Improving Image Steganography using a Proposed Mutated Levy-Flight Firefly Algorithm

Wafaa Hanna Zaki Sharaby
Departments of Management Information
Systems and Computer Science,
Higher Future Institute for Specialized Technological Studies,
Future Academy,
Cairo, Egypt

ABSTRACT

Today's data transmission over an unsecure channel has increased widely. There is a crucial need to some security measures to transmit our data securely. Steganography is an art of "invisible" communication. In steganography the secret message is concealed inside other media cover such as text, image, video and audio form. Firefly Algorithm (FA), metaheuristic algorithm has been used for solving various optimization problems. In this study, Levy flight firefly algorithm (LFA) is employed to solve the problem of 24-bit color image steganography. In the proposed approach, firefly algorithm is initialized with a population of fireflies which will carry each secret byte in the form of different patterns based on rotated reversed method to improve the search process and enhance the security issue. During the iterations, the pattern of the more attractive (brighter) firefly j is donated to the attracted (less bright) firefly i to improve its quality. The optimal carrier pixels are located by the brightest fireflies and are embedded with those rotated reversed secret bytes using 3-3-2 LSB replacement technique. The experimental results showed the efficiency of the proposed approach in terms of MSE and PSNR in decibels (dB) values.

General Terms

Security, Optimization Algorithms.

Keywords

Steganography, Cover-image, Steg-image, Pattern, LSB, Firefly Algorithm.

1. INTRODUCTION

Nowadays a lot of communication occurs through the Internet. Secret information prone to eavesdropping from hackers. To protect secret information, cryptography and steganography are both used to ensure data confidentiality. However, the main difference between them is that with cryptography, a third party can see that both parties are communicating in secret and the encrypted message can be noticed easily [1]. While steganography is the art and science of invisible communication [2]. Steganography is derived from two Greek words “stegos” and “grafia”. “stegos” means hidden and “grafia” means writing i.e. Steganography means “hidden writing” [2], [3]. In steganography the secret message is concealed inside other digital cover media such as Text, Image, video and audio form [1], [3], [4]. In this paper, 24-bit color image is used as the cover media referred to as "cover image". The cover image with secret message imbedded in it referred to as "Stego-image".

In spatial domain technique, substitution is applied between the bit values of the image pixels used as a carrier and the bit values of secret message. Due to its simplicity, significant computation reduction and its high level of robustness, the spatial domain scheme in image steganography has been widely used [5].

There are two important contradict factors should be taken into consideration in image steganography namely, visual quality and embedding capacity [6]. Visual quality refers to that amount of distortion caused in an image by the concealment process. While embedding capacity refers to the maximum amount of secret information can be concealed into an image. If the embedding capacity is to be maximized, visual quality is minimized and vice versa. However, the ultimate aim is providing a good visual quality of the stego-image without bringing perceptive distortion.

Many methods are proposed for image-based steganography but most significant and efficient method is Least Significant Bit (LSB) which replaces the least significant bits of pixels selected to hide the secret information. [5].

Swarm-intelligence is an artificial intelligence topic, has become increasingly popular during the last decade [7].

Recently, many methods of swarm-intelligence are successfully applied to solve a variety of optimization problems. Ant colony optimization (ACO) [8], Particle swarm optimization (PSO) [9], cuckoo search (CS) [10], firefly algorithm (FA) are notable examples of swarm-intelligence-based methods.

In 2008 X. S. Yang [12] developed the firefly algorithm (FA), stochastic, nature-inspired, meta-heuristic swarm-based optimization algorithm. Recent research illustrated the efficiency of the firefly algorithm as one of the more promising Swarm-intelligence techniques and its superiority over other meta-heuristic algorithms [10], [12]. In 2010 Yang formulated a new version of FA, the Levy-Flight Firefly Algorithm (LFA) [13], which combines levy-flight with search strategy via firefly for improving the randomization of basic FA. Later, in 2013 Sankalap Arora et. al. introduced a mutated firefly algorithm (MFA) which considers mutation probability and then perform mutation on fireflies to better explore search space. The basic principle of MFA is to learn from other fireflies by accepting good features from them and achieve better solution in less amount of time [14].

