

Information Hiding using LSB Technique based on Developed PSO Algorithm

Wisam Abed Shukur¹, Khalid Kadhim Jabbar²

¹Computer Science Dept., College of Education for Pure Sciences/Ibn Al-Haitham, University of Baghdad, Iraq

²Computer Science Department, College of Education, University of Mustansiriyah, Iraq

Article Info

Article history:

Received Jul 28, 2017

Revised Oct 7, 2017

Accepted Oct 20, 2017

Keyword:

Cover image

Developed PSO algorithm

Search space

Steganography

Stego image

ABSTRACT

Generally, The sending process of secret information via the transmission channel or any carrier medium is not secured. For this reason, the techniques of information hiding are needed. Therefore, steganography must take place before transmission. To embed a secret message at optimal positions of the cover image under spatial domain, using the developed particle swarm optimization algorithm (Dev.-PSO) to do that purpose in this paper based on Least Significant Bits (LSB) using LSB substitution. The main aim of (Dev.-PSO) algorithm is determining an optimal paths to reach a required goals in the specified search space based on disposal of them, using (Dev.-PSO) algorithm produces the paths of a required goals with most efficient and speed. An agents population is used in determining process of a required goals at search space for solving of problem. The (Dev.-PSO) algorithm is applied to different images; the number of an image which used in the experiments in this paper is three. For all used images, the Peak Signal to Noise Ratio (PSNR) value is computed. Finally, the PSNR value of the stego-A that obtained from blue sub-band color is equal (44.87) dB, while the stego-B is equal (44.45) dB, and the PSNR value for the stego-C is (43.97)dB, while the value of MSE that obtained from the same color sub-bands is (0.00989), stego-B equal to (0.01869), and stego-C is (0.02041). Furthermore, our proposed method has ability to survive the quality for the stego image before and after hiding stage or under intended attack that used in the existing paper such as Gaussian noise, and salt & pepper noise.

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Wisam Abed Shukur,
Computer Science Dept.,
College of Education For Pure Sciences/Ibn Al-Haitham,
Baghdad University,
Baghdad, Iraq.
Email: wisam_shukur@yahoo.com

1. INTRODUCTION

The big losses and digital signal transmission due to unwanted access of data with the high demand in both; the security of data becomes an imperative and critical concept. For data securing and preventing them from unauthorized access, encryption and steganography processes is used [1]. The most important concept in any communication process between sender and receiver via the transmission channel is security. The using of advance technology inside the World Wide Web (WWW) to exchange information leads to increase the challenges and risks. However, the management of challenges and risks is possible with using an advanced technology of secure networks but these technologies are not enough for information security over communication between sender and receiver. Therefore, additional mechanisms of security are needed to secure information. [2], an origin of steganography word is Greek, steganography means "covered writing" or "concealed writing" [3]. The main difference between steganography and cryptography is keeping the

existence of a message secret. The shared goal of steganography and cryptography is information protecting against malicious or unwanted persons or parties [4]. An embedding algorithm embeds secret information in a host image; the hiding process is performed with selected private or secret key to increase the complexity of hiding process.

Figure 1 shows a generic model of an image steganographic. After embedding process, transmitting a stego-image to the receiver via transmission medium or communication channel is performed. The receiver extracts hidden information which embedded using embedding technique by the sender from received stego-image with using same or another key according to type of steganography that selected initially. The receiver will apply an extraction technique on stego-image for that purpose. Via transmitting a stego-image from the sender to the receiver, there are many unauthorized persons or parties that notice a stego-image but without extracting the hidden contents of a stego-image [5]. The embedding techniques are selected according to type of domain, the types of embedding domains are spatial and frequency domains. The types of host or cover are text, audio, image and video [6]. The spatial domain is used in this work. In the spatial domain, the secret message is embedded in the specified positions by adding or replacing the bits of selected bits of cover or host image. Generally, the typical characteristics of spatial domain are all methods related to this domain are very easy and simple to understand, the execution time is low, a secret message is applied to the pixels directly without transforming an original image and finally a secret message is embedded in the region or part of host or cover image that considered as redundant [7]. There are many techniques related to the spatial domain of an image steganography such as Least Significant Bit (LSB) and Most Significant Bit (MSB) techniques. The LSB technique is used in the existing paper. This technique embeds secret information in the least significant bit of selected pixels of the host image. So, it exploits the point which the precision in several image formats is greater than the human vision. The variations of image colors are indistinguishable by human vision [8].

