Nexo Revista Científica
Vol. 36, No. 06, pp. 1103-1131/Diciembre 2023

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
https://doi.org/10.5377/nexo.v36i06.17468

Enhancing steganography using modified HHO and RC4

Mejora de la esteganografía utilizando HHO y RC4 modificados

Ranj T. Saber[1,*], Omar Y. Abdulhammed[2]

[1]Technical College of Informatics, Sulaimani Polytechnic University – Iraq
[2]College of science, Garmian University - Iraq

*ranj.tareq@spu.edu.iq, Tel.:+964770 1180 413
Omar.y@garmian.edu.krd, Tel.:+964772 526 4970

(recibido/received: 07-agosto-2023; aceptado/accepted: 23-noviembre-2023)

ABSTRACT

A lot of information is being sent around the globe these days, which increases the risk of knowledge leakage; as a result, it is crucial to preserve information security while exchanging data. Steganography and cryptography are the most essential methods, among many others, to guarantee the data's confidentiality. Encryption is making information unintelligible to anybody but the intended recipients. However, steganography is the study of hiding information in digital media so that nobody can detect it is there. This research introduces two methods for concealing and encrypting messages that improve the Stego image's visual quality and security while offering a sizable embedding capacity. A stream cipher method with a symmetric key, the RC4 algorithm, is utilized to encrypt and decode secret information. At the same time, a population-based metaheuristic, modified HHO, is employed to find the optimum spots in the cover medium to conceal encrypted sensitive data. Regarding security, picture quality, and attack resistance, the testing findings show that the proposed method excels over competing methods in terms of time and cost.

Keywords: Security; Steganography; Swarm Inelegance; Harry Hawk Optimizer; RC4 Algorithm;

RESUMEN

Hoy en día se envía mucha información a todo el mundo, lo que aumenta el riesgo de fuga de conocimientos; Como resultado, es crucial preservar la seguridad de la información al intercambiar datos. La esteganografía y la criptografía son los métodos más imprescindibles, entre muchos otros, para garantizar la confidencialidad de los datos. El cifrado hace que la información sea ininteligible para cualquiera que no sea el destinatario previsto. Sin embargo, la esteganografía es el estudio de ocultar información en medios digitales para que nadie pueda detectar que está allí. Esta investigación presenta dos métodos para ocultar y cifrar mensajes que mejoran la calidad visual y la seguridad de la imagen Stego al tiempo que ofrecen una capacidad de incrustación considerable. Se utiliza un método de cifrado de flujo con una clave simétrica, el algoritmo RC4, para cifrar y decodificar información secreta. Al mismo tiempo, se emplea una metaheurística basada en la población, HHO modificada, para encontrar los puntos óptimos en el medio de cobertura para ocultar datos confidenciales cifrados. En cuanto a la seguridad, la calidad de la imagen y la resistencia a los ataques, los resultados de las pruebas muestran que el método propuesto supera a los métodos de la competencia en términos de tiempo y costo.

Palabras claves: Seguridad; esteganografía; Inelegancia del enjambre; Optimizador Harry Hawk; Algoritmo RC4;

1. INTRODUCTION

The security of information conveyed to the recipient is a critical component of data communication. Steganography is communicating invisibly between two people by hiding and embedding their message in another object known as a cover Object (Image) (abd ulkareem and Abduljaleel n.d.; Abdel-Salam Nasr, AlRahmawy, and Tolba 2017).

Unlike encryption, which seeks to safeguard communications from eavesdroppers, steganography techniques seek to conceal the message from observers (ABDULHAMMED 2022; Abduljaleel et al. 2022).

Steganography has attracted substantial interest in research, development, and communities during the last two decades, owing to the Internet's and digital media's accelerating advances. This is referred to as “the science of unseen communication.” (ABDULHAMMED 2022; Alparone et al. 2008; Aniba and Aïssa 2009).

Image steganography is intended for data security, such as digital communication, invisible communication via digital media, and digitized ownership copyright protection (Bedi, Bansal, and Sehgal 2011).

The kind of cover image employed (2D or 3D pictures), target application type or retrieval process (reversible or irreversible), nature of an embedding process (spatial or transform domain), and adaptive steganography are the categories of steganography. In addition, each group might be labeled as Figure (1) (De Carvalho and Meneses 2000).

In this paper, a stream cipher RC4 Algorithm with a symmetric key is used to encrypt messages (plain text), and a modified Harris Hawks Optimization Algorithm (HHO) is used to find the best position to hide cipher messages in the cover image, which is used for transferring and establishing secure communication between Sender and receiver. One of the swarm intelligence approaches, the HHO algorithm, is based on the Hawks population's (agents') strategy for locating prey as the best fitness. In this situation, the workspace is the cover picture pixel with the best fitness value determined by agents (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020). As plain text will be encrypted using RC4 stream cipher algorithm (Stallings 2017) and changed to bindery format in the encoding phase, then each bit will be hidden using a replacement with cover image least significant bit (LSB) (Du et al. 2020) to produce a stego image in the embedding phase.

Instead of using the standard HHO technique, a modified version is used to hide information by assessing the Red (R) color of each pixel's value to find the optimal spot (pixel) for concealing information and then hiding the information in the blue (B) color of the same pixel. To achieve better performance and cost for the search, modified HHO work on separating the working place into parts (Blocks).

Using the modified HHO algorithm, in which the only change is to the least significant bit (LSB) of the Blue color of the determined pixel, we overcame stego image distortion based on image quality standards. We compared it to the original cover image and improved steganalysis (eavesdropping). Each pixel of the color image contains three primary colors: Red, Green, and Blue (abd ulkareem and Abduljaleel n.d.; Du et al. 2020; Féraud 2017).

RC4 stream cipher algorithm is used because it is fast and straightforward, and its weakness is overcome by using the dynamic key in the stego image communication.

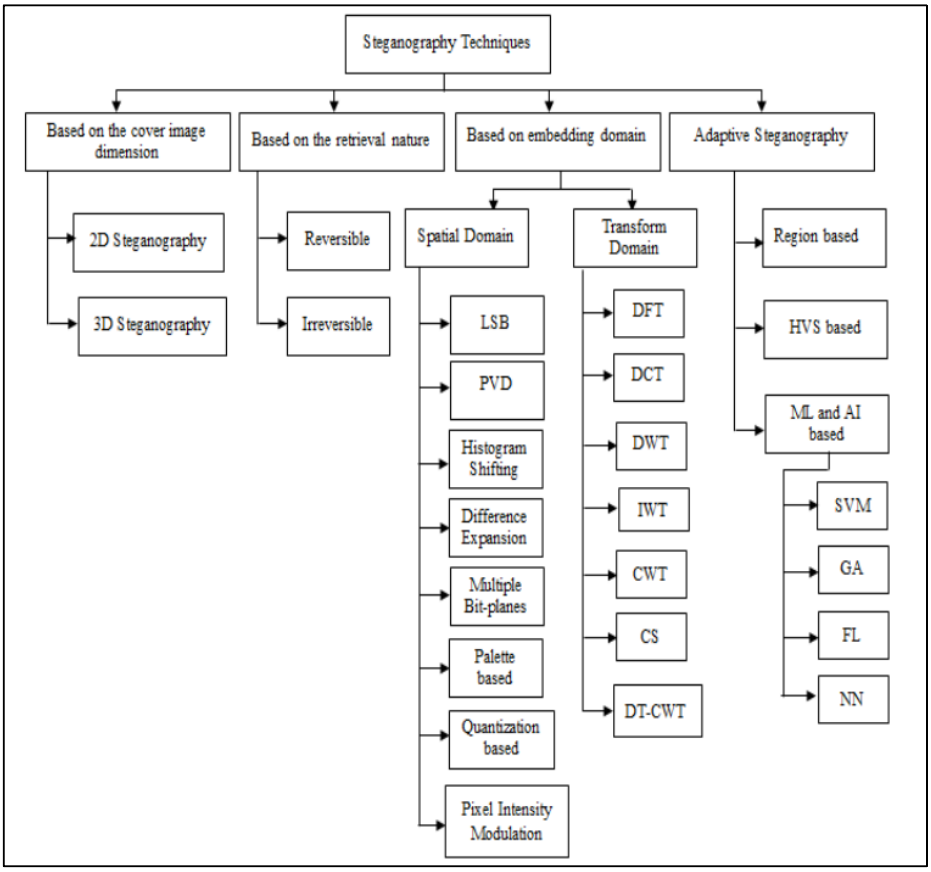


Figure 1. Classification of Image Stenography Techniques (De Carvalho and Meneses 2000).

2. STEGANOGRAPHY

Stenography is one form of security that aims at concealing the hidden message within an object (cover image) alongside Cryptography and Watermarking (S. Fluhrer, Mantin, and Shamir 2001). There are several categories for cover art. 2D pictures like those in grayscale and binary and 3D images like those in the RGB color space are included. Based on the size of the cover picture, the stenographic system may be divided into 2D image steganography and 3D image steganography (S. R. Fluhrer and McGrew 2001). Cover embedding in 2D and 3D can occur on pixel values in the spatial domain or coefficient values in the transform (Frequency) domain (Abduljaleel et al. 2022; De Carvalho and Meneses 2000). In this paper, a 3D cover image is used. 3D image steganography can generally be made in several ways: Geometrical domain (Fred Glover 1989; Hameed, Abdel-Aleem, and Hassaballah 2023), Topological domain (Jia et al. 2020)(Bao, Jia, and Lang 2019), and Representation domain (S. Heidari et al. 2017) steganography. The goal of 3D image steganography is to conceal the secret bit streams within a 3D cover image's vertex. When more weight needs to be carried, 3D cover image geometric models are more effective and practical.

Security, robustness, and capacity are the three primary factors (criteria) that a security system must achieve while creating steganography systems (Aniba and Aïssa 2009). additionally, the quality of the image is preserved.

3. KEY EMBEDDED PERFORMANCE INDICATOR

Key embedded performance indicators to evaluate distortion on Stego Image and algorithm efficiency are used to select the proper position. Below are the metrics used to compare the original images (cover image) and the encrypted ones (ABDULHAMMED 2022),(Evsutin et al. 2020).

1. Mean Squared Error (MSE) is the most frequently used image quality metric that compares the average square density of the cover image and Stego one (Féraud 2017). Based on below Eq. (1) (Nickfarjam and Azimifar 2012):

$$MSE = \frac{1}{V \times W} \sum_{i=1}^{V} \sum_{j=1}^{W} [I(i,j) - I^{c}(i,j)]^{2} \qquad 1$$

While the cover image is the Stego image, V is the Vertical length of the image, and W is the Wide length. The lower value is better, and 0 means the model is perfect.

2. Root Mean Squared Error (RMSE), besides MSE, sometimes RMSE is used based on the below Eq. (2) (Evsutin et al. 2020):

$$\mathrm{RMSE} = \sqrt{\mathrm{MSE}}. \qquad 2$$

RMSE values between 0.2 and 0.5 show that the model can relatively predict the data accurately.

3. Peak Signal-to-Noise Ratio (PSNR), the ratio between the maximum possible power of typical values for the Image to MSE called PSNR as shown below Eq. (3) (Evsutin et al. 2020):

$$\mathrm{PSNR}\ (\mathrm{dB}) = 10 \times \log_{10}\left(\frac{255^{2}}{\mathrm{MSE}}\right) \qquad 3$$

Its value is changed based on Image density, but the PSNR value is optimal from 60 dB to 80 dB(Chervyakov, Lyakhov, and Nagornov 2020).

4. Structural Similarity Index (SSIM): SSIM aims to capture the similarity of both images (Cover and Stego image) by calculating three aspects: luminance [$l(\mathbf{x}, \mathbf{y})$], contrast [$c(\mathbf{x}, \mathbf{y})$], and structure [$s(\mathbf{x}, \mathbf{y})$] (Yim and Bovik 2011) while X as the cover image and y as Stego image as Eq. (4, 5 and 6) (Bao, Jia, and Lang 2019) :

$$l(x,y) = \frac{2\mu_x \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \qquad 4$$

$$c(x,y) = \frac{2\sigma_x \sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \qquad 5$$

Where µx and µy are the Mean values of X and Y, σx and σy are the standard deviation of X and Y, and C1, C2 is the stabilizing constant.

