jan 2024

Multimedia Research

Received 12 April, Revised 24 April, Accepted 15 May

Modified Elgamal based Visual Cryptography via Hybrid Optimization Framework

Harish Goud Nayenolla

Both UMKC, Kansas, Missouri, USA
nharish250@gmail.com

Abstract: Visual cryptography (VC) is a technique for encoding a confidential image into varied shadow images known as shares. In VC, plain text is encoded in the form of images. The encrypted confidential text forms the shares that are transmitted via the internet using channels like email or fax and the shares are transmitted to the decryption procedure. The extant VC schemes increase the processing time and computational requirements in safeguarding the image. Therefore, there is a necessity to introduce a talented encryption method for improvement in the privacy and confidentiality of original images. Here, this working ends to establish a novel VC scheme. At first, the image from the transmitterend is encrypted by the use of a modified Elgamal algorithm with an optimal key generation procedure. Then, share generation is done, where the image is separated into N count of shares. Depending upon the share count, the EXOR operation is doneamid original image bits and keys. The resultant encrypted shared image is subsequently stored in the cloud server. In addition, at the receiver end, decryption is done, which is the reverse procedure of encryption. This work deploys Moth Flame Merged Whale Optimization (MFM-WO) for optimal key generation. Eventually, the superiority of the introduced approach is investigated via the assessment of several existing models.

Keywords: Visual cryptography; Multimedia; Share count; Modified Elgamal; MFM-WO Algorithm.

Nomenclature

Abbreviation	Description
AES	Advanced Encryption Standard
CS	Cuckoo Search
ECC	Elliptic Curve Cryptography
HAE-GWO	Harmonic Averaged Elephant and Grey Wolf Optimization
MSE	Mean Square Error
MCSO	Modified Cuckoo Search
MFM-WO	Moth Flame Merged Whale Optimization
MFO	Moth Flame Optimization
OGWO	Oppositional GWO
PBIL	Population-Based Incremental Learning
PSO	Particle Swarm Optimization
PSNR	Peak Signal to Noise Ratio
RSA	Rivest, Shamir and Adleman
VC	Visual Cryptography
VSS	Visual Secret Share
WOA	Whale Optimization Algorithm

1. Introduction

With the speedy development of network technologies, multimedia info is broadcasted over the Internet expediently [9] [10] [11]. A variety of secret data like commercial recognitions and military maps are transmitted over the Internet. When deploying confidential images, safety issues have to be considered since hackers might exploit weaker links over communication networks to steal data that they desire. For dealing with the safety issues of confidential images, a variety of image covert sharing techniques are introduced [12] [13].

VC was initially developed by Shamir and Noar in 1994 for the crisis of secret sharing. Sharing secret info is an earlier problem to be regarded in cryptography [14] [15]. For dealing with the safety issues of covert images, a variety of image secret sharing methods are introduced. VC is a cryptographic method that permits visual data (e.g. pictures, handwritten notes, and printed text) to be encoded such

https://doi.org/10.46253/j.mr.v7i1.a5

that the decryption is carried out by the individual visual system, devoid of the assistance of computers [16] [17]. VC method eradicates multifaceted computation issues in the decryption procedure, and the covert images are reinstated by the stacking function. This feature makes VC particularly helpful for the lower computational load necessity [18] [19].

In VC, the encryption procedure is the method of converting data through a mathematical function or an algorithm to make it illegible to anybody apart from the authoritative receiver who recognizes the confidential key [20] [21] [22]. The ElGamal cryptosystem is a public key cryptosystem method, whose safety depends upon the complexity in resolving the discrete logarithm crisis. This cryptosystem was developed by Egyptian cryptologist Taher ElGamal in 1985. Cryptography in digital computation is deployed to diverse kinds of digital file formats like video, images, text, etc [23] [24] [25]. Certainly, due to the requirement of image decryption, image encryption, and information security is a significant research area and it has extensive appliance vision.

The major contribution of the presented methodology is listed below:

- Introduces a new VC model, where the image stored in the cloud server is encrypted usinga modified Elgamal algorithm.
- Carries outoptimal key generation, where the keys are tuned in a fine manner using a novel algorithm.
- Introduces MFM-WOwhich is the hybridized concept of WOA and MFO models for optimal generation of key.

In this paper, section 2 describes the review of VC models. A summary of the proposed visual cryptography approach is represented in section 3. Section 4 portrays the modified Elgamal approach with optimal key for encryption. Section 5 depicts the generating shares and formation of encrypted share images and section 6 portrays optimal key generation via the newly introduced MFM-WO algorithm. Section 7 and Section 8 explain the result and conclusion respectively.

2. Literature Review

2.1 Related Works

In 2021, Srinivasa *et al.* [1] modified PSO and PBIL to optimize the threshold of VCS. Due to PSO's capabilities such as optimal global search, convergence speed, and simplicity, it was frequently deployed amongst fusion models. In addition, a hybridized PBIL-PSO was offered in this analysis.

In 2021, Karolin *et al.* [2] created every RGB pixel shared separately by the VSS method. These produced numerous shares of the covert images that were decrypted and encrypted with the RSA approach. In the encryption procedure, the multiplication method was deployed for the key generation procedure the public key was deployed for the encryption procedure and the private key was employed for the decryption procedure. The quality of the secret image was evaluated via MSE and PSNR values.

In 2021, Ahmad *et al.* [3] proposed an improved half-tone-oriented VC method for both color and binary images. Counterfeit share was produced by amalgamation of arbitrary white and black pixels. The adopted scheme consisted of 3 phases i.e., decryption, encryption, and detection. Halftoning, Encryption, VC, and a scheme of false share, made it much improved and secured. Accordingly, it facilitated the original renovated image to the real user; nevertheless, if the wrong password is entered, it gets the amalgamation of false shares with actual shares. Both black and colored images were processed with negligible ability usingthe developed method.