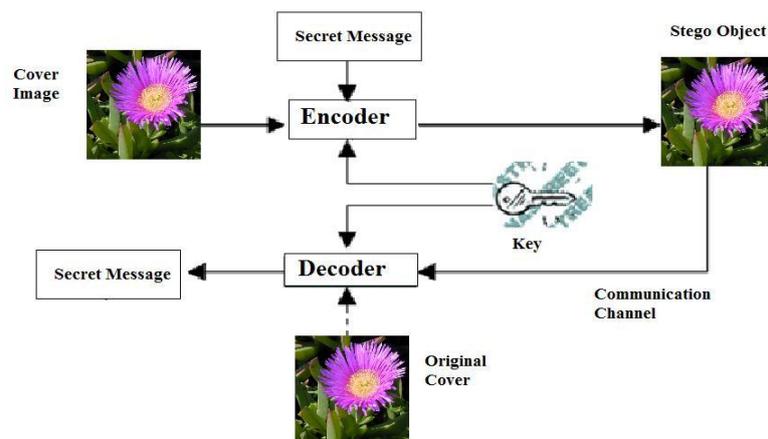


Figure 1. Generic Model of an Image Steganographic

2. THE RELATED ATTEMPTS

The techniques of data hiding are classified into LSB substitution of spatial domain; LSB is similar to many methods as Pixel Value Differencing (PVD). The principle work of LSB substitution method is replacing LSB's of pixels values within image that considered as cover to get stego image, this is most commonly used. Secret bits of sensitive information are replaced within LSB's bits of cover image. When result of matching process is not obtain? Then the adding or subtracting operations for value of cover image pixel are performed for one randomly. The core work of PVD based methods is computing the difference of two pixels that are consecutive to specify the depth of embedded bits. Chang et al. [9] the strategy of dynamic programming that proposed is pick the optimal or best via all tables of substitution efficiently. In [10] the PSO is used to hide a secret information or message in an image based on LSB and in [11] an image hiding within another image using LSB technique. These methods based PSO algorithm are better results than other standard LSB techniques. The technique that uses dynamic programming and genetic algorithms are based on effects that considered as visual for human. The data hiding techniques of spatial domain are producing good quality stego images.

3. RESEARCH METHOD

3.1. Particale Swarm Optimization Algorithm (PSO)

In 1995, by Kennedy and Eberhart, The PSO was introduced [12]. The model of PSO consists of many particles for swarm, At the beginning, this presents 'N' number of particles randomly. for each particle, the result of an objective function is obtained. the particle and its group of the flying velocity can be generated to next generation with seeking still to get better solution. The pbest represents the optimal value obtained via particle and the gbest represents the best value obtained among all the particles [13]. The random candidate solutions population is initialized. for searching a new solutions, they must move in an iterative manner via the d-dimensions search space of problem when the fitness function (f) can be computed as metric or measure for quality assessment. the position-vector x_i (where i is an index for particle) is used to represent a positions since each particle has a position. The velocity-vector v_i is used to represent a velocity. For each one of particle, the best position is remembered by them. a vector i -th, with its d -dimensional value is represented as pbest (pid). The best position-vector is stored in a vector i -th, and its d -th dimensional value which is represented as gbest (pgd). t represents time iteration, Equation (1) is used to determine the updating or modifying the velocity (v_{id}) from the old velocity to the new. The sum operation of the previous position and the new velocity is used to specify a new position (x_{id}) as shown below in Equation (2).