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x \sigma_y + C_3} \qquad 6$$

Where σx and σy are the correlations between X and Y, and C3 is the stabilizing constant. Finally, SSIM will be calculated as Eq. (7) formula (Bao, Jia, and Lang 2019):

$$SSIM(x,y) = \left[l(x,y)\right]^{\alpha} \left[c(x,y)\right]^{\beta} \left[s(x,y)\right]^{\gamma} \qquad 7$$

Where α, β, and γ are three parameters decided by the white of its parts. Also if we consider α = β = γ =1 and C3 = C2/2 (Yim and Bovik 2011) Eq. (8,9) will be:

$$\mathrm{SSIM}(\mathbf{x},\mathbf{y}) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2+\mu_y^2 + C_1)\,(\sigma_x^2+\sigma_y^2 + C_2)} \qquad 8$$

$$\mathrm{SSIM}(\mathbf{x},\mathbf{y}) = \frac{1}{M}\sum_{j=1}^{M} \mathrm{SSIM}(\mathbf{x}_j,\mathbf{y}_j) \qquad 9$$

M is the number of local windows over the image, and Xj and Yj are image patches covered by the Jth window(Yim and Bovik 2011). The resultant SSIM index is a decimal value between -1 and 1, where 1 indicates perfect similarity, 0 means no similarity, and -1 indicates perfect anti-correlation(Sara, Akter, and Uddin 2019).

5. Universal Quality Image Index (UQI) will be defined in particular cases when SSIM if C1 = C2 = 0, this will lead to unstable results while $(\mu_x^2+\mu_y^2)$ or $(\sigma_x^2+\sigma_y^2)$ is very close to zero (Knudsen et al. 1998; McGee et al. 2000), so UQI will be defined as Eq. (10) (Bedi, Bansal, and Sehgal 2011):

$$Q = 4\sigma_{xy}\,\hat{x}\hat{y} \big/ (\hat{x}^2 + \hat{y}^2)(\sigma_x{}^2 + \sigma_y{}^2) \qquad 10$$

X is the cover image, y is the Stego image, and X^ and Y^ are the corresponding averages of X and Y, respectively; σx2 and σy2 are the variances of X and Y, and σxy is the covariance of X and Y.
The expected result of UQI is [1 -1], which results in Xi = Yi for i= 1,2,3 … n. (Rao and Pandit 2011)

6. Multi-scale Structural Similarity Index (MS-SSIM) and the advanced version of SSIM called MS-SSIM, in which two images will be compared in SSIM by different image scales of the same size and resolution(Sara, Akter, and Uddin 2019) based on the Eq. (11) (Abdel-Salam Nasr, AlRahmawy, and Tolba 2017):

$$MS - SSIM(x,y) = [l_m(x,y)]^{\alpha_M} \cdot \prod_{j=1}^{M} [C_j(x,y)]^{\beta_j} \cdot [S_j(x,y)]^{y_j} \qquad 11$$

Where M corresponds to the lowest resolution, α, β, and γ are three parameters decided by the white of its parts. Also, if we consider α = β = γ =1 and Cj is a stabilizing constant. The best results for values are between 0.985 and 0.995 (Abdel-Salam Nasr, AlRahmawy, and Tolba 2017).

7. Erreur Relative Globale Adimensionnelle de Synthèse (ERGAS) gave an overall evaluation of the quality of a Stego image based on the Eq. (12) (Alparone et al. 2008):

$$\mathrm{ERGAS} \triangleq 100\frac{d_h}{d_l}\sqrt{\frac{1}{L}\sum_{l=1}^{L}\left(\frac{\mathrm{RMSE}(l)}{\mu(l)}\right)^2} \qquad 12$$

Where dh/dl is the ratio between the Cover image and Stego Image pixel sizes, μ(l) is the mean (average) of the lth band, and L is the number of rounds. This index measures distortion and thus must be as small as possible.

8. Relative Average Spectral Error (RASE) represents the specification of the average performance of a method in the considered spectral bands as Eq. (13) (Li 2006; Wald 2000):

$$RASE = \frac{100}{M}\sqrt{\frac{1}{N}\sum_{i=1}^{N} RMSE(B_i)^2} \qquad 13$$

Mi is the mean value for the N Spectral band of the spectral image Bi, and RMSE is the Root mean square error. A threshold of the acceptable image is set to 3. Less than 3, the error is small, and the image is good quality. Above 3, the error is significant, and the image is of lower quality(Wald 2000).

9. Spectral Angle Mapper (SAM) tries to calculate the angles formed between the cover image and Stego image based on the Eq. (14, 15) (De Carvalho and Meneses 2000),(Yuhas, Goetz, and Boardman 1992):

$$\alpha = \cos^{-1}\frac{\Sigma\, \mathbf{XY}}{\sqrt{\Sigma(\mathbf{X})^2\, \Sigma(\mathbf{Y})^2}} \qquad 14$$

This equation will also be written as:

$$\cos\alpha = \frac{\Sigma\, \mathbf{XY}}{\sqrt{\Sigma(\mathbf{X})^2\, \Sigma(\mathbf{Y})^2}} \qquad 15$$

Where α = SAM Angle formed between the reference spectrum and image spectrum, X = Image spectrum, and Y = Reference spectrum. An optimal value for SAM is near 1.

10. Visual Information Fidelity (VIF) is extracting from a measuring of two mutual information quantities: the mutual information between the input and the output of the HVS channel when no distortion channel is present (called the cover image information) and the mutual information between the input of the distortion channel and the output of the HVS channel for the Stego image. Like SSIM, the assessment result is represented using a value between 0 and 1(Mahmoudpour and Kim 2015; Wald 2000). Based on the Eq. (16):

$$\mathrm{VIF} = \frac{\sum_{j\in\mathrm{subbands}} I(\vec{C}^{N,j};\vec{F}^{N,j}|s^{N,j})}{\sum_{j\in\mathrm{subbands}} I(\vec{C}^{N,j};\vec{E}^{N,j}|s^{N,j})} \qquad 16$$

Where I is mutual information representing N elements of the RFCj (while RFs $\mathcal{N} = \{\vec{N}_i : i \in I\}$, $\vec{N}_i$ are zero mean un-correlated multivariate Gaussian with the same dimensionality as $\vec{C}_i$), it describes the coefficients from sub-band j. It denotes a realization of a particular reference image. The realization could be considered "model parameters" for the associated reference image. $\vec{E}$, and $\vec{F}$ correspondingly define(Sheikh and Bovik 2006).

11. Mean Absolute Error (MAE) is another measurement for quantified model evaluation, which is used mainly with RMSE, based on Eq. (17) (Chai and Draxler 2014):

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} |e_i| \qquad 17$$

Where n is a sample of error e calculated as (ei,i=1,2,3, …, n), the expected value is from 0 to ∞ , but a lower value is more accurate because a lower error is more efficient.

12. Mean square signal-to-noise ratio (SNR) is a level difference between the mean square error of the cover image and the mean square error of the Stego image, measured in dB as Eq. (18) (Rao and Pandit 2011).

$$SNR = 10\log_{10}\left(\frac{MSE2}{MSE1}\right)dB \qquad 18$$

MSE1 is the mean square error of the cover image, and MSE2 is the mean square error of the Stego image. SNR value is acceptable when it is more significant than 40 dB.

13. Correlation Coefficient CC: The correlation coefficient is a statistical measure of the cover image and Stego pixel values. After calculating and removing standard errors.(Pan 2011) Its values can range from -1 to 1. This can be represented by the Eq. (19) (Pan 2011):

$$\sigma^2_{X,Y} = \frac{\sum_{i=1}^{N}\left(X_i - \overline{X}\right)\left(Y_i - \overline{Y}\right)}{N} \qquad 19$$

Where σ2X, Y: Covariance between variables X and Y.
Xi: The ith observation of the X variable.
X¯: The mean value of variable X.
Yi: The ith observation of the Y variable.
Y¯: The mean value of variable Y.
N: Total number of observations for variables X and Y.

14. Bit Error Ratio (BER) is a percentage of the number of error bits divided by the total number of transmitted bits during a time, and as much as more minor is better(Aniba and Aïssa 2009; Helmy et al. 2017; Matalgah 2018).

15. Encryption Quality (EQ) can be calculated by the total changes in pixel values between the cover image and the encrypted (Stego) one, based on Eq. (20) (Nagy 2020).

$$\text{encryption quality} = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)}{256}. \qquad 20$$

Where HL (F) is the number of occurrences for each gray level L in the cover image (plain image), and HL(F`) is the number of occurrences for each gray level L in the stego image (cipher image). The expected value is between 0 and 1.

16. Unified Average Changing Intensity (UACI): This KPI is designed to measure the intensities modified between the Original picture and the Stego one; it will be calculated based on Eq. (21) (Nagy 2020).

$$UACI = \frac{1}{M * N}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C1(i,j) - C2(i,j))}{255}\right]100\% \qquad 21$$

Where M and N are the width and height of the encrypted picture, C1(i,j) is the interferogram encrypted before a pixel change. C2(i,j): is the encrypted interferogram after a pixel change. An acceptable value is 33.46%

17. Hamming Distance Measure (HD): calculating the delta between Stego and the Original image is called the Avalanche effect, measured by Hamming Distance (HD). HD in Information theory measures the dissimilarity between code words as Eq. (22) (Patil et al. 2016).

$$d_{\mathrm{H}}(\mathbf{x},\mathbf{y}) = \left|\{i \in \{1,\ldots,n\} | \mathbf{x}[i] \neq \mathbf{y}[i]\}\right| \qquad 22$$

Where X is the covered image, and Y is the Stego image, a much more significant dissimilarity means a better Algorithm. In this case, the maximum is 24.

18. Shannon Entropy (SN) and Randomness do not make a correlation between the cover image and Stego, which Entropy will measure. A higher entropy value will result in difficulty in recovering plain text from the Stego image attackers.(Patil et al. 2016), (McGee et al. 2000)
19. Histogram: the image's histogram is another quality tool for evaluating and comparing the Stego image with its original version. The histogram graph indicates the frequency of pixel intensity values, where the x-axis refers to the gray level intensities and the y-axis refers to the frequency of these intensities. By comparing the histogram graphs of two images, one can decide whether the images match (S. Heidari et al. 2017).

4. RC4 ALGORITHM

RC4 is classified as a steam cipher encryption method with variable key size, plain text one byte at a time. It was designed by Ron Rivest in 1987 for RSA (Rivest-Shamir-Adleman) Security; the Algorithm is based on the use of Random permutation as Eq. (23) (abd ulkareem and Abduljaleel n.d.; Stallings 2017).

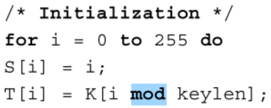
$$P(n,r) = \frac{n!}{(n-r)!} \qquad 23$$

It is used in standard techniques for communication between Web browsers and Servers known as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and in recent WiFi Protected Access (WPA) protocols, which are part of the IEEE 802.11 wireless LAN standard (Stallings 2017).

RC4 algorithm has a variable key size from 1 to 256 bytes (8 to 2048 bits), which is used to initialize 256-byte state vector S. S contains an 8-bit permutation number from 0 to 255; byte K is generated by selecting one of the 255 entries of S. These steps can be summarized as (Stallings 2017):

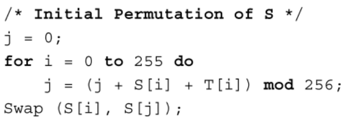
4.1. Initialization of S:

An array of S, as shown in Figure (2. a) will be initialized at the beginning of the RC4 algorithm from 0 to 255 ascending mean S [0] = 0, S [1] = 1, and S [255] = 255; another array will be created as T to transfer K to T if K is 256 bytes, otherwise if Keylen is not 256 first elements of T will be filled by K and the rest will be repeated until T will be completed. The procedure can be summarized as follows:(Stallings 2017)



```
/* Initialization */
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

In the next step, the initial permutation of S will be done for each element of S starting from S [0] to S [255], and this is based on the elements of T as shown below:

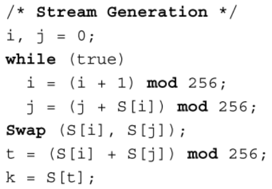


```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

The content of S will not be changed (will contain from 0 to 255) as shown in Figure (2. b), while the permutation operation is based on S content itself.