In this study, the proposed scheme combines the levy flight firefly algorithm with mutation concept as mutated levy flight firefly algorithm (MLFA) to improve the process of 24-bit image steganography utilizing the 3-3-2 LSB replacement technique.

To evaluate the performance of the proposed MLFA algorithm, the PSNR in decibels (dB) is computed between the original cover-image and the resulted stego-image. In order to compute the PSNR, the mean square error (MSE) is first computed. A higher PSNR value means, MSE between the original cover image and the marked image is minimum and the quality of the stego-image is preserved, original cover-image can be reconstructed without any distortion after extracting the embedded secret message [15].

Rest of the paper is organized as follows. In section 2 some selected related works. Section 3 gives a detailed description of the image steganography. Firefly algorithm is illustrated in section 4. The proposed scheme is presented in section 5. Sections 6 and 7 present the experimental results and conclusions.

2. RELATED WORK ON IMAGE STEGANOGRAPHY

A technique that can be used to conceal the secret message into the LSB bits of the cover image and to overcome the level of security issues is proposed in [8]. Ant colony Algorithm (ACO) is adopted to find the optimal LSB substitution matrix. The obtained results showed the efficiency of ACO and the PNSR value of the stego-image goes beyond 35 dB.

Saha et al. introduced a research to adopt the cat swarm optimization (CSO) strategy to obtain the optimal or near optimal solution of the stego-image quality problem. The secret data is concealed into a cover image using simple LSB substitution can degrade the image quality dramatically. The obtained results show that the proposed scheme can obtain a good solution with less computation time [16].

Genetic algorithm (GA) is inspired by the nature and have vast applications in different fields. In [17], a Jpeg steganography method is introduced, which uses the GA to solve the problem image steganography. This method can insert secret data in the cover-image in such that it is resistant to RS attacks. In the beginning, it uses the simple LSB replacement technique and conceals secret bits in the cover-image. In order to increase the security against RS analysis, after concealing the secret data in the cover-image by LSB, pixel values are detected by the GA. So, the existence of a secret data is hard to detect by RS analysis. The results showed that the resistance of the proposed method against steganalysis provides higher quality and a good trade-off between security and the resulted stego-image quality.

In [18], the basic Particle Swarm Optimization (PSO) is adapted and used as an optimization technique to solve the problem of optimizing a stego-image. The experimental results showed that the PSO obtained a superior result than other approach i.e. genetic algorithm.

3. IMAGE STEGANOGRAPHY BACKGROUND

Image steganography is a technique depending on concealing secret message behind any cover image, and hence it can be transferred over unsecure channels [3]. As shown in fig. 1, Image steganography has four components [5, 19]:

- **Cover Image:** the secret message carrier.
- **Key:** for embedding and extracting purpose.
- **Message:** the secret information to be hidden.
- **Stego Image:** the carrier image with concealed information.

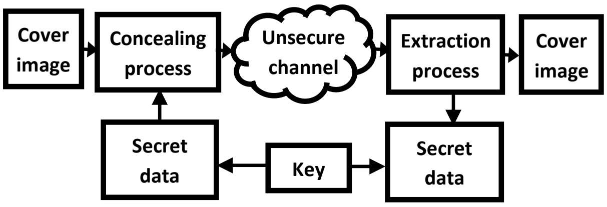


Fig 1: Generalized block diagram of steganography procedure

images can be classified into many types such as JPEG (Joint Photographic Experts), BMP (Bitmap), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), TIFF (Tagged Image File Format), and etc. Most of these extensions use RGB format to show intensity of pixel color.

Also, the image types are three; color, grayscale and binary [20]. There are four categories of this steganography; spatial domain, transform domain, distortion techniques and masking and filtering [5]. Spatial domain has seven schemes; LSB (Least Significant Bit), Pixel Value Differencing (PVD), Gray Level Modification (GLM), Parity Checker Method (PCM), Exploiting Modification Direction (EMD), Diamond Encoding (DE) and Optimal Pixel Adjustment Process (OPAP) [5]. In this research, the selected image type is the color image, while the preferred technique is the spatial domain Using LSB technique is the best approach under special domain. Therefore, the chosen scheme in this research is the least significant bit (LSB).