$$V_{(id+1)} = w * v_{id} + c_1 * r_1 * (pgd - x_{id}) + c_2 * r_2 * (pid - x_{id}) \quad (1)$$

$$X_{(id+1)} = x_{id} + v_{(id+1)} \quad (2)$$

Where i from 1 to N ; an inertia weight is described as w , r_1 and r_2 are considered as random numbers, to maintain the diversity of the population, these are used. These numbers are distributed in the interval $[0,1]$ of the d -th dimension for the i -th particle. c_1 acts a positive constant number, this constant is called coefficient of the self-recognition component; c_2 represents a positive constant number, this constant is called coefficient of the social component. From equation(2), a particle decides where to move from current position to next position, with its experience, it saves the memory of the best past position, and the most successful particle. to lead the particles in the search space effectively, during one iteration, the maximum moving distance must in between the maximum velocity $[-v_{max}, v_{max}]$. The steps of standard PSO algorithm are shown in algorithm (1) [14]:

Algorithm 1. The Standard PSO Algorithm

I/P: Parameters initialization (c_1 , c_2 , w , v_{max} , $Swarm_Size$, Max_Iter , r_1 , r_2).

O/P: highest fitness optimization

Step 1: Generating initial particles and velocities randomly

Step 2: For each particles, the fitness function is calculated.

Step 3: If new position is better than old position then updating process is performed.

Step 4: Specify the best particle and update the positions using Equations (1) and (2).

Step 5: If the high fitness is satisfied or maximum number of iterations has exceeded then go to 6 else go to 2.

Step 6: the best value is Stored then exit.

3.2. Developed PSO Algorithm

With particle swarm optimization (PSO), the problem is addressed using swarm of particles which moves at domain of search space looking for best solution. Each one of particles has position and velocity. The particles move within the search space by iteratively updating them. For strategies of an iteration for updating, two choices are found; synchronous or asynchronous [15]. Using the developed PSO algorithm in this work aims to secure transmitted information that sent by sender via insecure communication channel to the receiver. The important aim of the proposed system is to provide secure communication between sender and receiver. So, an optimal positions in the search space of problem are determined by using developed PSO algorithm to embed a secret message in the host or cover image. After determining an optimal solutions in the host or cover image by this developed algorithm, where starting point of particle did not specify in the PSO algorithm, a particle sometime put in center of the image or put randomly in any position of the search space. The new of developed PSO is to find the starting point. the host or cover image is divided into five parts as following sequence (upper right part, upper left part, lower left part, lower right part and center of image part). The standard PSO algorithm as shown above in algorithm (1) is performed in parallel manner on those five parts. For all locations in the image, the fitness function is computed through applying some steps of statistical calculations such as X-position, Y-position, Mean and Variance. The 2D-dimensional locations can

denoted by X-position and Y-position for the coefficients in the image. For each specified positions, the mean is computed by applying Equation (3) while the variance is calculated by applying Equation (4) as shown below.

$$\text{Mean (i)} = \frac{\sum_{j=1}^M X_i(j)}{M} \quad (3)$$

$$\text{Variance (i)} = \frac{\sum_{j=1}^M (X_i(j) - \text{mean}(i))^2}{M} \quad (4)$$

where: $x_i(j)$ is the datum in specific position, and M is the number of locations.

All information that related for each bird or particle are shown as following:

1. The current position fitness of the bird or particle is denoted by $f(x)$.
2. For each position in the search space, the best fitness is denoted by $f(\text{gbest})$.
3. The neighbors $f(x)$ best fitness is denoted by $f(\text{xbest})$.
4. The current position of the fitness bird or particle is denoted by L_x .
5. The best fitness position in the search space is denoted by L_{gbest} .
6. The best fitness position of the neighbor $f(x)$ is denoted by L_{xbest} .
7. The cognitive and social parameters are called acceleration parameters that bounded between 0 and 2, these parameters are denoted by α, β .
8. The random numbers distributed in $[0, 1]$ are denoted by rand1 & rand2 .
9. The maximum number of iteration is denoted by D .