4.2. Stream Generation

A key steam generation goes over elements of S, while T is no longer the user, and each element of S will be replaced based on a specific configuration as shown in Figure (2. c); it will start from S [0] and swapped with another byte of S [i], and k will be generated which later XOR with plain text to product encrypted text as shown below: (Stallings 2017)



```
/* Stream Generation */
i, j = 0;
while (true)
  i = (i + 1) mod 256;
  j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

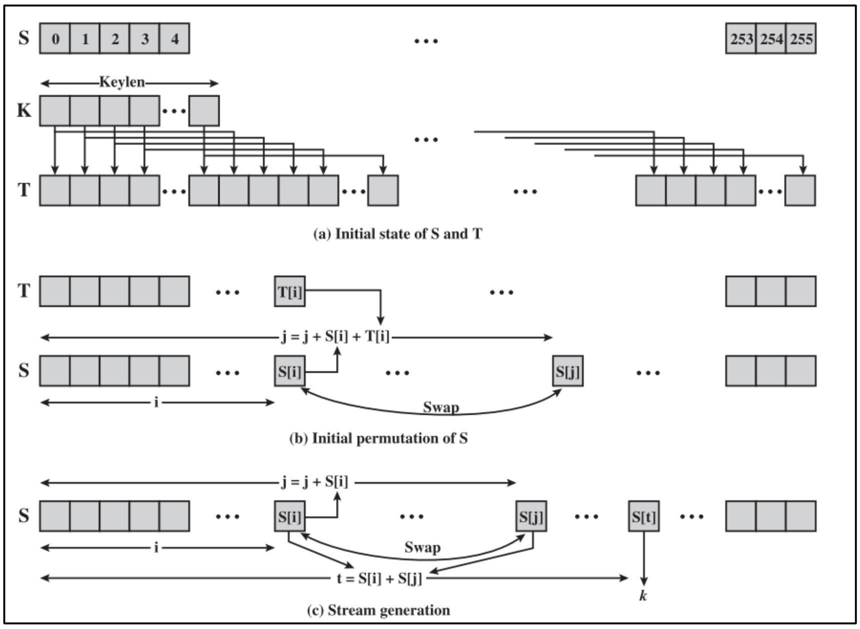


Figure 2. RC4 (Stallings 2017).

4.3. Strength of RC4

Due to its speed and simplicity, the RC4 encryption quickly became the most used stream cipher. However, several papers have been published examining ways to break the RC4 cipher (S. R. Fluhrer and McGrew 2001; Knudsen et al. 1998; Mantin and Shamir 2002). None of these methods can effectively compete with RC4 with a key length of at least 128 bits. A more severe problem is reported in (S. Fluhrer, Mantin, and Shamir 2001). The authors show that the WEP protocol, designed to offer secrecy on 802.11 wireless LAN networks, is vulnerable to a specific attack method. In its most fundamental form, the issue is not with RC4 itself but rather with the process by which keys are produced to serve as input to RC4. Therefore, in this study, a modified version of HHO was utilized to identify the optimal fitness parameters based on pixel red (R) value, and it incorporated a dynamic key in each stego image transmission.

5. HARRIS HAWKS OPTIMIZATION ALGORITHM

Harris Hawks Optimization (HHO) algorithm is one of the swarm intelligence algorithms that simulates the Hawks's mechanism for Hunting based on finding the best rabbit position from different hawks. This can be achieved by three phases: the exploration phase, the transition from exploration to exploitation, and the exploitation phase. (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020)

5.1 Exploration phase

In this phase, Hawks will distribute randomly among the locations, waiting for the prey (rabbit) to be found based on the q value. One of the below strategies will be adopted as Eq. (24) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

$$X(t+1) = \begin{cases} X_{rand}(t) - r_1 \left| X_{rand}(t) - 2r_2 X(t) \right| & q \geq 0.5 \\ (X_{rabbit}(t) - X_m(t)) - r_3(LB + r_4(UB - LB)) & q < 0.5 \end{cases} \quad 24$$

Where X(t + 1) is the position vector of hawks in the next iteration t, Xrabbit(t) is the position of rabbit, X(t) is the current position vector of hawks, r1, r2, r3, r4, and q are random numbers inside (0,1), which are updated in each iteration. LB and UB show the upper and lower bounds of variables. Xrand(t) is a randomly selected hawk from the current population, and Xm is the average position of the current population of hawks. (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020)

The average position of hawks is achieved using Eq. (25). (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020)

$$X_m(t) = \frac{1}{N}\sum_{i=1}^{N} X_i(t) \quad 25$$

Where Xi(t) determines the location of each hawk in each iteration, t and N indicate the total number of hawks as initialized at the beginning of the Algorithm. (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020).

5.2 Transition from Exploration to Exploitation Phase

In this phase, the Algorithm checks prey (rabbit) energy for escaping from Hawks by using Eq. (26) (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020)

$$E = 2E_0(1 - \frac{t}{T}) \quad 26$$

Where E indicates the escaping energy of the prey, T is the maximum number of iterations, and E0 is the initial state of its energy. (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020)

5.3 Exploitation phase

In this phase, it will determine the prey Energy E (|E|≥ 0.5 or |E|< 0.5) and its chance to run r (r>0.5 indicates failed to escape, or r<0.5 indicates success to escape) when it is in danger by four approaches (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

5.3.1 Soft besiege

It will be considered soft besiege while |E|≥ 0.5 and r≥0.5, so Eq. (27,28) will predict the next position of prey (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

$$X(t+1) = \Delta X(t) - E\left|JX_{rabbit}(t) - X(t)\right| \quad 27$$

$$\Delta X(t) = X_{rabbit}(t) - X(t) \quad 28$$