LSB is the less important section of a pixel. so, modifying LSBs of pixels cannot change an image too much. This method is very simple and easy to implement. For example, if a pixel $(01100111)_2$ and some secret bits $(100)_2$, we can conceal the secret bits inside the last three bits of the pixel. Consequently, the resulted pixel is (01100100)2. By retrieving the last three bits of the modified pixel, the secret bits can be recovered.

There are 3 types of digital steganography protocols [21]:

1. **Pure Steganography:** A system that doesn't necessitate exchanging of a cipher (such as a stego-key).
2. **Secret Key Steganography:** A system requiring exchanging a secret key. This takes a cover message with the secret message embedded inside. Only those who know that secret key can decode the secret message.
3. **Public Key Steganography:** A system using 2 keys (public and private) for security purposes.

Modifying LSB values in necessary for embedding the secret message inside the image (which is the carrier). The secret message is decomposed and concealed in the last r bits of a cover image so that hackers cannot notice it. In the simple least significant bit, the message size is 12.5% of the cover image, and this is considered small storage capacity. Consequently, some researchers later used the base technique concealing the message: 3.3.2. [22]. In this method, the first 3 bits of the message are embedded into the last three bits of the Red component, the second 3 bits into the last 3 bits of the Green component and the last 2 bits in the last 2 bits of the Blue one. Since the variation in blue is perceptible – more than both red and green – to the human eye, the researchers chose to put only 2 bits in the Blue component. In this paper, the author proposes a 24-bit color image steganography in spatial domain utilizing the 3-3-2 LSB replacement technique for embedding process.

4. FIREFLY ALGORITHM

4.1 Introduction to Firefly Algorithm

FA is a meta-heuristic algorithm inspired by the flashing patterns and behavior of fireflies [23]. Fireflies use this flashes for two main functions i) to attract mating partners or communication, and ii) as a protective warning mechanism. Yang simulated this behavior using the following three idealized rules:

I- All fireflies are unisex. So, one firefly will be attracted to other fireflies regardless their sex;

II- Attractiveness is proportional to their brightness, thus for any two flashing fireflies, the less bright one will move towards the brighter one. The brightness can decrease as their distance increase. If there is no brighter one than a particular firefly, it will move randomly.

The brightness of a firefly is determined by the landscape of the objective function.

4.2 Structure of the Classic FA

There are two important issues in firefly algorithm, light intensity variation and other is formulation of the attractiveness. For simplicity, it is assumed that the attractiveness of a firefly is determined by its brightness which in turn is associated with the objective function $f(x)$ at a particular location x.

Since a firefly's attractiveness is proportional to the light intensity by another firefly, the attractiveness β of a firefly can be formulated by:

$$\beta = \beta_0 e^{-\gamma r^2}, \qquad (1)$$

Where, β_0 is the attractiveness at distance $r = 0$ and γ is the light absorption coefficient at the source. With each movement of fireflies, their attractiveness decreases with the distance from its source, and light is also absorbed by the air.

For any two fireflies I and J at position Xi and Xj, the distance between them is

$$r_{ij} = \|x_i - x_j\| = \sqrt{\sum_{k=1}^{d} (x_{i,k} - x_{j.k})^2}, \qquad (2)$$

Where $x_{i,k}$ is the kth component of the spatial coordinate x_i of ith firefly.

The movement of firefly i towards another brighter firefly j is formulated by

$$x_i^{t+1} = x_i^t + \beta_0 e^{\gamma r_{ij}^2}\left(x_j^t - x_i^t\right) + \alpha \varepsilon_i^t, \qquad (3)$$

Where, the second term is the attraction while the third term is a randomization parameter. α is a randomization parameter normally selected within range [0,1] and ε_i^t is a vector of random numbers drawn from a Gaussian or uniform distribution. For the most cases of implementation, $\beta_0 = 1$ and γ varies from 0.01 to 10 [15], [20].