Each particle moves in the multi-dimensional solutions space with different speeds, therefore, its velocity or speed is according to their moving. For each position, saving information of its previous movement in the problem space is recorded. The movement of particle is influenced by just two factors, the first factor is the local best solution and the second factor is the global best solution. A particle updates its velocity and position if it can specifying a best location that considered as better than others locations which visited previously. The velocity and position updating process is performed using Equation (5) and Equation (6) respectively.

$$f_i(t+1) = f(x) + \alpha \text{ rand1} (L_{\text{gbest}} - L_x) + \beta \text{ rand2} (L_{\text{xbest}} - L_x) \quad (5)$$

$$L_{x_i}(t+1) = L_x + f_i(t+1) \quad (6)$$

With each iteration, The global best location (gbest) is compared to the five parts. the location acts the best starting point of selected locations when the gbest is equaled. This is considered as the start point of the PSO search space which produces the best locations or positions. The developed PSO algorithm for finding best position is shown in algorithm (2). for an iteration process of the algorithm, if better solution is satisfied, then the global best position and the best local position are modified or updated. This process is continuous until the determined number of iterations is exhausted. In this work, The number of iterations is 500 iteration[8].

Algorithm 2. Developed PSO Algorithm

Input : 128*128 cover image , parameters $\alpha, \beta, \text{rand1}, \text{rand2}$, max iteration D , variable W , best location $xx, (L1, L2, L3, L4, L5) = \text{particles}$

Output: Selected locations

Begin

Step 1: Set $D=1, W=0$

Step 2: Position fitness is computed using Equatin (3) and Equation (4)

Step 3: For the selected image do the following

- a. Divided the image region into five section
- b. Specify the center of each section
- c. Initialize the five particle position and velocities in center of each section
- d. Determine the fitness of gbest for each particle
- e. Choose the best of them
- f. Optimize (evaluate fitness) to the better
- g. If the particle fitness $f(x) < \text{particle best fitness } f(\text{xbest})$ Then $f(\text{xbest}) = f(x)$ and $L_{\text{xbest}} = L_x$
- h. If $f(x) < f(\text{gbest})$ Then $f(\text{gbest}) = f(x)$ and $L(\text{gbest}) = L_x$
- i. Update

Particle velocity using Equation (5)

Particle position using Equation (6)

j. If $L1(gbest) = L2(gbest) = L3(gbest) = L4(gbest) = L5(gbest)$ Then Stop the iteration
 $xx = L1(gbest) = L2(gbest) = L3(gbest) = L4(gbest) = L5(gbest)$ Else
 Combine any equal of $(L1(gbest), L2(gbest), L3(gbest), L4(gbest), L5(gbest))$ go to step 3(d)

Step4: Set $D=1, W=0$

Step 5: Calculate the fitness according to Equation (3) and Equation (4) of the image

Step 6: Initialize the particle position and velocities in (xx) of the image

Step 7: optimize (evaluate fitness) of the image
 If particle fitness $f(x) <$ particle best fitness $f(xbest)$ Then $f(xbest) = f(x)$ and $Lxbest = Lx$

Step 8: optimize 2 (evaluate fitness) of image
 If $f(x) <$ $f(gbest)$ Then $f(gbest) = f(x)$ and $Lgbest = Lx$

Step 9: Adjustment process Velocity of particle by Equation (5) Position of particle by Equation (6)

Step 10: List= value (best), $D=D+1$

Step 11: If $(D \leq 500)$ Then Repeat from step (7) Terminate

Step 12: **End**

2.3. Steganography using Developed PSO Algorithm

After a secret message selecting, it must converted into binary form, the number of secret message bits is equal to 500 bit. We select an image with size 128x128 pixels, and then apply the developed PSO algorithm to select the best 500 location of selected image above. The values of the best 500 location are divided into three main parts, each part of them represents a color such as part1 of values represents Red color, part2 of values represents Green color and finally part3 of values represents Blue color. After that all values are converted into binary form. In hiding process, it hide one bit from a secret message in the least significant bit of the blue color that selected to hide information in it, the following algorithm illustrate the embedding stage, while Figure 2 shows the flowchart of embedding stage, and the extraction stage illustrated in algorithm 4.