In 2019, Ren *et al.* [4] presented a new method for attaining recognition results of the revealed confidential images by imitating the recognition process of human eyes. The detection rate was deployed for computing the comprehensibility of the revealed confidential image. Investigational outcomes established that the recognition rate was measured as a new visual evaluation measure of VCS for confidential images. In addition, the adopted model was more proficient than the other existing approaches.

In 2018, Geetha *et al.* [5] developed a VC technique, which was divided into 3 phases such as (a) partition of color band, (b) creation of several shares, and (c) Optimal Decryption and Encryption. Here, OGWO-oriented ECC was proposed for optimal decryption and encryption. At first, the color image was splitin to 3 bands and consequently, diverse image shares were produced depending upon measures of pixel. Furthermore, the image shares were split into blocks and the real image was decrypted using the optimal key created by the OGWO scheme.

In 2019, Ali *et al.* [6] deployed a new robust image watermarking scheme depending upon VC and block categorization. At first, the original image was disintegrated into non-overlapping blocks. Afterward, SVM and canny edge recognition classification techniques were deployed to categorize these blocks into non-smooth and smooth groups. For confirming the image possession, the watermark was

recovered by load, the master shares as well as owner share. Furthermore, the betterment of the implemented model was confirmed in terms of robustness.

In 2019, Geetha *et al.* [7] presented image decryption and encryption using a diffusion system with a union of chaotic maps. Usually, the deployed VC system was split into 3 phases, i) separation of color band, ii) creation of a lot of shares, iii) Decryption and Encryption. At first, the color image was splitinto 3 bands, and diverse image shares were produced depending upon pixel measures. After that, the decryption and encryption were performed through the diffusion technique associated with the chaotic map.

In 2020, Gurunathan and Rajagopalan [8] deployed a technique for encrypting confidential information and it guaranteed that the interceptor could not observe the subsistence of such encrypted data. Furthermore, by exploiting the steganography scheme, the presented work split the images into varied blocks to improve the quality of the image, and the capability of confidential messages was increased together with its safety level. Here, the CS was employed to discover an optimal solution for transforming the message in all blocks. Moreover, the investigational results revealed that the performances of the devised model outperformed than existing models concerning embedding capability and safety level.

2.2 Review

Table 1 shows the reviews on VC in multimedia applications. Initially, PSO was employed in [1] with enhanced convergence speed and improved simplicity. Nevertheless, higher memory costs may occur. RSA model was deployed in [2] with minimal error rates and high PSNR. Yet, it needs implementation on cost factors. AES algorithm was presented in [3] that raised the sensitivity with better accuracy, but future works are concerned with clear view and higher visibility. A Gaussian based model was presented in [4] that raised the recognition rate with better visual quality, but the text-oriented CAPTCHA is not considered. OGWO method was used in [5] that reduce the error and it also offers high PSNR. However, it needs more consideration on multiple VC schemes. In addition, the SVM model was implemented in [6] that accomplished better robustness to attacks with high PSNR; nevertheless, cost factors are not considered. Likewise, the Diffusion method was introduced in [7] that offered high security and it also offers minimal error. However, multiple visual cryptographic methods are not implemented. CS model was utilized in [8] that offers improved image quality and it moreover offers enhanced embedding capability, but robustness should be concerned more.

Table 1. *Review of Conventional VC Systems*

Author	Adopted scheme	Features	Challenges
Srinivasa *et al.* [1]	PSO	❖ Enhanced convergence speed ❖ Improved simplicity	❖ Higher memory costs may occur
Karolin *et al.* [2]	RSA model	❖ Minimal error rates ❖ High PSNR	❖ Need implementation on cost factors
Ahmad *et al.* [3]	AES algorithm	❖ Superior accuracy ❖ Improved sensitivity	❖ Future work is on the concern of clear view and higher visibility.
Ren *et al.* [4]	Gaussian approach	❖ Better recognition rate ❖ Higher visual quality	❖ Need contemplation on text-oriented CAPTCHA.
Geetha *et al.* [5]	OGWO technique	❖ High PSNR ❖ Minimal error	❖ Needs more deliberation on multiple VC schemes.
Ali *et al.* [6	SVM model	❖ Robust to attacks ❖ Higher PSNR	❖ Cost factors are not considered.
Geetha *et al.* [7]	Diffusion technique	❖ High security ❖ Minimal error	❖ Numerous VC techniques are not implemented.
Gurunathan and Rajagopalan [8]	CS model	❖ High image quality ❖ Enhanced embedding capability	❖ Robustness has to be considered more.

3. A Summary of Proposed Visual Cryptography approach

The developedVCalgorithm includes 2 principal phases such as (a) encryption and (b) decryption. The steps are as follows:

Step 1: At first, the image sent from the transmitter side is encrypted using a modified ElGamal approach with an optimal key generation procedure.

Step 2: Subsequently, share generation is performed, where the image is separated into N count of shares. Depending upon the count of shares, the key is divided evenly.

Step 3: As the subsequent step, the pixels in the original image are split into odd and even ones that are further divided depending upon the count of shares.

Step 4: Then, the XOR function is done among the divided original image bits and split key. The resultant encrypted shared image is further accumulated in cloud surroundings.

Step 5: At last, decryption occurs, which is the reverse procedure of encryption.

Here, optimal key generation is performed by deploying the MFM-WO scheme, which assists in obtaining the described objective function in an accurate way with optimal training. Fig. 1 shows the illustrative depiction of the offered VC approach.