Where ΔX(t) is the difference between the position vector of the rabbit and the current location in iteration t, r5 is a random number inside (0,1), and J = 2(1− r5) represents the unexpected jump strength of the rabbit throughout the escaping procedure. The J value changes randomly in each iteration to simulate the nature of rabbit motions (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

5.3.2 Hard besiege

It considers a Hard besiege while |E| < 0.5 and r≥0.5. So, the next position of prey will be predicted by Eq. (29) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002). Figure (3) illustrates this case.

$$X(t+1) = X_{rabbit}(t) - E\left|\Delta X(t)\right| \quad 29$$

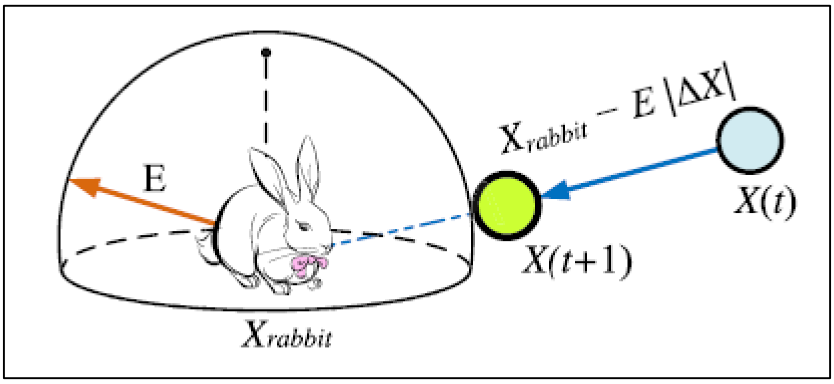


Figure 3 Example of overall vectors Hard besiege case

5.3.3 Soft besiege with progressive rapid dives

It will consider a soft besiege with Progressive rapid dives while |E| ≥ 0.5 and r<0.5, so the next position of Hawk will be predicted by Eq. (30) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

$$Y = X_{rabbit}(t) - E\left|JX_{rabbit}(t) - X(t)\right| \quad 30$$

Supposed that prey has enough energy while and with leapfrog (as called in (Fred Glover 1989)), the levy flight (LF) concept is utilized in the HHO algorithm. This is the zigzag mechanism used by prey (Rebait) for escaping. Hawk will respectively dive accordingly to the LF parameter using Eq. (31) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002):

$$Z = Y + S \times LF(D) \tag{31}$$

Where D is the dimension of the problem, S is a random vector by size one × D, and LF is the levy flight function, which is calculated using Eq. (32) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002):

$$LF(x) = 0.01 \times \frac{u \times \sigma}{|v|^{\frac{1}{\beta}}}, \sigma = \left(\frac{\Gamma(1+\beta) \times sin(\frac{\pi\beta}{2})}{\Gamma(\frac{1+\beta}{2}) \times \beta \times 2^{(\frac{\beta-1}{2})})} \right)^{\frac{1}{\beta}} \tag{32}$$

Where u and v are random values inside (0, 1), β is a default constant set to 1.5. The position of Hawk will be updated based on Eq. (33), while the value of Y and Z is obtained by Eq. (30, 31). Soft besiege with progressive raped dives is illustrated in Figure (4) (Chai and Draxler 2014; Chervyakov, Lyakhov, and Nagornov 2020; Du et al. 2020; Mantin and Shamir 2002).

$$X(t+1) = \begin{cases} Y & ifF(Y) < F(X(t)) \\ Z & ifF(Z) < F(X(t)) \end{cases} \tag{33}$$

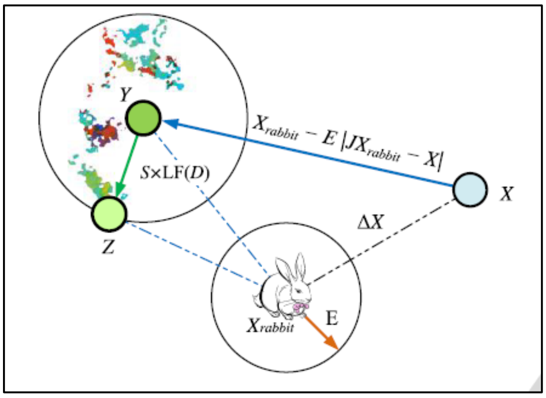


Figure 4 Example of Soft besiege with progressive reaped dives

5.3.4 Hard besiege with progressive rapid dives

It is considered as Hard besiege with Progressive rapid dives while |E| < 0.5 and r<0.5, so the next position of Hawk will be predicted by Eq. (34), which is slid similarly to soft besiege progressive rapid dived but using Xm as Eq. (35) (Bao, Jia, and Lang 2019; Du et al. 2020; A. A. Heidari et al. 2019; Jia et al. 2020).

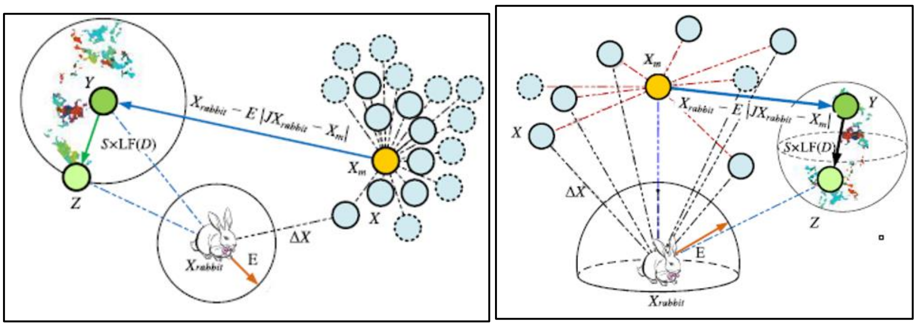
$$X(t+1) = \begin{cases} Y & ifF(Y) < F(X(t)) \\ Z & ifF(Z) < F(X(t)) \end{cases} \tag{34}$$

Where Y and Z obtain from Eq. (35, 36)

$$Y = X_{rabbit}(t) - E\,|JX_{rabbit}(t) - X_m(t)| \tag{35}$$

$$Z = Y + S \times LF(D) \tag{36}$$

Where Xm is from Eq. (25) illustration of this case from Figure (5).


Y
$S \times \mathrm{LF}(D)$
Z
$X_{rabbit} - E\,|JX_{rabbit} - X_m|$
X_m
X
ΔX
X_{rabbit}
E
X_m
$X_{rabbit} - E\,|JX_{rabbit} - X_m|$
Y
X
ΔX
$S \times \mathrm{LF}(D)$
Z
E
X_{rabbit}

(a) (b)

Figure 5 Hard besiege with progressive rapid dives; (a) the process in 2D space; (3) the process in 3D spaces

6. USING HHO FOR STEGANOGRAPHY

Steganography, one of the security system approaches, can use the Modified HHO algorithm to determine where the cover picture should be placed to hide the cipher message and cause a minor distortion. The modified HHO method emphasizes breaking the cover picture into smaller sections (Blocks of pixels). These are applied on each portion (Block) to choose the optimal location among nine matrix pixels (3 pixels * 3 pixels) by reading the pixel's red finesse value and comparing it to the red fitness values of the other 9 pixels in the same section (Block) using the Eq. (37) (Modified HHO Equation):

$$\min \quad R(r)\ \in P(i,j,0)\ [Where\ i < 3\ \&\ j < 3] \tag{37}$$

The Modified HHO equation is used as a function (F24) in Flowchart 1 to identify the ideal Red color pixel. The embedding procedure involves selecting the optimal Red value for a hidden ciphered message and replacing the LSB of the Blue color value for the same pixel with a bit of the ciphered message from the encoding process that has to be communicated. This procedure will be repeated until the ciphered message has been encoded into the cover image to generate a stego image. As shown in Figure (6).