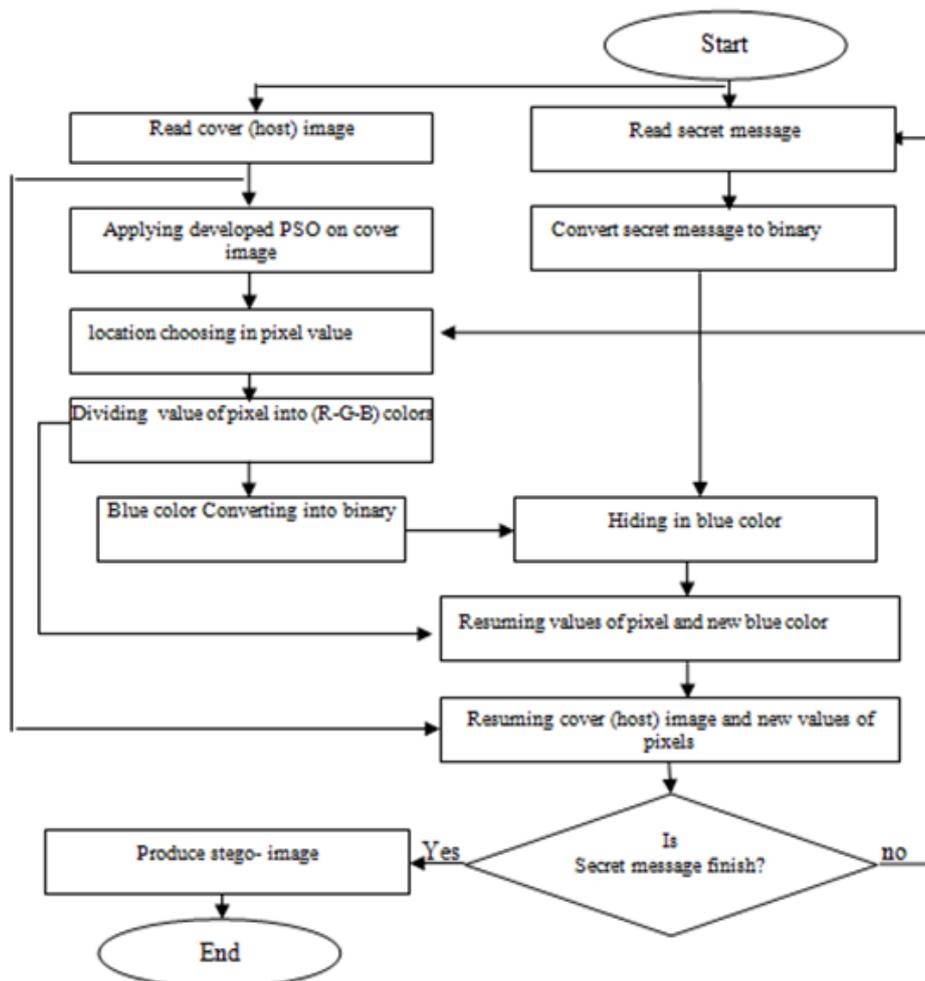


Figure 2. Flowchart of Embedding Stage Using Dev. PSO

Algorithm 3. Embedding Stage**Input:** Cover Image, Secret Message.**Output:** Stego Image.**Begin**Step 1: Read the cover image as: C_o .Step 2: Read a secret message as: S_m .Step 3: Convert S_m into binary form to produce S_m' .Step 4: Apply the developed PSO over C_o .

Step 5: Choose the optimal location in pixel value, and then divide the pixel value into the three color sub-bands Red, Green, and Blue.

Step 6: Choose the blue sub-band as: C_b , Then convert it into the binary form to produce C_b' .Step 7: Embedded S_m' inside C_b' to produce B .Step 8: Reconstruct the B' into the C_b .Step 9: Reconstruct C_b into the cover image to produce a stego image as: S_i .Step 10: **End**.**Algorithm 4. Extraction Stage****Input:** Stego Image.**Output:** Secret Message.**Begin**Step1: Read S_i .Step2: Apply the invers of developed PSO over S_i .

Step3: Choose the optimal location in pixel value, then divided it into Red, Green, and blue sub-bands.