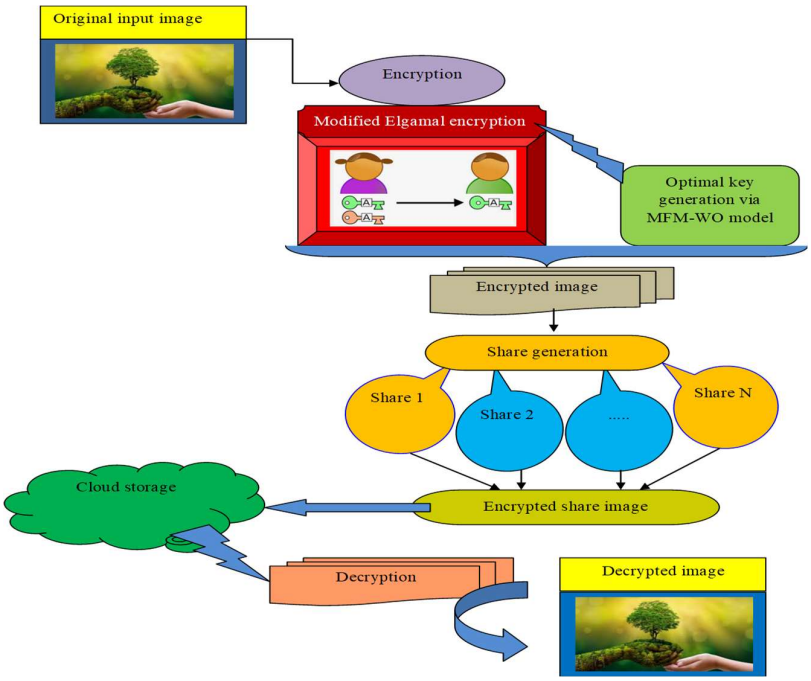


Fig.1.*Pictorial demonstration of the proposed framework*

4. Modified ElGamal Approach with Optimal Key for Encryption

At first, an optimal key is created, by which the input image is encrypted using a modified Elgamal approach. In this research, the optimal key is created with 8 bits.

4.1 Optimized Modified ElGamal Algorithm

The ElGamal-based cryptographic model was introduced in 1985 and it depends upon the complexity of discrete log issues for finite fields. It comprises of 3 phases [40].

Key Generation:

Select q as a larger prime integer and, α , β are considered as primary roots of q

Here, $d = (\alpha.\beta)^{-1} \bmod q$

Select o as arbitrary integer between $1 < o < q$ -1

Evaluate $X = (\alpha.\beta)^{o} \bmod q$

Private key: $\{o, \beta, d\}$

Public key: $\{q, \alpha, X\}$

Encryption:

Choose m as message

Select 2 arbitrary integers k_1, k_2 , where, $1 < k_1$, $k_2 \le q-1$

Select the shared secret key k_3 where, $1 \le k_3 \le q-1$

$$K = (k_1)^{k2} X^{k3} \bmod q \quad (1)$$

$$C_1 = \alpha^{k3} \bmod q \quad (2)$$

$$C_2 = (k_1)^{k2} \bmod q \quad (3)$$

$$C_3 = K.m.X \bmod q \quad (4)$$

Cipher text $C = \{C_1, C_2, C_3\}$ is send to user

Secretly share k_3 to the user

Decryption:

Recover one-time key, K

$$K = C_1^o . C_2 . \beta^{k3 . o} \bmod q \quad (5)$$

Discover $K^{-1} \bmod q$

Retrieve message $m = K^{-1} C_3 d^o \bmod q$

5. Generating Shares and Formation of Encrypted Share Image

The input image is divided into varied counts of shares. In the adopted method, the count of shares is regarded as 4. Assume that the pixel of the original input image includes 8 bits. Consider 8-bit values as 10101011. Amongst these, the odd and even bit values are isolated. Accordingly, odd bit values are symbolized by $R_1 = 1111$ and even bit values are symbolized by $R_2 = 0001$. These even and odd bit values are then divided depending on the share count, i.e. 4. As a result, $R_{11} = 11$, $R_{12} = 11$, $R_{21} = 00$ and $R_{22} = 01$ are produced. In addition, the created optimal key is divided into diverse keys based on share count. As 4 shares are concerned in this work, the keys are divided into 4. Therefore, keys $K_1 = 10$, $K_2 = 10$, $K_3 = 10$ and $K_4 = 11$ are created. In the subsequent step, the keys and the original image bits are EXOR-ed. On considering the aforesaid illustration, $A = R_{11} \oplus K_1$, $E = R_{12} \oplus K_2$, $C = R_{21} \oplus K_3$ and $D = R_{22} \oplus K_4$ are evaluated and the resultant image is accumulated in the cloud and is known as an encrypted shared image. In addition, the reverse procedure of encryption is made throughout the procedure of data decryption.

6. Optimal Key Generation Via Newly Introduced MFM-WO Algorithm

For improved encryption, the keys K are chosen optimally, as it remains a foremost aspect of the encryption procedure. Here, a novel MFM-WO model is introduced for optimization purposes. The input to the implemented method is shown in Fig. 2, which, nh corresponds to the total key count. The objective function of the introduced scheme indicated as Obj is specified in Eq. (6), which ϖ implies the original image and ρ_k implies k^{th} share and $corr$ correlation.

$$Obj = Min\left(\frac{1}{\sum_{k=1}^{N} corr(\varpi, \rho_k)}\right) \quad (6)$$

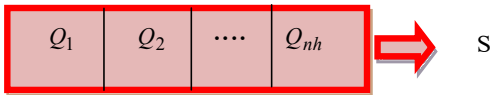


Fig.2.*Solution encoding*

Though the conservative WOA [29] model encompasses several enhancements; it endures particular limits like local optima. For this reason, the concept of MFO [30] is mingled with it to establish a new algorithm termed MFM-WO. Hybridized optimization schemes are said to be capable of specific search issues [31] [32] [33] [34].The steps followed in the proposed MFM-WO are as follows.