4.3 Levy-Flight Firefly Algorithm (LFA)

LFA [13], is a hybrid firefly algorithm, was developed by Xin-She Yang in 2010 and it combines the three idealized rules of the firefly algorithm together with the Levy flights as an efficient search strategy. In this algorithm, the attractiveness β and the distance r between two fireflies are the same as in firefly algorithm, but the movement of a firefly i towards another brighter firefly j is a random walk, where the step length is drawn by the Levy distribution.

$$\begin{aligned} x_i^{t+1} = x_i^t + \beta_0 e^{\gamma r_{ij}^2}\left(x_j^t - x_i^t\right) + \alpha\ sign\left[rand - \frac{1}{2}\right] \\ \oplus L\acute{e}vy, \qquad (4) \end{aligned}$$

Where, the third term is a randomization via $L\acute{e}vy - Flight$ with α being the randomization parameter. The product $\oplus$ means entry wise multiplications. The random step length is drawn from a $L\acute{e}vy$ distribution which has an infinite variance with an infinite mean.

$$L\acute{e}vy \sim u = t^{-\lambda}, \quad (1 < \lambda \leq 3), \qquad (5)$$

Lévy distribution is obtained by Mantegna's algorithm [24], where the step length s can be calculated as follows.

$$s = \frac{u}{|v|^{1/\beta}}, \qquad (6)$$

Where u and v are normally distributed stochastic variables. But u is calculated as $u\sigma_u$, where

$$\sigma_u = \left\{\frac{\Gamma(1+\beta)\sin(\pi\beta/2)}{\Gamma[(1+\beta)/2]\beta 2^{(\beta-1)/2}}\right\}^{1/\beta}, \qquad \sigma_v = 1. \qquad (7)$$

The resulting distribution (for s) has the same behavior of a Levy distribution for $|s| \geq |s_0|$ where s_0 is the smallest step.

4.4 The Interaction between Fireflies

By performing the random walk via levy flight as presented in equation 3, each firefly moves towards all of the brighter fireflies based on the objective function. To illustrate this, let we have a population of 10 fireflies, the following fig. 2 simply represents the updating positions of two fireflies (i.e. 10 and 9) in a 2d search space with all 10 fireflies in the population group.

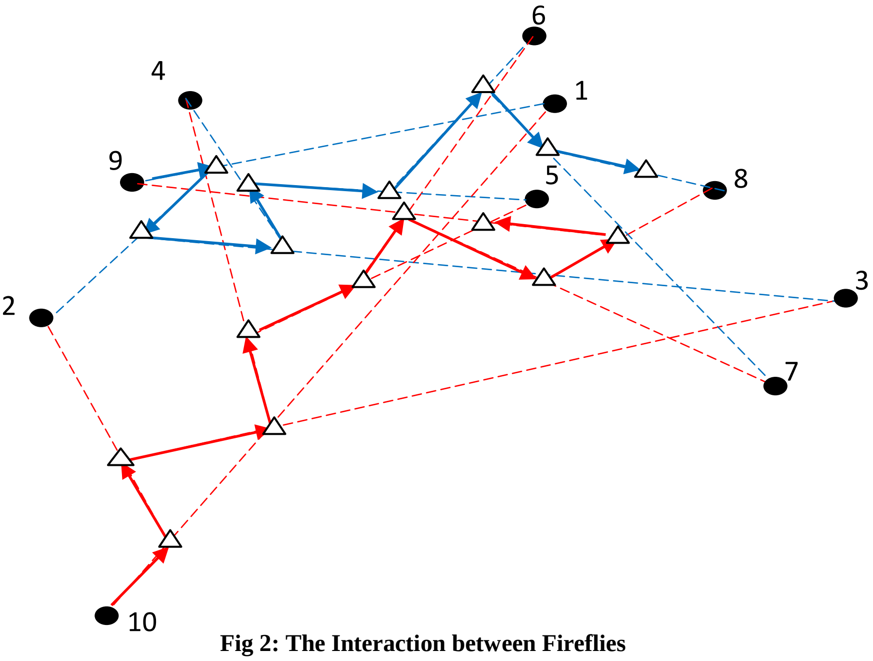


Fig 2: The Interaction between Fireflies

4.5 Mutated Firefly Algorithm (MFA)

In 2014, Arora et. al. are introduced MFA [14]. It is a modified firefly algorithm, it explores the search space by adding features to less bright firefly from the brighter firefly. In this algorithm, the fireflies are arranged in a way that best firefly is placed at top and worst firefly at bottom. Then, only the upper 40% fireflies (which have good features) will donate their features to lower 40% based on the following mutation probability P_m

$$MP = f_{new} - f_{old} \quad (8)$$

Where, f_{new} denotes the fitness of the new firefly and f_{old} denotes the fitness of the original (old) firefly. For a generation that undergoes n_m mutation operations, the average mutation progress value MP is given by (9)

$$\widetilde{\mathrm{MP}} = \frac{1}{\mathrm{n_m}} \sum MP \qquad (9)$$

Mutation rates are adjusted before the end of each generation, using this average progress values.