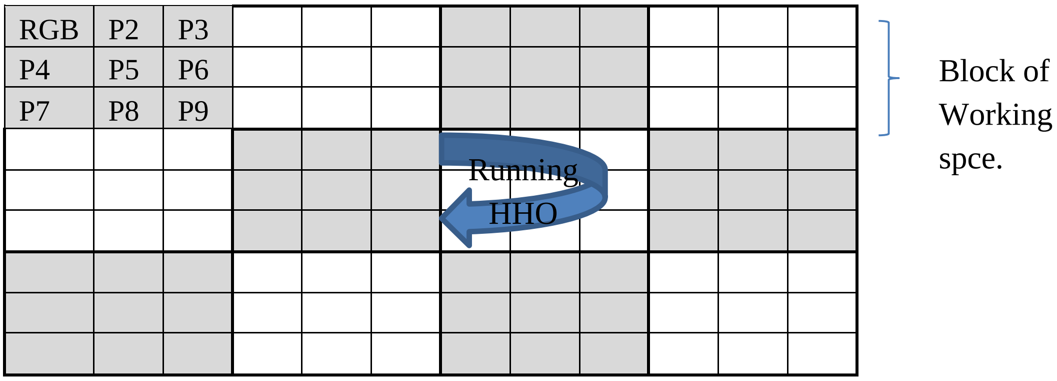
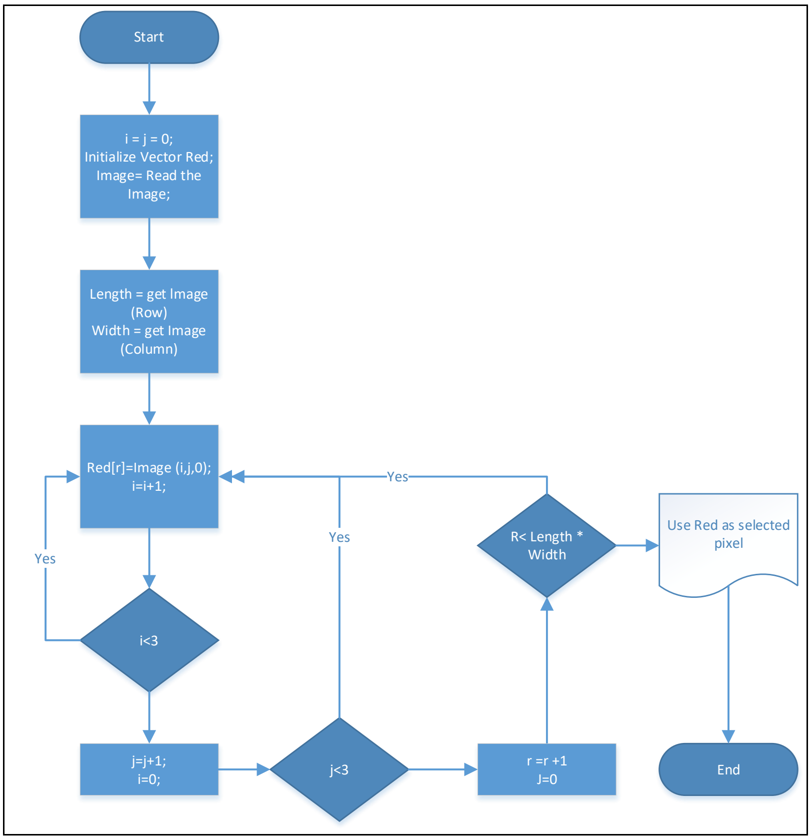


Figure 6 Image Clustering and HHO running

The sender (user) dynamically inputs the encrypted cipher key and message, with the cipher key encoded in the cover picture; the cipher text is then inserted; the recipient will use the same procedures to decipher the stego image. To minimize overlap and improve efficiency, the distribution of the Hawks on each pixel (Hawks position) of the components (Block) on the cover image or image is not simply determined at startup.



Flowchart 1 F24, used to find the best Red position in the Picture pixels

After the plaintext has been encrypted using RC4, the modified HHO (F24) process is executed inside the HHO algorithm (Flowchart 2) as a simple method that scans the picture based on the Hawk distribution on sections (Blocks) that recover efficient pixels in each 9 pixels matrix (3 X 3). As the user will dynamically input the RC4 key beside the plane text to the cover image, hiding will be based on converting the encrypted by security RC4 algorithm text to binary and hiding each bit in the blue color pixel part of (RGB). For instance, assume the plan text is "Hi," the encryption will be in binary as "10001001111001", and each bit will be saved in a founded pixel on the Blue part.

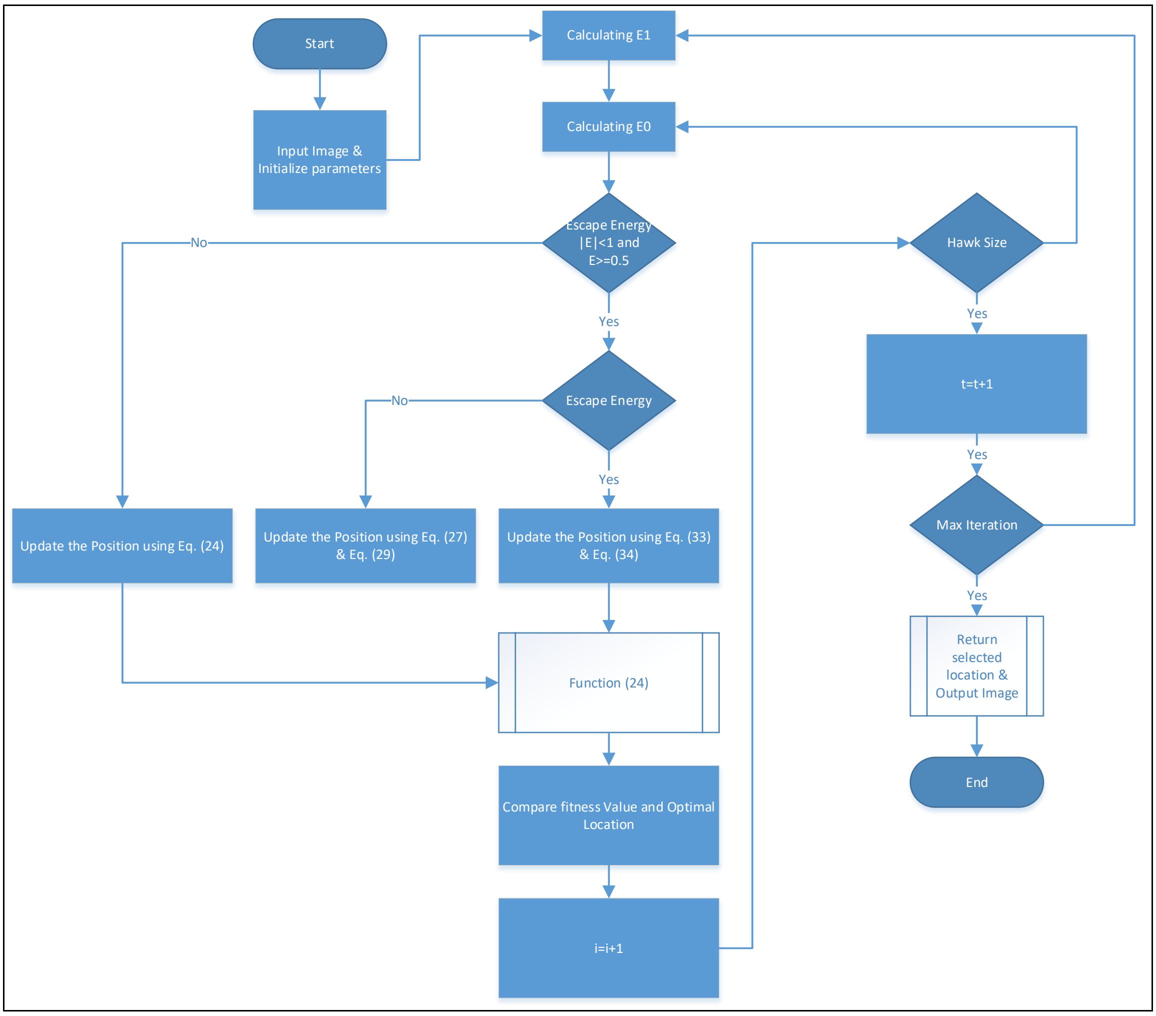
Plain Text	
H	i

Decoded binary from RC4													
1	0	0	0	1	0	0	1	1	1	1	0	0	1

"1" will replace the last digit of the first Block of (Figure 6) and may be the Blue part of P8:

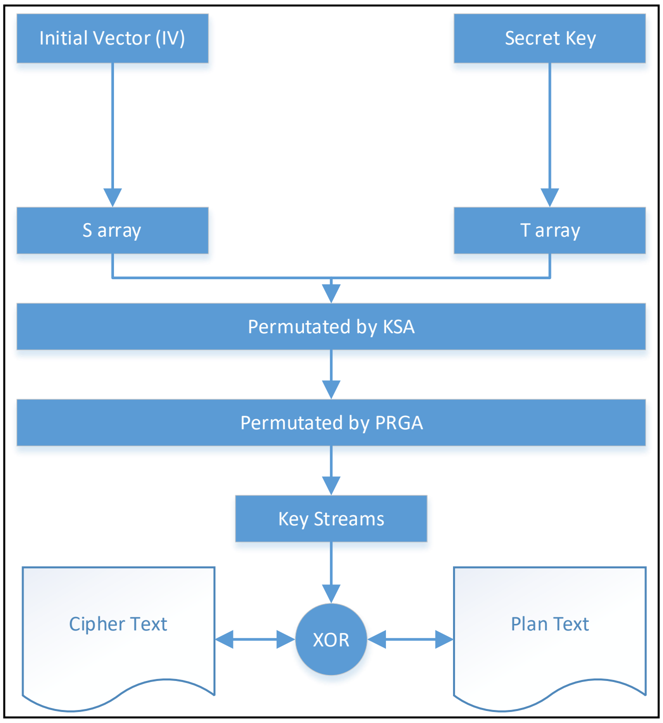
Pixel (P8) before being replaced by encrypted data "1."																							
Red								Green								Blue							
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	0	1	0	0	0	1	0	1	0

Pixel (P8) after being replaced by encrypted data "1."																							
Red								Green								Blue							
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	0	1	0	0	0	1	0	1	1

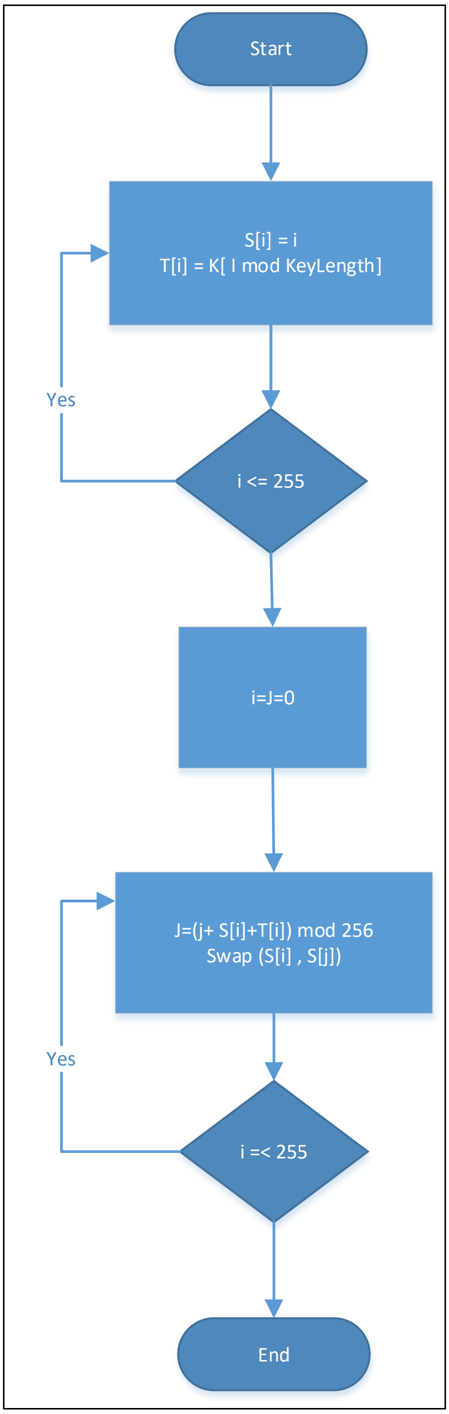

Start
Input Image & Initialize parameters
Calculating E1
Calculating E0
Escape Energy |E|<1 and E>=0.5
No
Yes
Escape Energy
No
Yes
Update the Position using Eq. (24)
Update the Position using Eq. (27) & Eq. (29)
Update the Position using Eq. (33) & Eq. (34)
Function (24)
Compare fitness Value and Optimal Location
i=i+1
Hawk Size
Yes
t=t+1
Yes
Max Iteration
Yes
Return selected location & Output Image
End

Flowchart 2 HHO Procedure calling F24 using Swarm intelligence

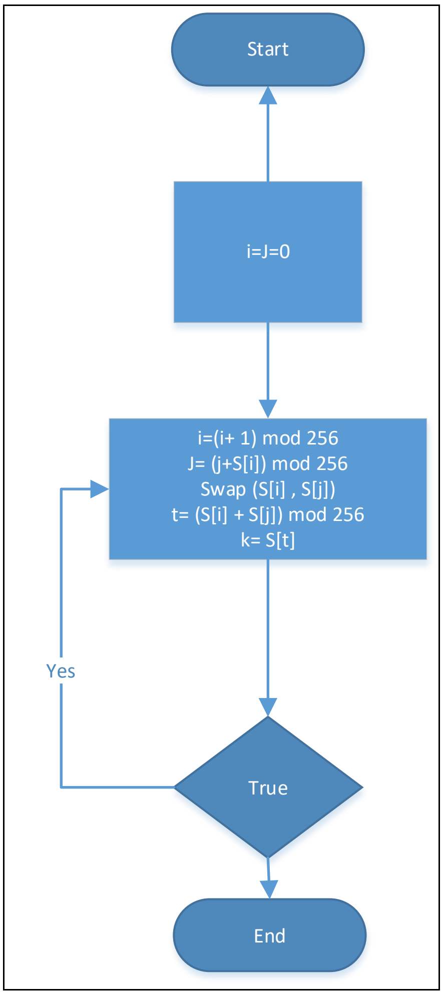
RC4 procedure has two input Initial vectors and a Sector key to generate another two arrays, S, T which will be used as input for the key Scheduling Algorithm (KSA) as clarified in (flowchart 4), and Pseudo Random number Generation Algorithm (PRGA) as described in (flowchart 5). This key stream will be ready for Encryption and Decryption, which, to address the RC4 key problem, is dynamically placed at the beginning of the stego image using a modified HHO algorithm.



Flowchart 3 RC4 Main Procedure



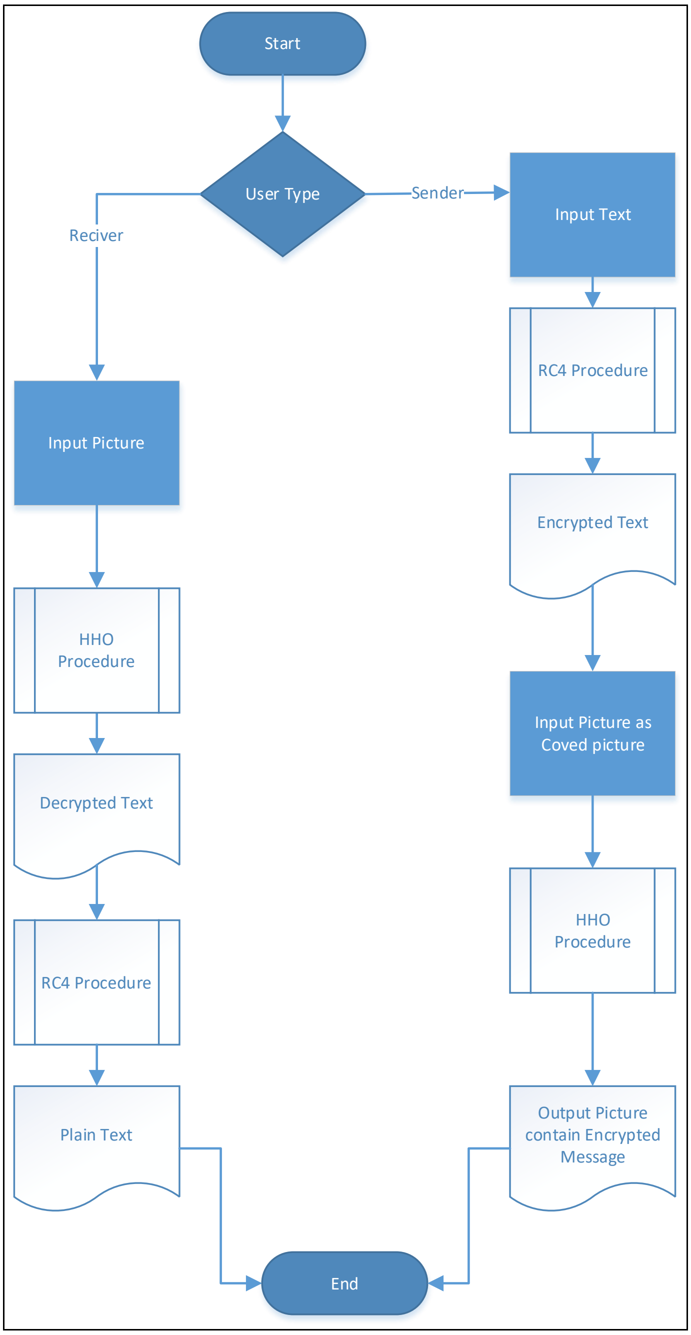
Flowchart 4 (PRGA) Pseudo Random Number Generation Algorithm



Flowchart 5 (KSA) Key Scheduling Algorithm

By combining Modified HHO (F24) and RC4 in the main procedure to embed and hide encrypted messages as described in (Flowchart 6) if the user:

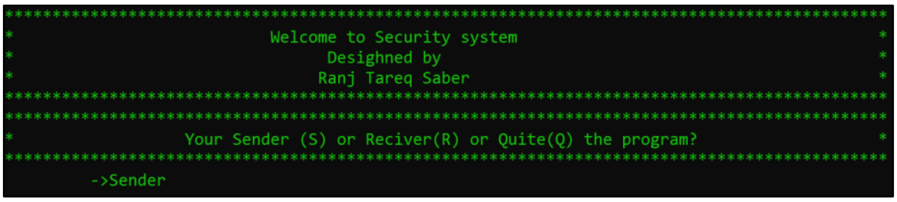
1. Is the Sender,
   a. Application asking for inputting cipher Key and message. Then, the RC4 algorithm will be applied to cipher the message.
   b. In the second step, the Application prompts the user to select the cover image.
   c. Application will generate stego image by applying Modified HHO procedure on cover image specified in step (1. b) and cipher message in step (1. a).
2. Is the Receiver,
   a. Application asks the user to select the Stego image.
   b. Modified HHO procedure will extract the cipher message and the key.
   c. In the last stage, RC4 will extract the message (plain text) from the cipher message.



Flowchart 6 Main Flowchart of Enhancement Steganography by using HHO and RC4

7. RESULTS

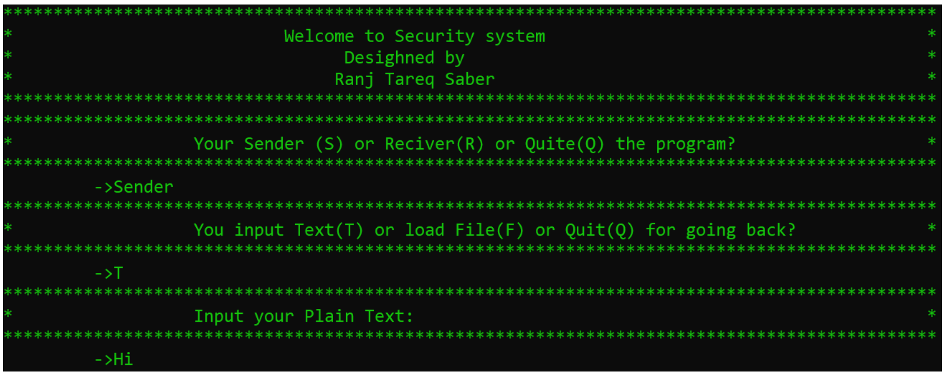
In the following processes, we will examine how the Application communicates with the user by demonstrating how the Modified HHO (F24) algorithm and the RC4 Algorithm are used. In the first stage of this process, the program ascertains whether the user is the message's sender or its reviser by analyzing the stego image, as demonstrated in (Figure 7).