The most noteworthy of humpback whales is their astonishing hunting method. These whales could find out the prey's position and enclose them. As per the presented MFM-WO model, chaotic population-based initial generation is carried out using a tent map as shown in Eq. (7), wherein, x_i refers to random

integer created using the chaotic map, $S_{i,\min}$ and $S_{i,\max}$ refers to minimum and maximum positions respectively.

$$S_i = S_{i,\min} + \left(S_{i,\max} - S_{i,\min}\right)x_i \tag{7}$$

After the attainment of optimal searching agents, the other search agent attempts to update their location toward optimal agents for better searches. This action is pointed out by Eq. (9) and Eq. (10). If probability $p < 0.5$, the update occurs based on distance factor $\left(\vec{P}\right)$.Conventionally, p is chosen randomly, however, as per the developed MFM-WO model, p is determined based on the individual populace as shown in Eq. (8), wherein, it refers to the current iteration, N to count of individuals in the populace and S^* symbolizes the position vectors of required solution, $||$ refers to absolute value, S refers to the location vector, f_i refers to fitness and '.' refers to "element-by-element multiplication".

$$p = \frac{f_i it_i}{\sum_{j=1}^{N} f_i it_j} \tag{8}$$

$$\vec{P} = \left|\vec{A}.\vec{S}^*(it) - \vec{S}(it)\right| \tag{9}$$

$$\vec{S}(it+1) = \vec{S}^*(it) - \vec{J}.\vec{P} \tag{10}$$

It is to note that S^* should be updated in all the iterations with improved solutions. The coefficient vectors J and G are computed as shown by Eq. (11) and Eq. (12), wherein, $\vec{r}$ represent the arbitrary vector in [0, 1] and $\vec{y}$ refer to the random integer between two to zero.

$$\vec{J} = 2y.\vec{r} - \vec{y} \tag{11}$$

$$\vec{G} = 2.\vec{r} \tag{12}$$

Exploitation phase: It is attained by diminishing the value of $\vec{y}$ in Eq. (11). Note that the difference $\vec{J}$ is reduced by $\vec{y}$, i.e. $\vec{J}$ refers to random value among $[-y, y]$ wherein, y is minimized to 0 from 2 for further iterations.

A spiral formulation is createdamongstthe location of whaleand prey as in Eq. (13). Conventionally, if $p \geq 0.5$, the update occurs based on the exploitation phase, however, as per the MFM-WO model, the update takes place based on the MFO update as shown in Eq. (13), wherein, F_j denotes j^{th} flame, Dis refers to the distance among i^{th} moth and j^{th} flame, b refers to constant and v refers to arbitrary count.

$$S(it+1) = Dis'.e^{bv}.\cos(2\pi v) + F_j \tag{13}$$

Exploration phase: As per this phase, an alternately chosen exploration agent is identified. Such a phase $\left|\vec{J}\right| > 1$ highlightsthe search and allows the WOA model to perform a wide-ranging search. It is portrayed as in Eq. (14) and Eq. (15), wherein, $\vec{S}_{rand}$ is a randomwhaleelected from the present populace. Algorithm 1 illustrates the pseudocode of the MFM-WO model.

$$\vec{P} = \left|\vec{G}.\vec{S}_{rand} - \vec{S}\right| \tag{14}$$

$$\vec{S}(it+1) = \vec{S}_{rand} - \vec{J}.\vec{P} \tag{15}$$

Algorithm 1: MFM-WO approach
Initializing population based on chaotic population using tent map as shown in Eq. ().
Compute the fitness as in Eq. (6)
While it <maximum (it)
For every search agents
Compute p as in Eq. (8)
Update $y, J, v, G and p$
if 1 $p < 0.5$
if 2 $(\|J\| < 1)$
Update position as shown in Eq. (10)
else if 2 $(\|J\| \geq 1)$
Choose an alternate explore agent $\vec{S}_{rand}$
Update the position as shown in Eq. (15)
end if 2
else if 1 $p \geq 0.5$
Update position based on MFO formulation as shown in Eq. Eq. (13)

		end if 1
	end for	
	Compute the fitness	
	if there exists a better solution, update S^*	
	$t = t + 1$	
end while		
return S^*		

7. Results and discussions

7.1 Simulation Set Up

The developed VC approach using MFM-WO oriented modified Elgamal encryption was implemented in Matlab and resultants were observed. The execution was done relating to "Auditing time, PSNR, key sensitivity, encryption quality and correlation" for three types of images namely; Lena, cameraman, and Baboon. Subsequently, the improvement of the adopted MFM-WO model was calculated by distinguishing it from existing models such as MFO [27], WOA [33], AES [3], blowfish [38], ECC [39], HAE-GWO [37], MCSO [35] and chaotic logistic map [36]. Moreover, PSNR analysis was carried out for varied noise levels (in %) that range from 0, 10, 15, 20, 25 and 30. Here, the convergence analysis was computed for different iterations that range from 0, 5, 10, 15, 20, and 25. The sample images achieved for the adopted model at every stage are revealed in Fig. 3.