4.6 The Proposed Scheme

In successive three stages, in the first stage the proposed algorithm is initialized with a population of fireflies which will carry each secret byte in the form of different reversible mutation patterns to optimize the search process; these fireflies are moved to a random pixel's locations and evaluated to detect their brightness as an initial state. In the second stage, in iterated process, the brightness of each firefly is updated after its movement towards other brighter one. In the third stage, the optimal carrier pixel is embedded in its RGB components using 3-3-2 LSB technique.

Before starting to embed the secret message into the cover image, we have to covert the secret message into binary format. The way that proposed MLFA finds the optimal pixel's locations for embedding is explained in detail below.

4.6.1 Stage 1: Set up the objective function:

Generally, Peak Signal-to-Noise Ratio (PSNR) or Mean square error (MSE) is used to measure the image quality. Therefore, the objective function is to maximize the PSNR or minimize the MSE.

MSE is the average squared difference between the cover-image and the stego-image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. Here, the author adopts the following formulation as our objective function.

$$f(I') = \sum (C_I - C_{I'})^2 \qquad (10)$$

Where C_I and $C_{I'}$ represent the value of the corresponding cover and stego-pixel color component C $(C \in [R, G, B])$.

4.6.2 Stage 2: Detecting the best location

4.6.2.1 Set up Parameters, which Include:

U: Upper pound: X and Y axis coordinates = (511,511).

L: Lower pound: X and Y axis = (0,0).

N: Number of fireflies = 25 fireflies (equally 5 groups).

MaxGeneration: maximum number of iterations = 100.

$\boldsymbol{\beta_0}$: the attractiveness at distance $(r = 0) = 1$.

$\boldsymbol{\gamma}$: is the light absorption coefficient at the source = varies from 0.01 to 10.

$\boldsymbol{\alpha}$: is a randomization parameter normally selected within range [0, 1] = $\boldsymbol{\alpha \epsilon (0, 1)}$.

4.6.2.2 Different Patterns Constitution:

Given a one secret byte in the form of eight-bit binary representation i.e. [B_1 B_2 B_3 B_5 B_6 B_7 B_8], Let L_B is the number of bits to be rotated to the left and reserved. The proposed scheme will construct the different five patterns for the inputted secret byte at L_B = [2, 3, 4, 5, 6] as shown in figure 3.

Pattern	L_B	The constructed Pattern							
1	2	B_3	B_4	B_5	B_6	B_7	B_8	B_2	B_1
2	3	B_4	B_5	B_6	B_7	B_8	B_3	B_2	B_1
3	4	B_5	B_6	B_7	B_8	B_4	B_3	B_2	B_1
4	5	B_6	B_7	B_8	B_5	B_4	B_3	B_2	B_1
5	6	B_7	B_8	B_6	B_5	B_4	B_3	B_2	B_1

Fig. 3: Constituted Different Patterns

4.6.2.3 Initialize Firefly Population:

In the proposed approach, the population of fireflies is divided into equally 5 groups. Each group will carry the inputted secret byte in the form of specific pattern. Then all of those fireflies are moved to random locations (pixels) in the search space (cover-image) as an initial state. Fig. 2 shows the typical structure of the firefly.

K	Pattern (Index)	X Coordinate	Y Coordinate	Secret Byte

Fig. 3: The Firefly Structure

4.6.2.4 Firefly's Position and Features Updating

The firefly algorithm (FA) is an iterative algorithm. In each iteration, the embedded pixel for each firefly is obtained by embedding its own restructured secret byte in that firefly position. Once this process is completed then the cost function, the sum of squared differences (SSD) for the carrier-pixel and stego-pixel is calculated to determine the light intensity of that firefly using eq. 10. then each firefly's position and features are updated using eq. 4 and eq. 8, respectively. The best location is found when the following stopping criteria occur when the maximum number of iterations has been reached.