```
*********************************************************************************************
*                           Welcome to Security system                                      *
*                                 Desighned by                                              *
*                                Ranj Tareq Saber                                           *
*********************************************************************************************
*********************************************************************************************
*                  Your Sender (S) or Reciver(R) or Quite(Q) the program?                   *
*********************************************************************************************
         ->Sender
```

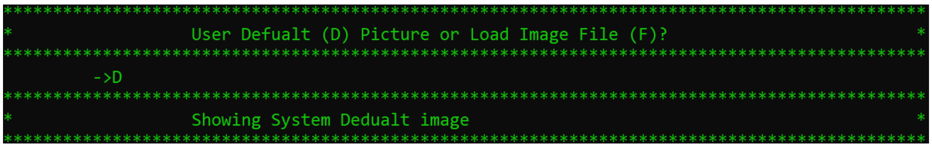
Figure 7 Main Menu

Once the Sender Option App has been chosen, the recipient will be prompted to enter the message they want to receive as an encrypted picture (Figure 8). Once the text has been entered, the system will prompt the user to choose an accompanying image, as seen in (Figure 9).



```
*********************************************************************************************
*                            Welcome to Security system                                     *
*                                  Desighned by                                             *
*                                 Ranj Tareq Saber                                          *
*********************************************************************************************
*********************************************************************************************
*                  Your Sender (S) or Reciver(R) or Quite(Q) the program?                   *
*********************************************************************************************
         ->Sender
*********************************************************************************************
*                  You input Text(T) or load File(F) or Quit(Q) for going back?             *
*********************************************************************************************
         ->T
*********************************************************************************************
*                  Input your Plain Text:                                                   *
*********************************************************************************************
         ->Hi
```

Figure 8 Input Text



```
*********************************************************************************************
*                  User Defualt (D) Picture or Load Image File (F)?                         *
*********************************************************************************************
         ->D
*********************************************************************************************
*                  Showing System Dedualt image                                             *
*********************************************************************************************
```

Figure 9 Selecting the Cover image

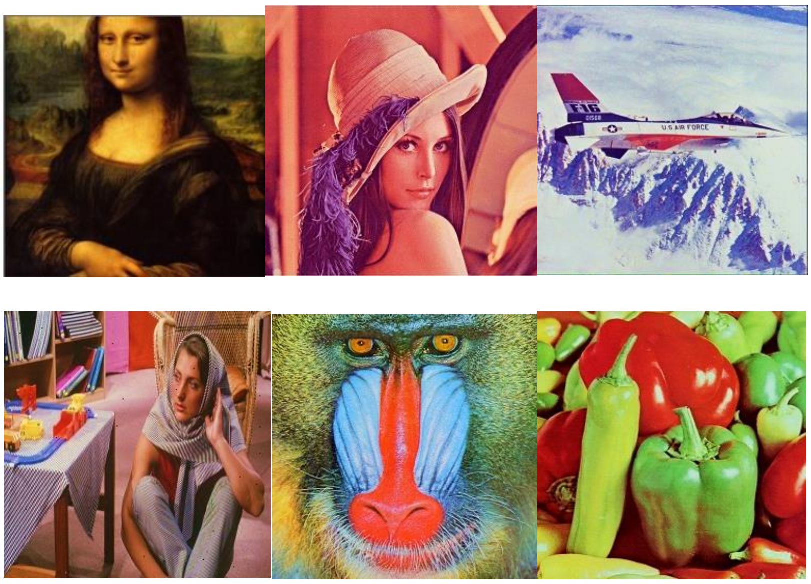
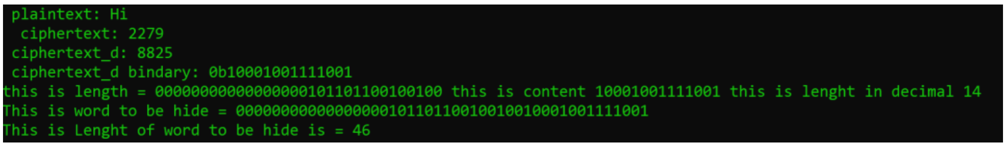


Figure 10 Cover picture (a) Monaliza, (b) Lena, (c) Airplane, (d) Barbara, (e) Baboon and (f) Pepper

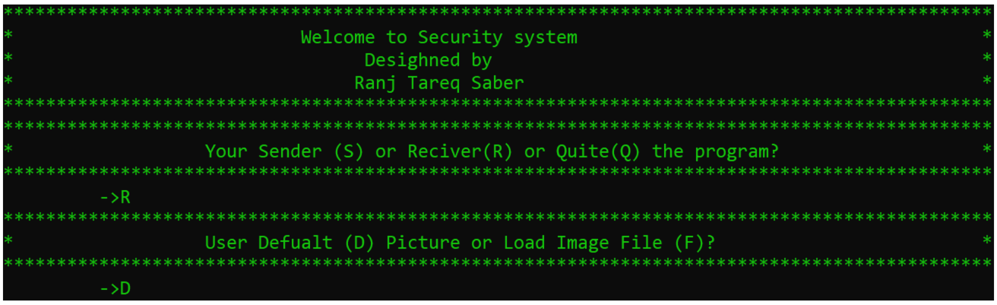
The message will be encrypted before being concealed (Figure 11).



```
 plaintext: Hi
  ciphertext: 2279
 ciphertext_d: 8825
 ciphertext_d bindary: 0b10001001111001
this is length = 00000000000000000101101100100100 this is content 10001001111001 this is lenght in decimal 14
This is word to be hide = 0000000000000000010110110010010010001001111001
This is Lenght of word to be hide is = 46
```

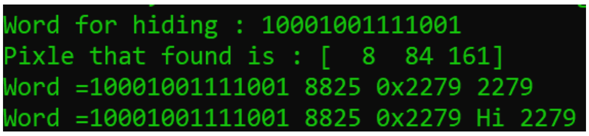
Figure 11 Plain Text Conversion to Binary

The receiver can then get the encrypted data from the stego image by selecting the stego image using the receiver option (Figure 12). The obtained information will be shown in (Figure 13).



```
*********************************************************************************************
*                          Welcome to Security system                                       *
*                                Designhed by                                               *
*                               Ranj Tareq Saber                                            *
*********************************************************************************************
*********************************************************************************************
*                 Your Sender (S) or Reciver(R) or Quite(Q) the program?                    *
*********************************************************************************************
         ->R
*********************************************************************************************
*                 User Defualt (D) Picture or Load Image File (F)?                          *
*********************************************************************************************
         ->D
```

Figure 12 Receiver Option

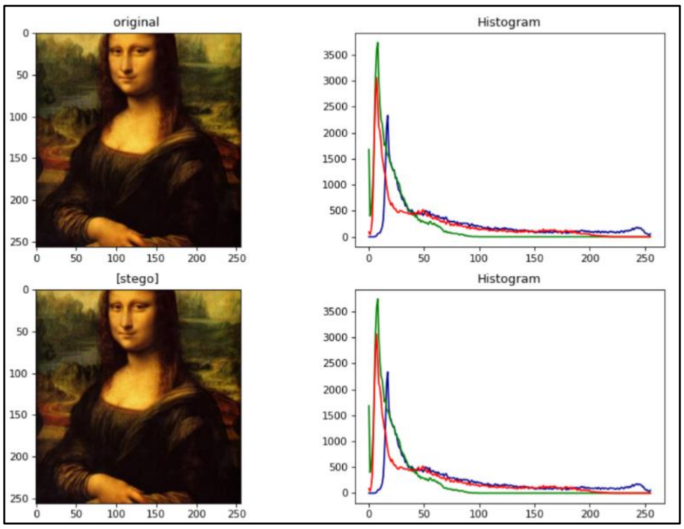