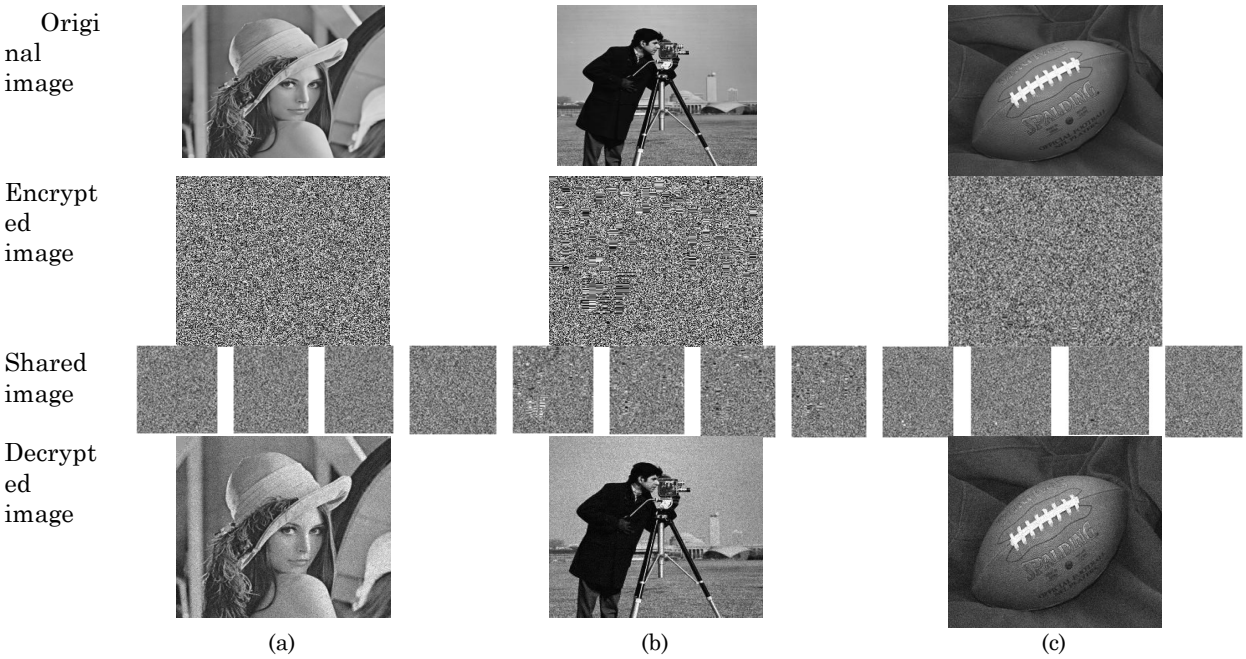


Fig.3.*Sample image of developed scheme for "(a) image 1 (Lena) (b) image 2 (Cameraman) and (c) image 3 (Baboon)"*

7.2 PSNR Analysis

The performances of the introduced MFM-WO scheme are assessed over extant models concerning PSNR. Fig. 4 portrays the PSNR value attained for 3 types of images (Lena, cameraman, and Baboon). It reveals the correlation between the original image as well as reconstructed image. While scrutinizing the graph, the higher rates of PSNR values have guaranteed the development of the presented scheme. Accordingly, the PSNR resultants for image 1 (Lena) are portrayed in Fig. 5 (a), and PSNR resultants for image 2 (cameraman) are described in Fig. 5 (b), and the PSNR resultants for image 3 (baboon) are shown in Fig. 5 (c) for diverse noise levels that lie from 0, 10, 15, 20, 25, and 30. On scrutinizing the whole graphs, the offered MFM-WO scheme has acquired improved outcomes than the evaluated methods. Especially, superior PSNR values assure the improved encryption potential of the offered scheme. From Fig. 5 (a), the offered MFM-WO approach has attained superior PSNR value, i.e. 3.7%, 7.4%, 7.4%, 3.7%, 3.7%, 7.4%, 11.11%, and 11.11% improved than MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map models while the noise level is 10. In addition, from the graph, it is noted that the PSNR values for every technique go on lessening with a rise in the level of

noise. Nevertheless, the developed MFM-WO approach has shown superior PSNR values than the evaluated schemes. In particular, from Fig. 5 (c), the PSNR of the developed MFM-WO technique is 7.4%, 7.4%, 7.4%, 11.11%, 11.11%, 11.11%, 3.7%, and 3.7% superior to traditional methods such as MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map models when the noise level is 10. On exploring the PSNR values obtained for the 2nd image from Fig. 5 (b), the developed MFM-WO approach has represented a superior value over other approaches, i.e. the adopted model has attained a superior PSNR value of 27.5, whereas, methods such as MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and the chaotic logistic map has acquired comparatively negligible values of 26, 25.5, 26.5, 26.5, 26, 25.5, 24.8 and 26 in that order. i.e., the PSNR of offered MFM-WO approach is 5.77%, 7.84%, 3.77%, 3.77%, 5.77%, 7.84%, 10.89%, and 5.77% superior to traditional methods such as MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map models when the noise level is 10. On the whole, the performances of the proposed MFM-WO are established over other schemes.

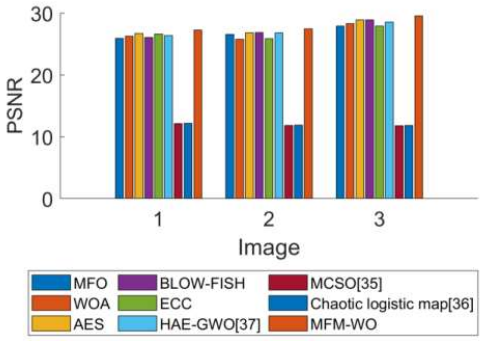
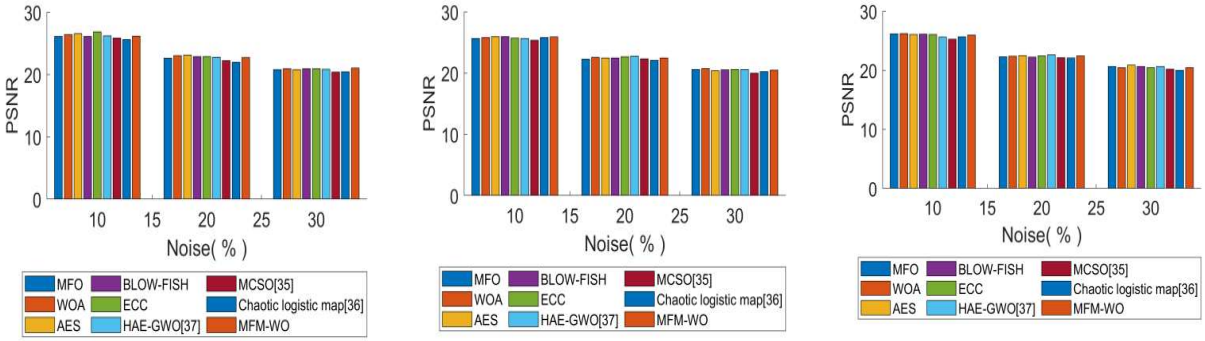


Fig.4.*PSNR analysis of developed scheme over extant schemes for three types of images*



(a) (b) (c)

Fig.5. *PSNR analysis of developed scheme over extant schemes for "(a) image 1 (b) image 2 and (c) image 3"*