The proposed image steganography can be formalized as follows.

Inputs:

A cover-image, $I = P_1, P_2, \ldots, P_{H \times W}$,

A secret byte stream $S = b_1, b_2, \ldots, b_n$,

Outputs:

A stego-image, $I' = P'_1, P'_2, \ldots, P'_{H \times W}$,

```
Define an objective function f(x)
Define the upper bound U and lower bound L for the design variables
For each secret byte
    Constitute the different 5 patterns
    Generate an initial population of fireflies $x_i$ (i=1 to n)
    Divide these population into equally 5 groups, each
    group will carry the current secret byte in the form of
    corresponding pattern.
    Light intensity $I_i$ at $X_i$ is determined by equation (10).
    Define light absorption coefficient γ=0
    While (t< MaxGeneration)
        Sort the fireflies based on their light intensity
        For i= 1 to n, all n fireflies
            For j= 1 to n, all n fireflies
                If ( $I_i < I_j$)
                Move firefly i towards firefly j by equation (4).
                Donate the features (pattern form) of firefly j to
                firefly I based on equation (8).
                Evaluate new solutions and update the light
                Intensity by equations (11 and 12).
            End for j
        End for i
        Rank the fireflies and find the most attractive female
        for each male
    End while
    Post-process results and visualization
End For
```

4.6.3 Stage 3: Embedding process

After founding the best location, i.e. referring to the optimal carrier pixel, we can embed the secret byte in the LSB of RGB (Red, Green and Blue) pixel value of this carrier pixel in 3, 3, 2 orders respectively. At first, three bits of the secret byte are concealed inside three bits of LSB of Red pixel, next three bits in the three bits of LSB of Green pixel. Finally, the remaining two bits of secret byte are concealed in two bits of LSB of Blue pixel.

5. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed scheme, MATLAB simulations are performed by using three standard 24-bit 512×512 size images e.g. 'Lena', 'Peppers' and 'Baboon' from the USC image database [29]. These original images are shown in Fig. 4 (A). The proposed algorithm is applied on them as a cover-images and the obtained stego-images are portrayed in Fig. 4 (C).

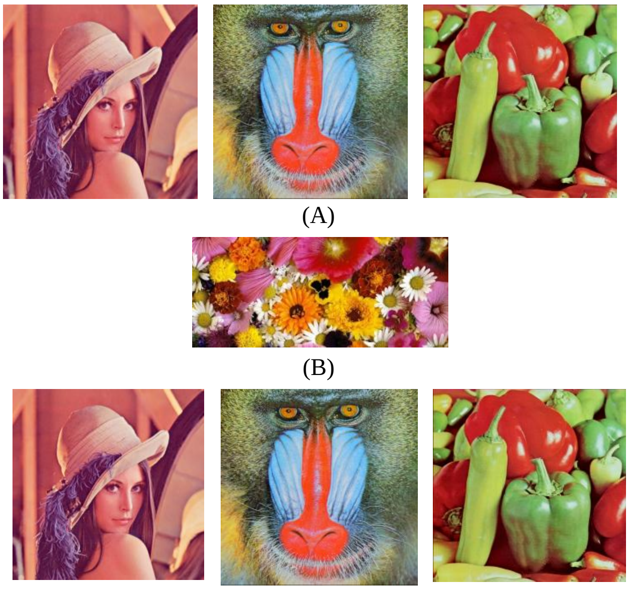
The PSNR given by Eq. (11) and Mean square error (MSE) given by Eq. (12) are chosen as objective measure to evaluate the proposed scheme.

$$PSNR = 10 log_{10} \frac{L^2}{MSE} \qquad (11)$$

Where, L is peak signal level for an image color component c ($C \in [R, G, B]$respectively it is taken as 255.

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (I_{i,j} - I'_{i,j})^2 \qquad (12)$$

Where, $I_{i,j}$ represents original image and $I'_{i,j}$ represents corresponding stego-image having resolution of $H \times W$ pixels.