```
Word for hiding : 10001001111001
Pixle that found is : [  8  84 161]
Word =10001001111001 8825 0x2279 2279
Word =10001001111001 8825 0x2279 Hi 2279
```

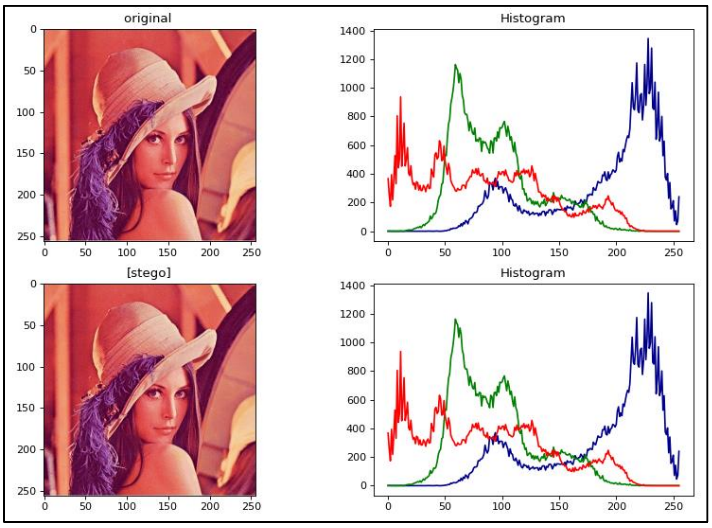
Figure 13 Retrieved data

8. DISCUSSION

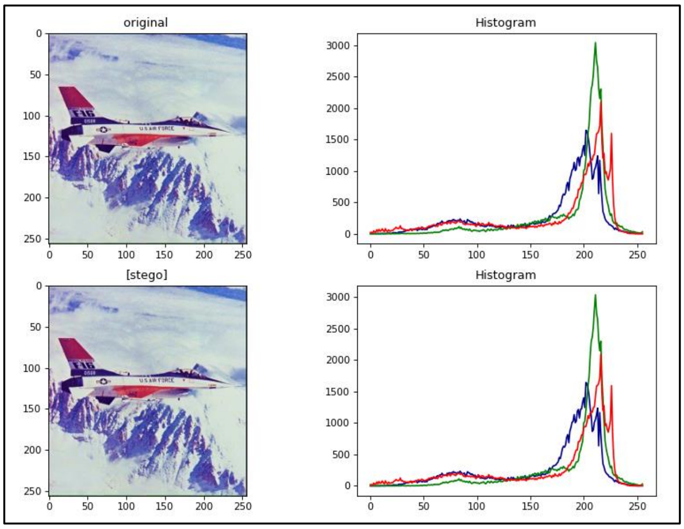
The measurable Quality image KPIs help to compare the original cover art to the stenographical version. The histograms of color distribution in both images are identical, as can be seen in (Figure 14). The Stego image's histogram is another quality tool for comparing it to the original. The histogram graph shows pixel intensity frequency, with the x-axis representing gray level intensities and the y-axis frequency. Comparing histogram graphs of two photos can determine if they match (Nagy 2020). In this study, the affected histogram is the Blue color of the selected bit by the modified HHO algorithm.



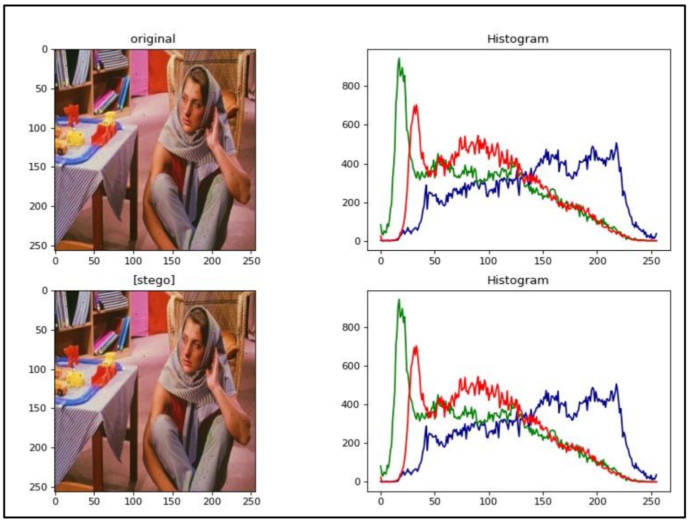
(a)Monaliza



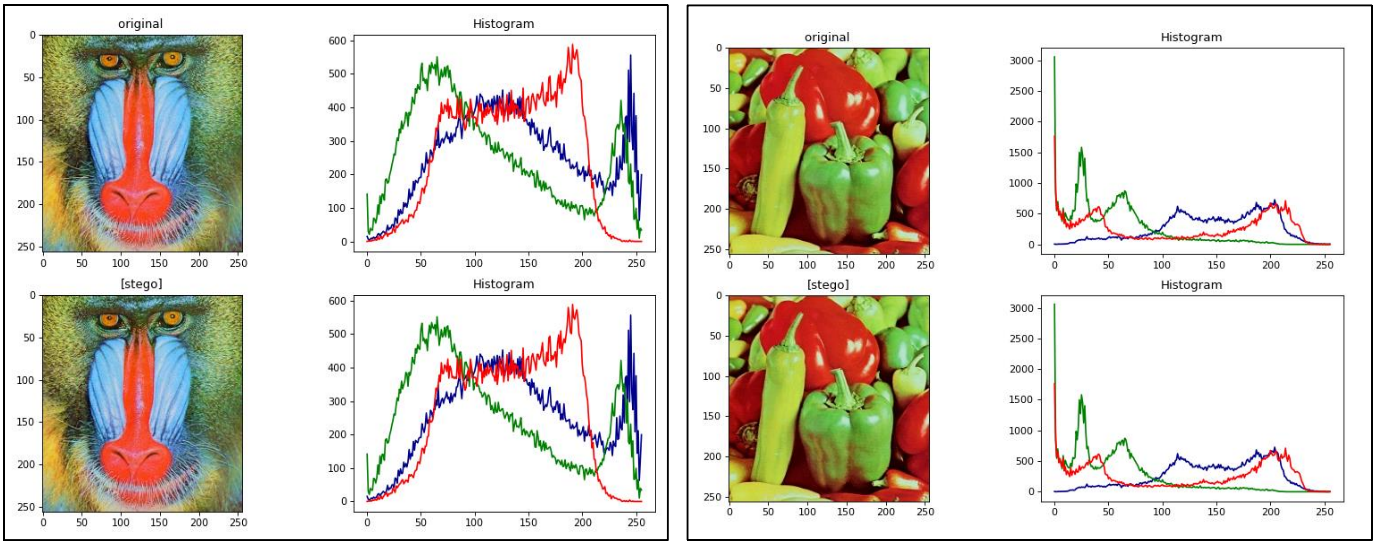
(b) Len



(c) Airplane



(d) Barbara

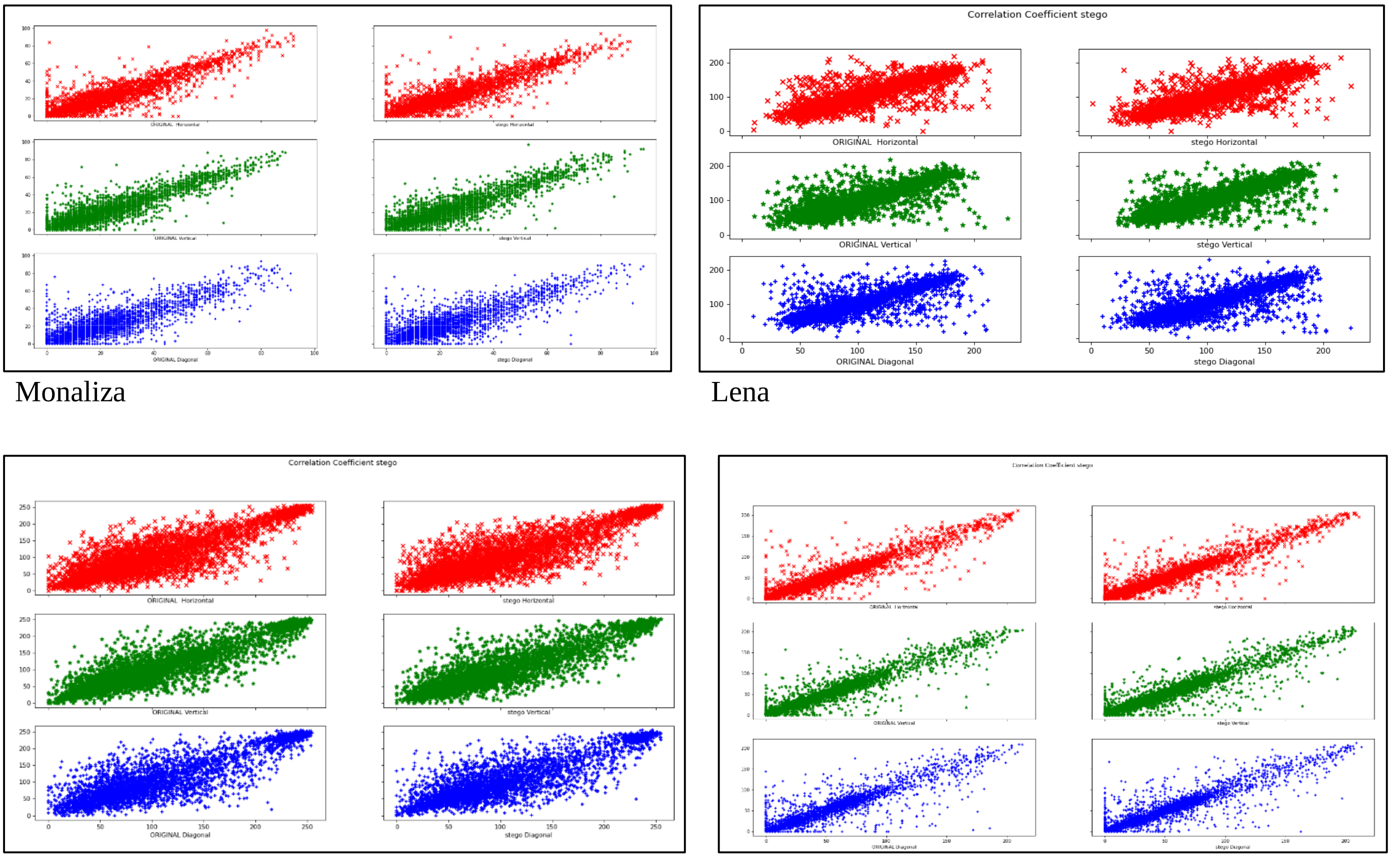


(e) Baboon

(f) Pepper

Figure 14 Histogram of Original cover and Stego image.

Additionally, both images' (original cover and Stego one) correlation coefficient (CC) has only slightly changed since CC is a statistical measure of the cover picture and Stego pixels; its typical values are -1 to 1 after the removal of calculation errors (Jia et al. 2020). As can be observed in (Figure 15), a slight alteration in the blue color values of the pixel is principally brought on by a change in the LSB of the pixel's blue color caused by Modified HHO.

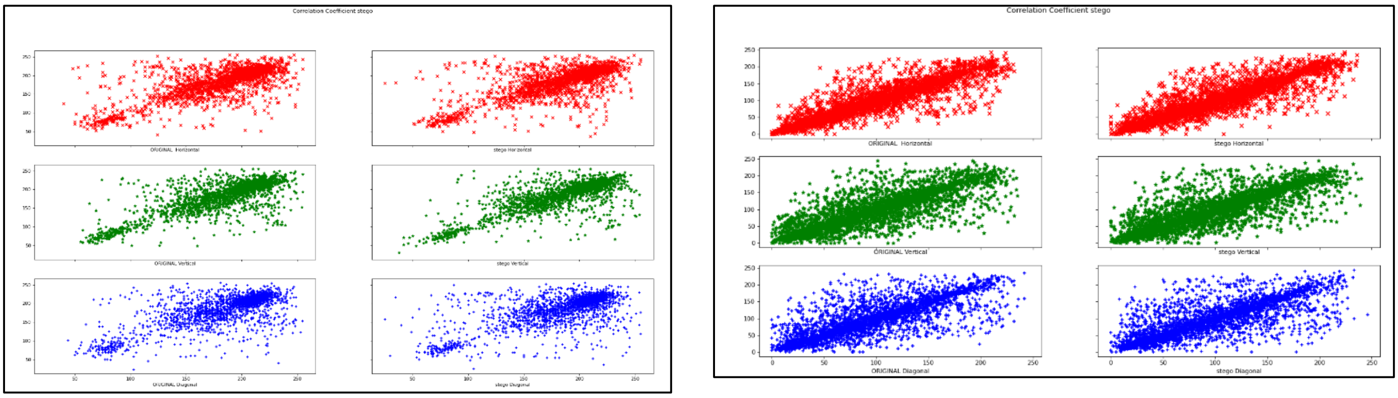


Monaliza

Lena

Airplane

Barbara



Baboon

Pepper

Figure 15 Correlation coefficient of original cover and stego image.

Additional image quality (Table 1) lists the key performance indicators (KPI) for distortion, with the threshold value underlined in the final column. As highlighted in red, RMSE, UACI, and SMA have not achieved the required threshold.

Figure (16) shows image quality KPIs for (CC, MS-SSIM, SCC, SSIM, UQI, and VIF) achieved 1, a required threshold value for these KPIs.

Figure (17) shows BER as 1%, except the Pepper image achieved 0.8%, which, as small as possible, is the most desirable value for BER KPI.

Figure (18) SNR value is different from 7K to 17K, which is more significant than 40, an acceptable SNR value.

Figure (19) image quality for (HD, PSNR, and SE) also achieved the required KPI image quality threshold.

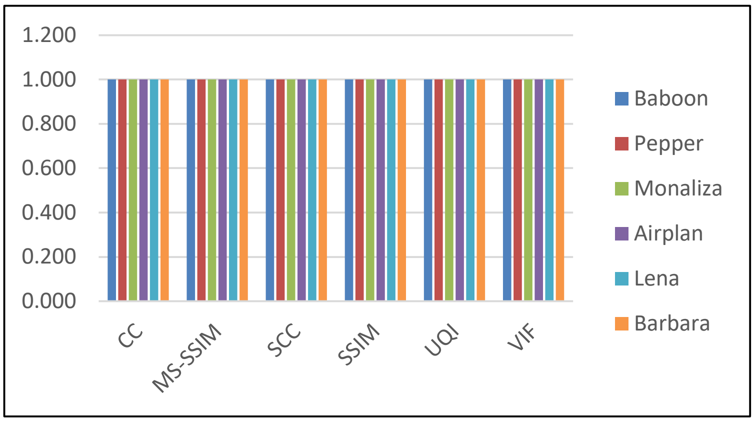


Figure 18 Image Quality (CC , MS-SSIM, SCC, SSIM, UQI, VIF)

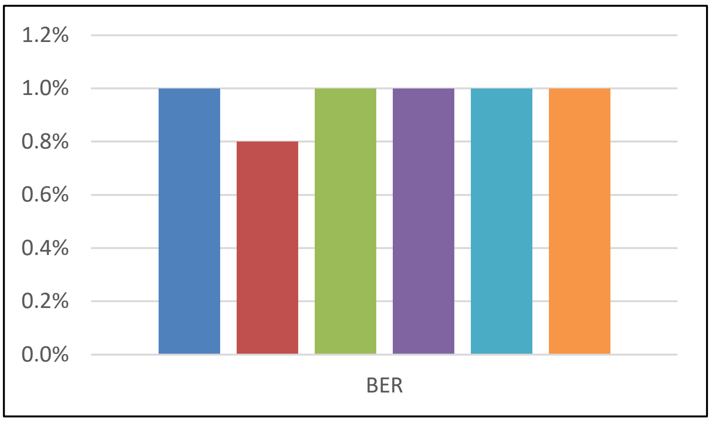


Figure 19 Image Quality (BER)

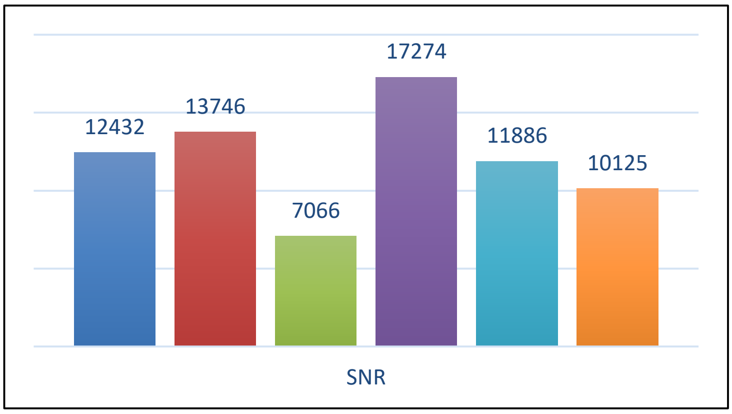


Figure 17 Image Quality (SNR)

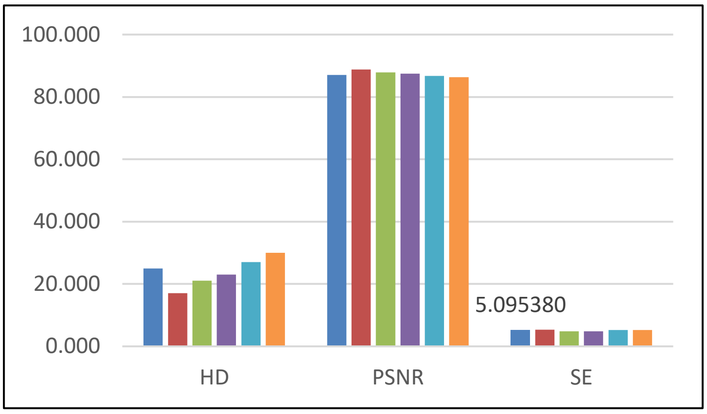


Figure 16 Image Quality (HD, PSNR,SE)

Table 1. Distortion KPI Value.

KPI Name	Monaliza KPI Value	Lena KPI Value	Airplane KPI Value	Baebaea KPI Value	Baboon KPI Value	Pepper KPI Value	Threshold Value
MSE	1.0678219483174177E-4	1.3729139335509657E-4	1.1695192767286004E-4	1.5254599261677396E-4	1.271216605139783E-4	8.644272914950524E-5	0 (model is perfect)
RMSE	1.0334966058846057-2	0.01171875	0.010815916488174577	0.012352647110032733	0.011276372445109888	0.009298734932998503	0.2 and 0.5
PSNR	87.84581517641413	86.75437048216345	87.4507297635774	86.2967955765567	87.08860803703296	88.76351890997059	60 dB or higher
MAE	0.010333573331994096	0.011717170796188057	0.010814458949055833	0.012350982483054279	0.011274852855533327	0.00929748184733216	0 to ∞
SNR	7065.569329670537	11886.314508399675	17274.29514952907	10125.152127252211	12431.527999405384	13745.547846056748	>40 dB
CC	0.9999999817321101	0.9999999847091187	0.999999759773577	0.9999999779556855	0.9999999821033729	0.9999999915872784	1 to -1
BER	0.010678273780769954 ~ 1%	0.013729209146704226 ~ 1%	0.011695252236081378 ~ 1%	0.015254676829671365 ~ 1%	0.012712230691392802	0.008644316870147106	small as possible
EQ	0.1484375	0.1484375	0.0859375	0.234375	0.1171875	0.1328125	0 to 1
UACI	4.1875370522251676E-5	5.3839762100037866E-5	4.58635010481804E-5	5.9821957888930964E-5	4.9851631574109134E-5	3.389910947039421E-5	33.46%
HD	21.0	27.0	23.0	30.0	25.0	17.0	Near to 24
SE	4.790522889514206	5.212694582890209	4.778454472890404	5.218285871844319	5.0953800196130326	5.274237912205447	>1
SSIM	(0.9999999528861689, 0.9999999528888995)	(0.9999998719419176, 0.9999998719445137)	(0.9999999953893889, 0.9999999953909177)	(0.999999945363459, 0.9999999454124082)	(0.9999999909500099, 0.9999999909621969)	(0.9999999776685798, 0.9999999776709094)	1 (Similar),0,-1
UQI	0.9999999996485104	0.9999999995748093	0.9999999997300305	0.999999995779867	0.9999999983246882	0.9999999997276116	[1 -1]
MS-SSIM	(0.9999999996630775+0j)	(0.9999999988615368+0j)	(0.999999999892485+0j)	(0.9999999996063318+0j)	(0.9999999999291549+0j)	(0.9999999997955609+0j)	1 (Similar),0,-1
ERGAS	0.10158723659463458	0.15378603293689838	0.0392188984448795	0.22533552488520736	0.14580628994511502	0.09667954647049949	small as possible
RASE	0.013304030728713794	0.019510972867967536	0.00576586096144637	0.030943837513353452	0.021090380032196307	0.012011926997387495	<3
SAM	5.9207500363108156e-05	3.48313579706255e-05	3.50690628604431e-05	4.619317214943722e-05	4.3196803761148287e-05	3.4408786761805654e-05	Near to 1.
VIF	0.9999998027473311	0.9999996294051586	0.9999999162786789	0.9999997760683743	0.9999997729651723	0.9999998742133341	1 to 0

9. CONCLUSIONS

While CIA (Confidentiality, Integrity, and Availability) is the most vital metric to consider when developing a security system, the performance with which the system responds is equally essential. Therefore, Modified Harry Hawk Optimization (F24) was used for this study to locate the optimal position for hiding encrypted text using the RC4 algorithm. This was accomplished by partitioning the workplace into smaller blocks (parts), which improved the algorithm's performance (in terms of time and CPU cycle cost) during the embedding process, whereby the key will be constantly adjusted and updated in the receiver section of the stego image to circumvent the security flaws in the RC4 stream cipher technique, the primary benefit of which is its speed. Image quality KPI evaluators show that comparing the Cover image with the Original and Stego images achieved the best KPI. Besides, time for plan text retrieval from encrypted text is acceptable, less than 6 Sec per character. Using the LSB part of the blue color of the pixel while searching for position based on the red color value improved the change on the cover image to have minimal distortion compared to other works (Hameed, Abdel-Aleem, and Hassaballah 2023),(Abduljaleel et al. 2022). Both caused more distortion on the stego image by hiding the message in all colors (Red, Green, and Blue) of the cover image and consuming more time for searching but with better capacity to hide information.

REFERENCES

abd ulkareem, Maysaa, and Iman Qays Abduljaleel. “Analysis of a Modified on Rivets Cipher (RC4) Algorithn by Chaotic Algorithm.” : 473–84.

Abdel-Salam Nasr, M., Mohammed F. AlRahmawy, and A. S. Tolba. 2017. “Multi-Scale Structural Similarity Index for Motion Detection.” *Journal of King Saud University - Computer and Information Sciences* 29(3): 399–409. http://dx.doi.org/10.1016/j.jksuci.2016.02.004.