7.3 Convergence Analysis

Thecost (convergence) analysis of the introduced approach over conventional optimization approaches regarding cost is describedin Fig. 6. Here, the investigation is done for a diverse count of iterations that ranges from 0, 5, 10, 15, 20, and 25. On noticing the examination outcomes, the introduced approach has obtained the least amount of cost values for each iteration when distinguished over the conventional schemes. From Fig. 6, the offered model achieved a much superior cost value from the 0th iteration to the 5th iteration. After 5th iteration, there is a sudden drop incost values for proposed and distinguished models. Also, the convergence function of the adopted method is found to have obtained a stable cost value from the 15th iteration to the 25th iteration. After the 25th iteration, the recommended model has attained the lowest cost values ofevery other distinguished model. The higher convergence is the most important reason for harmonic interference in both the MFO and WOAalgorithms. Predominantly, on noticing the cost value in Fig. 6, the implemented method has obtained a condensed cost value (33.2), and it is 1.51% and 1.17% superior to traditional MFO and WOA models when the number of iterations is 20. As a result, the overall evaluation demonstrates the impact of the proposed MFM-WO model on improved convergence to the described objective. The proposed features thus assist in the steady convergence of cost function by guaranteeing optimal key creation for encryption purposes.

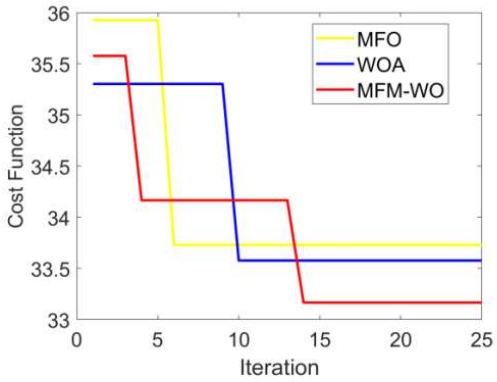


Fig.6.*Convergence analysis of developed method over traditional methods*

7.4 Analysis of Correlation, Encryption Quality and PSNR

The performance of the developed MFM-WO method over the existing techniques concerning correlation, encryption quality, and PSNR is elucidated in this division. Here, Table 2 demonstrates the performance of the deployed MFM-WO method over the conservative methods for correlation, Table 3 analyses the encryption quality and Table 4 analyses the PSNR values. Subsequently, the examination was done for 3 types of images (Lena, cameraman, and Baboon). Accordingly, the correlation analysis is shown in Table 2, in which the developed approach has established a higher correlation than the distinguished schemes. On exploring Table 4, the PSNR of the introduced approach is higher for all image types (Lena, cameraman, and Baboon) than the existing approaches. Particularly, in Table 2, the introduced MFM-WO method attains higher PSNR than other models for image 3 (baboon). Predominantly, the PSNR of the developed model for 3rd image is 5.78%, 4.41%, 2.17%, 2.26%, 5.78%, 3.45%, 60.17% and 59.93% superior to MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO and chaotic logistic map models for image 3. In Table 3, the encryption quality is superior for the developed model than the compared models for all image types (Lena, cameraman, and Baboon). Indefinite cases, the encryption quality of distinguished models is found to be superior to the deployed MFM-WO approach, nevertheless, while considering the other constraints like PSNR, cost, and correlation values, the introduced MFM-WO method attains higher performance than the extant models. Therefore, this deviation can be considered insignificant. Hence, the introduced algorithm affirmed superior performance in satisfying the described VC model.

Table 2. *Correlation Analysis of the presented approach over existing approaches for varied images*

Methods	MFO	WOA	AES	Blowfish	ECC	HAE-GWO [37]	MCSO [35]	Chaotic logistic map [36]	MFM-WO
Image 1	0.32197	0.3281	0.32691	0.32438	0.33233	0.3397	0.32697	0.32717	0.34199
Image 2	0.31098	0.32161	0.3227	0.33615	0.34828	0.34743	0.32832	0.31962	0.34906
Image 3	0.34037	0.33963	0.33975	0.31424	0.33726	0.32853	0.31849	0.31394	0.34294

Table 3. *Encryption Quality Analysis of the presented approach over existing approaches for varied images*

Methods	MFO	WOA	AES	Blowfish	ECC	HAE-GWO [37]	MCSO [35]	Chaotic logistic map [36]	MFM-WO
Image 1	123.44	122.6	122.58	123.1	123.01	123.25	77.842	87.587	123.36
Image 2	117.67	117.57	117.83	117.85	118	117.74	73.648	90.939	117.8
Image 3	73.734	73.032	73.152	72.947	73.194	73.664	45.731	120.65	73.034

Table 4. *PSNR Analysis of of presented approach over existing approaches for varied images*

Methods	MFO	WOA	AES	Blowfish	ECC	HAE-GWO [37]	MCSO [35]	Chaotic logistic map [36]	MFM-WO
Image 1	25.889	26.249	26.669	26.035	26.578	26.348	12.109	12.166	27.232
Image 2	26.533	25.771	26.808	26.834	25.825	26.768	11.814	11.843	27.43
Image 3	27.909	28.276	28.896	28.871	27.91	28.538	11.759	11.83	29.523

7.5 Analysis ofAuditing time and Key sensitivity

The performances of developed MFM-WO are evaluated over extantmodels (MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map) regarding varied metrics like auditing time and key

sensitivity. The examination of the deployed MFM-WO model is compared over MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map models for varied types of images (Lena, cameraman, and Baboon). Consequently, analysis was held using the dataset in [39] and the pertinent results are shown in Table 5 and Table 6. In Table 5, for all types of images, the presented MFM-WO model has attained better outcomes (minimal auditing time) than distinguished models. Principally, minimal auditing time values promise better performance of the developed scheme. On examining Table 5, the auditing time of the developed approach for image 3 is lower than other image types, i.e. for image 3; the auditing time of the developed approach is 0.16431, whereas, for image 2, the developed model has obtained comparatively higher auditing time values of 0.17277. Likewise, for image 1 (Lena), the outputs for the developed model are minimal compared to models. Thus, the developed approach has interpreted more effectual outputs than distinguished schemes for every image type. For instance, for image 3, the auditing time of the developed approach is 4.06%, 3.2%, 16.06%, 16.62%, 8.73%, 14.23%, 0.76%, and 15.04% better than the values obtained for conventional schemes like MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map respectively. In addition, the values attained by the developed MFM-WO scheme for varied keys such as 1, 2, 3, and 4 areshown in Table 6. Thus from the assessment, better efficacy of the developed MFM-WO is established with the incorporation of optimization theory.