Step4: Select the blue sub-band as C_b , then convert it into binary form to produce C_b' .Step5: Apply the invers of embedding satge to produce the secret message as: S_m .Step6: Reconstruct C_b' to the C_b after reconverting it.Step7: Reconstruct C_b to the blue sub-band, and reconstruct the sego image.Step8: Recover S_m to produce the S_m .Step9: A secret image S_m extracted.Step10: **End**.**3. RESULTS AND ANALYSIS**

The subjective side depending on the value of performance matrix such as: PSNR, and MSE which the computation time before and after the developed PSO is compared and tabulated for each image that used in the proposed methdo, and the histogram plots also compared, Furthermore the developed PSO is calculated for N of iterations. In this section, the results of applying the developed PSO algorithm to determine an optimal solution in search space of problem are shown. Figure 3 shows the three original images that used in our proposed method (take into consideration image texture), each one with its histogram. The value that determined by five particles and the best location in each one of selected image are shown in Table 1.

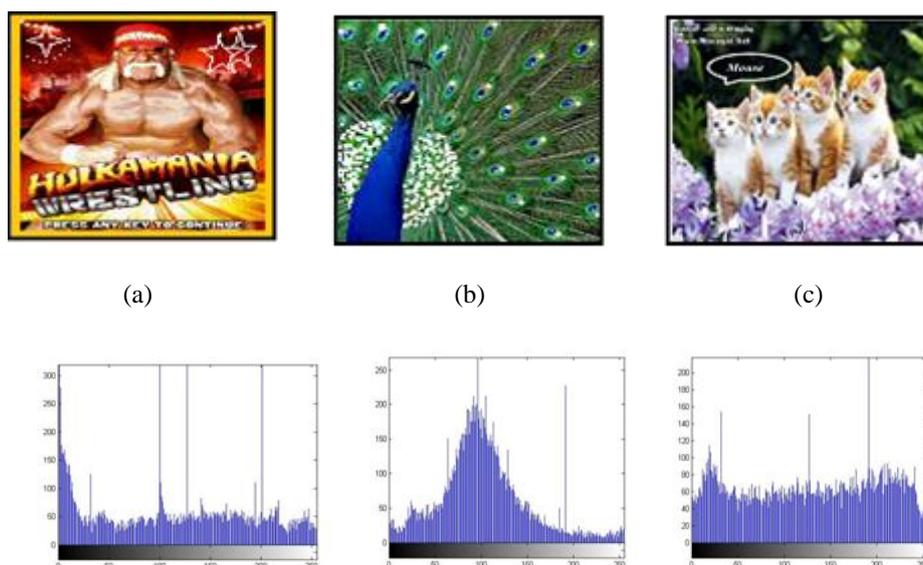


Figure 3. The Original Images

Table 1. Values and Locations of Finding Optimal Starting Location For Dev.- PSO

PSO Number	Location of First iteration	value	Location Before End Iteration	Value	End Location	Value
Pso1	(2,1)	208	(3,1)	124	(5,3)	238
Pso2	(12,11)	236	(5,3)	238	(5,3)	238
Pso3	(6,7)	232	(9,9)	223	(5,3)	238
Pso4	(8,9)	234	(9,9)	223	(5,3)	238
Pso5	(8,8)	88	(9,11)	149	(5,3)	238

The following Figure 4 shows the relationship of locations and values that selected by developed PSO algorithm as illustrated below.