(A)

(B)

(C)

Fig. 4: (A) the cover-images. (B) the secret-image.

(C) the obtained stego-images.

Table I shows the Cover-Images and the Concealed Message characteristics. H and W represent image width and height.

Table 1: The cover-images and the concealed message

Cover-images		**Secret image**	
Image name	**Resolution (W*H)**	**Image name**	**Resolution (W*H)**
Penguin.png	512 × 512	Flowers.png	400 × 200
Lena.png	512 × 512		
Baboon.png	512 × 512		

Table 2 and fig. 5 represent the PSNR values of testing and interpolated image color component a (a ∈ [r, g and b]) respectively.

As mentioned before in section 5, low values of MSE and high values of PSNR are desired for good image steganography. According to [7], the accepted value of PSNR is greater than 30 dB.

Table 2: Evaluation measures of the proposed scheme

Cover-Image	**The Proposed Scheme Results**	**3,3,2 LSB Technique Results**
Penguin	46.6487	41.3921
Lena	55.6126	42.5362
Baboon	51.9413	36.5497

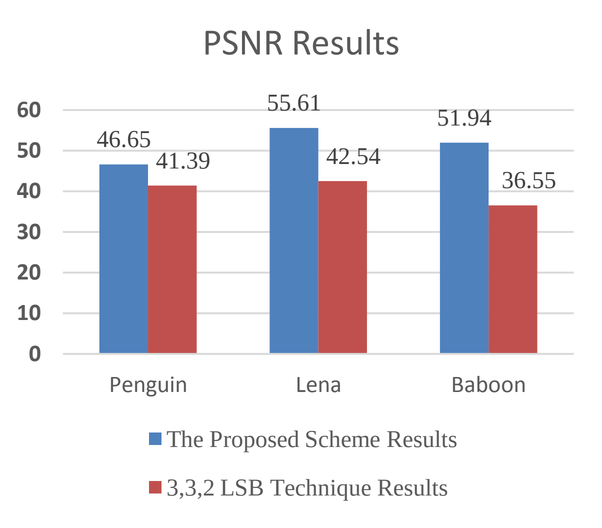


Fig. 5: Performance results according to Eq. (11).

As can be seen in table 2 and fig. 5, the proposed FA-based scheme reached the best results, when compared with the 3,3,2 LSB Technique.

6. CONCLUDED REMARKS

An improved 24-bit image steganography scheme is designed based on firefly's Mutation probability concept combined with the characteristics of levy flight firefly optimization algorithm. During the execution, coordinates of the optimal cover pixels for embedding are located by a population of fireflies taking into account two considerations: The first one, each secret byte is re-structured into different 5 patterns and be carried by those population of fireflies to optimize the search process and enhance the security level of information hiding. The second consideration is that based on combines l´evy-flight with search strategy via firefly as a random walk, the locations of these fireflies are updated to move from pixel to another in the cover image's search space. Finally, based on the objective function, the best firefly for each inputted secret byte is detected to help in the process of embedding utilizing the 3-3-2 LSB replacement technique.

Experimental results show that the proposed approach is considered a high embedding efficiency approach due to the low modification on the host image that makes the stego-image have a very good quality. PSNR and MSE measurements are used to measure the visual quality and all the obtained experimental results have a PSNR above 40 dBs.

7. REFERENCES

[1] Darshni, P.; Ghanekar, U., "A Hybrid Data Hiding Scheme to Enhance the Capacity of One-Third Probability Embedding Method," Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on , vol., no., pp.269,272, 13-14 Feb. 2015.

[2] Das, P.; Kushwaha, S.C.; Chakraborty, M., "Multiple embedding secret key image steganography using LSB substitution and Arnold Transform," Electronics and Communication Systems (ICECS), 2015 2nd

International Conference on , vol., no., pp.845,849, 26-27 Feb. 2015.

[3] Mishra, Rina; Bhanodiya, Praveen, "A review on steganography and cryptography," Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in , vol., no., pp.119,122, 19-20 March 2015.

[4] Huy Nguyen Tien; Bac Le, "Noise reduction approach for LSB matching revisited," Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2013 IEEE RIVF International Conference on , vol., no., pp.76,79, 10-13 Nov. 2013.