Table 5. *Analysis ofAuditing time attained bythe presented approach over existing approaches for varied images*

Methods	MFO	WOA	AES	Blowfish	ECC	HAE-GWO [37]	MCSO [35]	Chaotic logistic map [36]	MFM-WO
Image 1	0.18147	0.19134	0.1785	0.19649	0.19572	0.17419	0.17922	0.18357	0.16787
Image 2	0.19058	0.18324	0.19469	0.17858	0.18538	0.17522	0.19595	0.18491	0.17277
Image 3	0.17127	0.16975	0.19575	0.19706	0.18003	0.19157	0.16557	0.1934	0.16431

Table 6. *Key sensitivity Analysis attained bythe presented approach for varied keys*

Methods	MFM-WO	Key 1	Key 2	Key 3	Key 4
Image 1	0.34199	0.28967	0.070345	0.15307	0.087191
Image 2	0.34906	0.16838	0.06144	0.16632	0.073594
Image 3	0.34294	0.18553	0.24394	0.10611	0.21719

8. Conclusion

This work developed a new VC approach for the secured storing of multimedia data in the cloud. At first, the image from the transmitted side was encrypted via a modified Elgamal algorithm with the optimal generation of the key. Accordingly, share generation was done, in which the image was divided into N count of shares. As per the share count, the EXOR operation was made among original image bits and keys. After that, the consequential encrypted shared image was stored in the cloud server. Finally, decryption was done at the receiver end, which was the reverse course of action of encryption. Consequently, optimal key generation was performed usingthe MFM-WO model that assisted in obtaining the objectives. From the outcomes, for image 1 (Lena), the outputs for the developed model were minimal than the compared models. Thus, the developed approach has interpreted more effectual outputs than distinguished schemes for every image type. For instance, for image 3, the auditing time of the developed approach was 4.06%, 3.2%, 16.06%, 16.62%, 8.73%, 14.23%, 0.76%, and 15.04% better than the values obtained for conventional schemes like MFO, WOA, AES, blowfish, ECC, HAE-GWO, MCSO, and chaotic logistic map respectively. In the future, it needs contemplation on text-oriented CAPTCHA.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Srinivasa Rao KanusuSridhar Mandapati, "A hybrid population based incremental learning algorithm with Particle Swarm Optimization for general threshold Visual Cryptography schemes", Materials Today: Proceedings, Available online, 6 February 2021, In press, corrected proof.