ABDULHAMMED, OMAR YOUNIS. 2022. “A Robust Image Steganography Based on a Novel Technique by Using Improved DNA and Chaotic Approach.” *The Greeks and the New*: 11–35.

Abduljaleel, Iman Qays et al. 2022. “A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques.” *Journal of Sensor and Actuator Networks* 11(4).

Alparone, Luciano et al. 2008. “Multispectral and Panchromatic Data Fusion Assessment without Reference.” *Photogrammetric Engineering and Remote Sensing* 74(2): 193–200.

Aniba, G., and S. Aïssa. 2009. “BER Evaluation for General QAM in Nakagami-m Fading Channels.” *Electronics Letters* 45(6): 319–21.

Bao, Xiaoli, Heming Jia, and Chunbo Lang. 2019. “A Novel Hybrid Harris Hawks Optimization for Color Image Multilevel Thresholding Segmentation.” *IEEE Access* 7(June): 76529–46.

Bedi, Punam, Roli Bansal, and Priti Sehgal. 2011. “Using PSO in Image Hiding Scheme Based on LSB Substitution.” *Communications in Computer and Information Science* 192 CCIS(PART 3): 259–68.

De Carvalho, O.A, and P.R. Meneses. 2000. “Spectral Correlation Mapper (SCM): An Improvement on the Spectral Angle Mapper (SAM). In: Summaries of the 9th JPL Airborne Earth Science Workshop.” *Summaries of the 9th JPL Airborne Earth Science Workshop, JPL Publication 00-18* 9(equation 2).

Chai, T., and R. R. Draxler. 2014. “Root Mean Square Error (RMSE) or Mean Absolute Error (MAE)? - Arguments against Avoiding RMSE in the Literature.” *Geoscientific Model Development* 7(3): 1247–50.

Chervyakov, Nikolay, Pavel Lyakhov, and Nikolay Nagornov. 2020. “Analysis of the Quantization Noise in Discrete Wavelet Transform Filters for 3D Medical Imaging.” *Applied Sciences (Switzerland)* 10(4).

Du, Pei et al. 2020. “A Novel Hybrid Model Based on Multi-Objective Harris Hawks Optimization Algorithm for Daily PM2.5 and PM10 Forecasting.” *Applied Soft Computing Journal* 96: 1–24.

Evsutin, Oleg, Anna Melman, Roman Meshcheryakov, and Senior Member. 2020. “Digital Steganography and Watermarking for Digital Images : A Review of Current Research Directions." 8: 166589–611.

Féraud, Jean-Francois. 2017. "Image Quality Assessment: From Error Visibility to Structural Similarity." *Dictionaire critique de la langue française* 13(4): 506–75.

Fluhrer, Scott, Itsik Mantin, and Adi Shamir. 2001. "Weaknesses in the Key Scheduling Algorithm of RC4\rSelected Areas in Cryptography." *Springer* 2259: 1–24. https://link.springer.com/chapter/10.1007/3-540-45537-X_1%0Ahttp://dx.doi.org/10.1007/3-540-45537-X_1.

Fluhrer, Scott R., and David A. McGrew. 2001. "Statistical Analysis of the Alleged RC4 Keystream Generator." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 1978: 19–30.

Fred Glover. 1989. "Tabu Search - Part I." *Orsa Journal on Computing* 1(3): 190–206.

Hameed, Mohamed Abdel, Omar A. Abdel-Aleem, and M. Hassaballah. 2023. "A Secure Data Hiding Approach Based on Least-Significant-Bit and Nature-Inspired Optimization Techniques." *Journal of Ambient Intelligence and Humanized Computing* 14(5): 4639–57. https://doi.org/10.1007/s12652-022-04366-y.

Heidari, Ali Asghar et al. 2019. "Harris Hawks Optimization: Algorithm and Applications." *Future Generation Computer Systems* 97(March): 849–72.

Heidari, Shahrokh et al. 2017. "Quantum Red-Green-Blue Image Steganography." *International Journal of Quantum Information* 15(5).

Helmy, Mai, El Sayed M. El-Rabaie, Ibrahim M. Eldokany, and Fathi E.Abd El-Samie. 2017. "3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm." *3D Research* 8(4). https://doi.org/10.1007/s13319-017-0145-8.

Jia, Heming et al. 2020. "Pulse Coupled Neural Network Based on Harris Hawks Optimization Algorithm for Image Segmentation." *Multimedia Tools and Applications* 79(37–38): 28369–92.

Knudsen, Lars R, Willi Meier, Bart Preneel, and Vincent Rijmen. 1998. "Analysis Methods for (Alleged) RC4." : 327–41.

Li, Shutao. 2006. "Fusion of Multi-Spectral and Panchromatic Images by Complex Steerable Pyramids." *Advances in Modelling and Analysis B* 49(1–2): 13–21.

Mahmoudpour, Saeed, and Manbae Kim. 2015. Emerging Trends in Image Processing, Computer Vision and Pattern Recognition *A Study on the Relationship between Depth Map Quality and Stereoscopic Image Quality Using Upsampled Depth Maps*. Elsevier Inc. http://dx.doi.org/10.1016/B978-0-12-802045-6.00010-7.

Mantin, Itsik, and Adi Shamir. 2002. "A Practical Attack on Broadcast RC4." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 2355: 152–64.

Matalgah, Mustafa M. 2018. "Error Performance of Cryptography Transmission in Wireless Fading Channels." *IEEE Vehicular Technology Conference* 2018-Augus(August 2018).

McGee, Kiaran P. et al. 2000. "Image Metric-Based Correction (Autocorrection) of Motion Effects: Analysis of Image Metrics." *Journal of Magnetic Resonance Imaging* 11(2): 174–81.

Nagy, Marius. 2020. "Quantum Steganography by Harnessing Entanglement as a Degree of Freedom." 8: 213671–81.

Nickfarjam, A. M., and Z. Azimifar. 2012. "Image Steganography Based on Pixel Ranking and Particle Swarm Optimization." *AISP 2012 - 16th CSI International Symposium on Artificial Intelligence and Signal Processing* (Aisp): 360–63.

Pan, B. 2011. "Recent Progress in Digital Image Correlation." *Experimental Mechanics* 51(7): 1223–35.

Patil, Priyadarshini, Prashant Narayankar, D. G. Narayan, and S. M. Meena. 2016. "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish." *Procedia Computer Science* 78(December 2015): 617–24. http://dx.doi.org/10.1016/j.procs.2016.02.108.

Rao, N.V., and S.N.N. Pandit. 2011. "Computational Image Quality Metrics for Watermarking Applications." *CVR Journal of Science and Technology* 1(1): 1–7.

Sara, Umme, Morium Akter, and Mohammad Shorif Uddin. 2019. "Image Quality Assessment through

FSIM, SSIM, MSE and PSNR—A Comparative Study.” *Journal of Computer and Communications* 07(03): 8–18.

Sheikh, Hamid Rahim, and Alan C. Bovik. 2006. “Image Information and Visual Quality.” *IEEE Transactions on Image Processing* 15(2): 430–44.

Stallings, William. 2017. *Cryptography and Network Security : Principles and Practice*.

Wald, Lucien. 2000. “Quality of High Resolution Synthesised Images: Is There a Simple Criterion ?” *Third conference “Fusion of Earth data: merging point measurements, raster maps and remotely sensed images”*: 99–103.

Yim, Changhoon, and Alan Conrad Bovik. 2011. “Quality Assessment of Deblocked Images.” *IEEE Transactions on Image Processing* 20(1): 88–98.

Yuhas, RH, Alexander F H Goetz, and Joe W Boardman. 1992. “Descrimination among Semi-Arid Landscape Endmembers Using the Spectral Angle Mapper (SAM) Algorithm.” *Summaries of the Third Annual JPL Airborne Geoscience Workshop, JPL Publ. 92–14, Vol. 1*: 147–49.

PROFILE OF THE AUTHORS

Ranj Tareq Saber: Ph.D. Student working on Swarm Intelligence & Security Algorithm enhancement, Upon entering university, pursued a degree in Software Engineering at 2004, delving into the vast landscape of algorithms and machine learning. The spark of passion for artificial intelligence and face recognition with neural network was ignited during undergraduate studies, after getting MSC in Computer Sience in 2009 leading to explore diverse facets of the field.