[5] Shelke, S.G.; Jagtap, S.K., "Analysis of Spatial Domain Image Steganography Techniques," Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on , vol., no., pp.665,667, 26-27 Feb. 2015.

[6] Nayak, D.K.; Bhagvati, C., "A threshold-LSB based information hiding scheme using digital images," Computer and Communication Technology (ICCCT), 2013 4th International Conference on , vol., no., pp.269,272, 20-22 Sept. 2013.

[7] Blum C, Merkle D (eds) (2008) Swarm intelligence: introduction and applications. Springer, Berlin/Heidelberg, Germany.

[8] Ching-Sheng Hsu; Shu-Fen Tu, "Finding Optimal LSB Substitution Using Ant Colony Optimization Algorithm," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on , vol., no., pp.293,297, 26-28 Feb. 2010.

[9] Majid Kiamini ,Saeid Fazli ," A High Performance Steganographic Method using JPEG and PSO Algorithm," IEEE, 2008.

[10] Arora, S.; Singh, S., "A conceptual comparison of firefly algorithm, bat algorithm and cuckoo search," Control Computing Communication & Materials (ICCCCM), 2013 International Conference on , vol., no., pp.1,4, 3-4 Aug. 2013.

[11] X.-S. Yang and X. He, Firefly algorithm: Recent advances and applications. International Journal of Swarm Intelligence 1, 36 (2013).

[12] Fister, I., Fister Jr, I., Yang, X-S. and Brest, J. (2013b) 'A comprehensive review of firefly algorithms', Swarm and Evolutionary Computation, Vol. 13, pp.34–46.

[13] Yang X-S. Firefly algorithm, Levy flights and global optimization. In: Research and development in intelligent systems XXVI. Springer; 2010. p. 209–18.

[14] Arora, S.; Singh, S., "A conceptual comparison of firefly algorithm, bat algorithm and cuckoo search," Control Computing Communication & Materials (ICCCCM), 2013 International Conference on , vol., no., pp.1,4, 3-4 Aug. 2013.

[15] Pravalika, S.L.; Joice, C.S.; Raj, A.N.J., "Comparison of LSB based and HS based reversible data hiding techniques," Devices, Circuits and Systems (ICDCS), 2014 2nd International Conference on , vol., no., pp.1,4, 6-8 March 2014.

[16] Z.-H. Wang, C.-C. Chang, and M.-C. Li: Optimizing Least-significant-bit Substitution Using Cat Swarm Optimization Strategy, Information Sciences, In Press (2010).

[17] S. Wang, B. Yang, and X. Niu, Secure steganography method based on genetic algorithm, Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 1, pp. 28-35, 2010.

[18] Rafael Lima De Carvalho, Warley Gramacho Da Silva and Ary Henrique Oliveira De Morais. Optimizing Image Steganography using Particle Swarm Optimization Algorithm. International Journal of Computer Applications, Volume 164 - No.7, April 2017.

[19] Shelke, S.G.; Jagtap, S.K., "A novel approach: Pixel matching based image steganography," Pervasive Computing (ICPC), 2015 International Conference on , vol., no., pp.1,4, 8-10 Jan. 2015.

[20] Patel, K.; Ragha, L., "Binary image Steganography in wavelet domain," Industrial Instrumentation and Control (ICIC), 2015 International Conference on , vol., no., pp.1635,1640, 28-30 May 2015.

[21] B. Dunbar, "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", Sans Institute, Vol. 2002, pp. 1-9, 2002.

[22] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan and A. A. Zaidan, "High Rate Video Streaming Steganography," 2009 IEEE International Conference on Information Management and Engineering (ICIME), Kuala Lumpur, 2009, pp. 550-553.

[23]] X. S. Yang, Firefly algorithms for multimodal optimisation, Proc. 5th Symposium on Stochastic Algorithms, Foundations and Applications, (Eds. O. Watanabe and T. Zeugmann), Lecture Notes in Computer Science, 5792: 169-178 (2009).

[24] Mantegna, R. N., "Fast and Accurate Algorithm for Numerical Simulation of L'evy stable Stochastic Processes", in Physical Review E, vol. 49, Issue 4, 1994, pp. 4677-4683.