[2] Karolin, M., Meyyappan, T.,"Authentic secret share creation techniques using visual cryptography with public key encryption. Multimed Tools", Appl 80, pp. 32023 – 32040 (2021). https://doi.org/10.1007/s11042-021-11202-6.
[3] Ahmad, S., Hayat, M.F., Qureshi, M.A.,"Enhanced halftone-based secure and improved visual cryptography scheme for colour/binary Images", Multimed Tools Appl 80, 32071 – 32090,2021. https://doi.org/10.1007/s11042-021-11152-z.
[4] Ren, Y., Liu, F., Yan, W.,"A new visual evaluation criterion of visual cryptography scheme for character secret image", Multimed Tools Appl 78, 25299 – 25319,2019. https://doi.org/10.1007/s11042-019-7698-x.
[5] P. GeethaV. S. JayanthiA. N. Jayanthi, "Optimal visual cryptographic scheme with multiple share creation for multimedia applications", Computers & Security, vol. 78 (Cover date: September 2018) pp. 301 - 320, 27 July 2018.
[6] Ali FatahbeygiFardin Akhlaghian Tab, "A highly robust and secure image watermarking based on classification and visual cryptography", Journal of Information Security and Applications, vol. 45 (Cover date: April 2019), pp. 71 - 78, 22 January 2019.
[7] Geetha, P., Jayanthi, V.S. & Jayanthi, A.N,"Multiple share creation based visual cryptographic scheme using diffusion method with a combination of chaotic maps for multimedia applications", Multimed Tools Appl 78, pp. 18503 – 18530,2019. https://doi.org/10.1007/s11042-019-7163-x.
[8] Gurunathan, K., Rajagopalan, S.P,"A stegano - visual cryptography technique for multimedia security", Multimed Tools Appl, Vol. 79, pp. 3893 – 3911 2020. https://doi.org/10.1007/s11042-019-7471-1.
[9] Jinu Mohan, Dr Rajesh R, "ENHANCING home security through visual CRYPTOGRAPHY", Microprocessors and Microsystems, Volume 80 (Cover date: February 2021), Article 103355, 24 October 2020.
[10] Jyoti TripathiAnu Saini Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security", Procedia Computer Science, Volume 167 (Cover date: 2020), pp. 323 - 333, 16 April 2020.
[11] Pei-Ling ChiuKai-Hui Lee, "Efficient constructions for progressive visual cryptography with meaningful shares", Signal Processing, vol. 165 (Cover date: December 2019), Pages 233 - 249, 9 July 2019.
[12] Xiaotian Wu, Ching-Nung Yang, "Probabilistic color visual cryptography schemes for black and white secret images", Journal of Visual Communication and Image Representation, vol. 70 (Cover date: July 2020), Article 102793, 11 March 2020.
[13] B. Yan, Y. Xiang, and G. Hua, "Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach," IEEE Transactions on Image Processing, vol. 28, no. 2, pp. 896 - 911, Feb. 2019. doi: 10.1109/TIP.2018.2874378.
[14] Y. Chen, "Fully Incrementing Visual Cryptography From a Succinct Non-Monotonic Structure," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1082-1091, May 2017. doi: 10.1109/TIFS.2016.2641378.
[15] N. Askari, H. M. Heys and C. R. Moloney, "Novel Visual Cryptography Schemes Without Pixel Expansion for Halftone Images," in Canadian Journal of Electrical and Computer Engineering, vol. 37, no. 3, pp. 168-177, Summer 2014. doi: 10.1109/CJECE.2014.2333419.
[16] X. Wu and W. Sun, "Extended Capabilities for XOR-Based Visual Cryptography," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1592-1605, Oct. 2014. doi: 10.1109/TIFS.2014.2346014.
[17] Z. Fu, Y. Cheng and B. Yu, "Visual Cryptography Scheme With Meaningful Shares Based on QR Codes," IEEE Access, vol. 6, pp. 59567 - 59574, 2018. doi: 10.1109/ACCESS.2018.2874527.
[18] Z. Stanisavljevic, J. Stanisavljevic, P. Vuletic and Z. Jovanovic, "COALA - System for Visual Representation of Cryptography Algorithms," IEEE Transactions on Learning Technologies, vol. 7, no. 2, pp. 178 - 190, 1 April-June 2014. doi: 10.1109/TLT.2014.2315992.pril 2018, In press, corrected proof.
[19] Sugawara, S., Harada, K. & Sakai, D.,"High-chroma visual cryptography using interference color of high-order retarder films", Opt Rev 22, pp. 544 –552,2015. https://doi.org/10.1007/s10043-015-0095-4
[20] Li, P., Yang, CN. & Kong, Q.,"A novel two-in-one image secret sharing scheme based on perfect black visual cryptography", J Real-Time Image Proc 14, pp. 41 – 50,2018. https://doi.org/10.1007/s11554-016-0621-z
[21] Selva Mary, G., Manoj Kumar, S.,"Secure grayscale image communication using significant visual cryptography scheme in real time applications", Multimed Tools Appl, Vol. 79, 10363–10382,2020. https://doi.org/10.1007/s11042-019-7202-7
[22] Yan, B., Wang, YF., Song, LY., "Size-invariant extended visual cryptography with embedded watermark based on error diffusion", Multimed Tools Appl. Vol. 75, pp. 11157 – 11180, 2016. https://doi.org/10.1007/s11042-015-2838-4
[23] Sridhar, S., Sathishkumar, R. & Sudha, G.F.,"Adaptive halftoned visual cryptography with improved quality and security", Multimed Tools Appl, Vol. 76, 815 – 834, 2017. https://doi.org/10.1007/s11042-015-3066-7
[24] Hodeish, M.E., Humbe, V.T.,"An Optimized Halftone Visual Cryptography Scheme Using Error Diffusion", Multimed Tools Appl, Vol. 77, pp. 24937 – 24953, 2018. https://doi.org/10.1007/s11042-018-5724-z.
[25] Zhuhong Shao, Yuanyuan Shang, Jiasong Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography", Signal Processing: Image Communication, October 2016.
[26] Zhuhong ShaoYuanyuan ShangJiasong Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography", Signal Processing: Image Communication, October 2016.
[27] B. Pushpa Devi, Kh. Manglem Singh & Sudipta Roy, "New Copyright Protection Scheme for Digital Images Based on Visual Cryptography", IETE Journal of Research, Vol. 63:6, pp. 870 - 880,2017. DOI: 10.1080/03772063.2017.1324328.

[28] Sanjeev Narayan Bal, Manas Ranjan Nayak, Subir Kumar Sarkar, "On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching", Journal of King Saud University - Computer and Information Sciences, Available online 23.
[29] Seyedali Mirjalili, Andrew Lewis, "The Whale Optimization Algorithm", Advances in Engineering Software, vol. 95, pp. 51-67, May 2016.
[30] SeyedaliMirjalili, " Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm", Knowledge-Based Systems, Vol. 89, pp. 228-249, November 2015.
[31] M. Marsaline Beno, Valarmathi I. R, Swamy S. M, and B. R. Rajakumar, "Threshold prediction for segmenting tumour from brain MRI scans", International Journal of Imaging Systems and Technology, Vol. 24, No. 2, pp. 129-137, 2014. DOI: https://doi.org/10.1002/ima.22087.
[32] Renjith Thomas and MJS. Rangachar, "Hybrid Optimization based DBN for Face Recognition using Low-Resolution Images", Multimedia Research, Vol.1,No.1, pp.33-43,2018.
[33] Devagnanam J,Elango N M, "Optimal Resource Allocation of Cluster using Hybrid Grey Wolf and Cuckoo Search Algorithm in Cloud Computing", Journal of Networking and Communication Systems, Vol.3,No.1, pp.31-40,2020.
[34] SK.Mahammad Shareef and Dr.R.Srinivasa Rao, "A Hybrid Learning Algorithm for Optimal Reactive Power Dispatch under Unbalanced Conditions", Journal of Computational Mechanics, Power System and Control, Vol.1,No.1, pp.26-33,2018.
[35] Alif Siddiqua Begum, A., Nirmala, S.,"Secure visual cryptography for medical image using modified cuckoo search", Multimed Tools Appl, Vol. 77, 27041–27060, 2018. https://doi.org/10.1007/s11042-018-5903-y
[36] Sharma, Priyamwada & Sharma, Vedant.,"Secret Image Sharing Over Cloud Using One-Dimensional Chaotic Map", 10.1007/978-981-13-6351-1_2, 2019.
[37] Arun Vuyuru, "Optimization Assisted Blowfish Cryptography based Visual Cryptographic Model for Multimedia Application ", In communication.
[38] Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, no. 6, August 2012.
[39] Vengala, D.V.K., Kavitha, D. & Kumar, A.P.S.,"Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment", Complex Intell. Syst., 2021. https://doi.org/10.1007/s40747-021-00305-0.
[40] Alfred J Menezes, Paul C van Oorschot, Scot A Vanstone, "Handbook of AppliedCryptography", CRC Press, 1997.