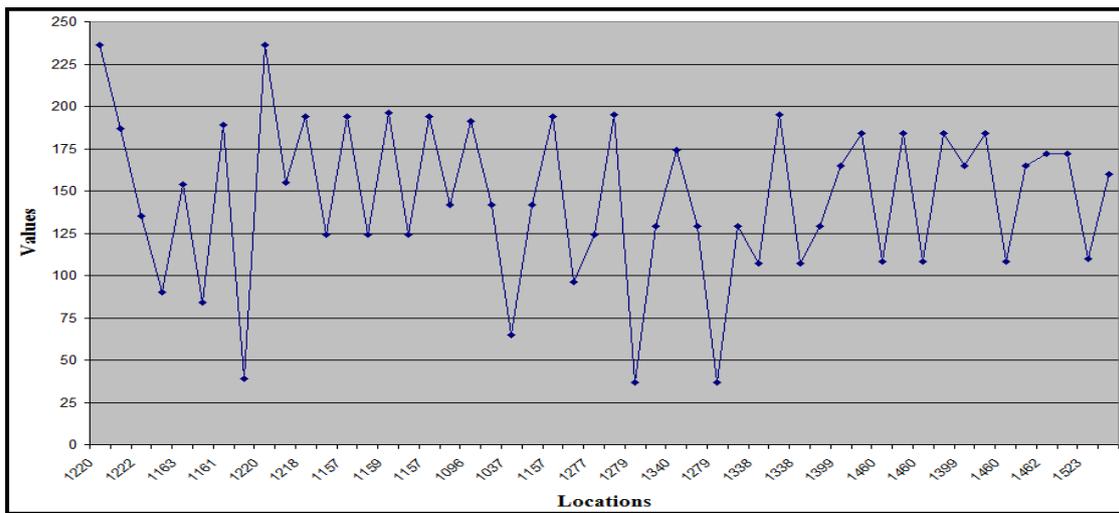


Figure 4. Relationship Between Locations and Values by Dev.-PSO Algorithm

The locations with its values located by developed PSO algorithm are shown in Table 2.

Table 2. Some Values and Locations Selected by Developed PSO Algorithm

S	Value	Location in two dimension	Location in two dimension
1	236	1220	(21, 20)
2	187	1221	(21, 21)
3	135	1222	(21, 22)
4	90	1223	(21, 23)
5	154	1163	(20, 23)
6	84	1162	(20, 22)
7	189	1161	(20, 21)
8	39	1160	(20, 20)
9	236	1220	(21, 20)
10	155	1219	(21, 19)

The Figure 5 shows the produced image after located the optimal location for each one that pointed by green color by using developed PSO Algorithm, the optimal location are different form one to another because of its texture diffirents, there same images are used as cover or host image to perform the developed PSO algorithm on them. The produced image are exposed to some types of intended attack such as salt and pepper that illustrated in Figure 6, while the results under Gaussian noise illustrated in Figure 7.

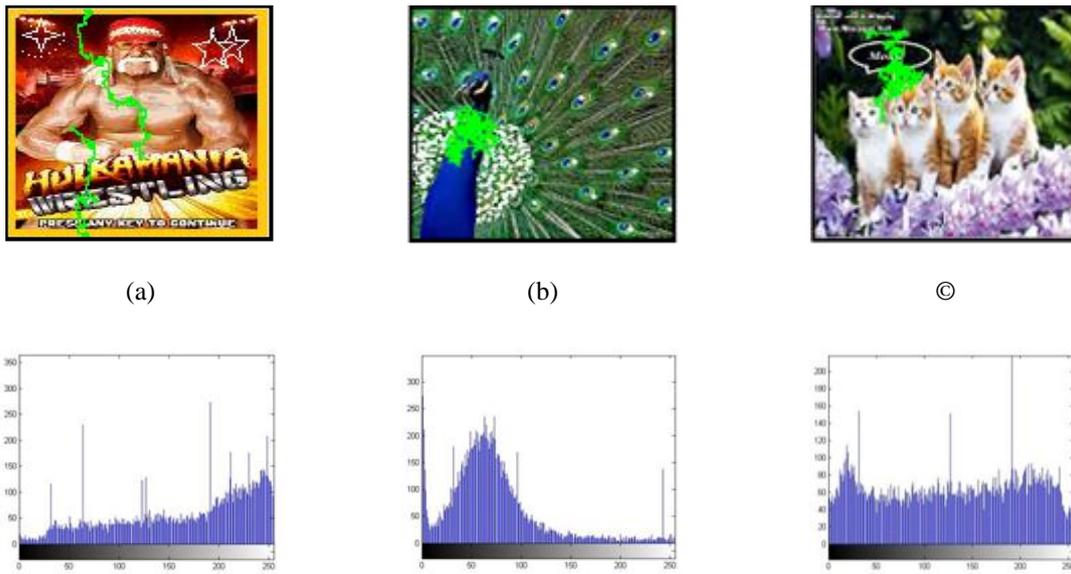


Figure 5. Images after Located a location process

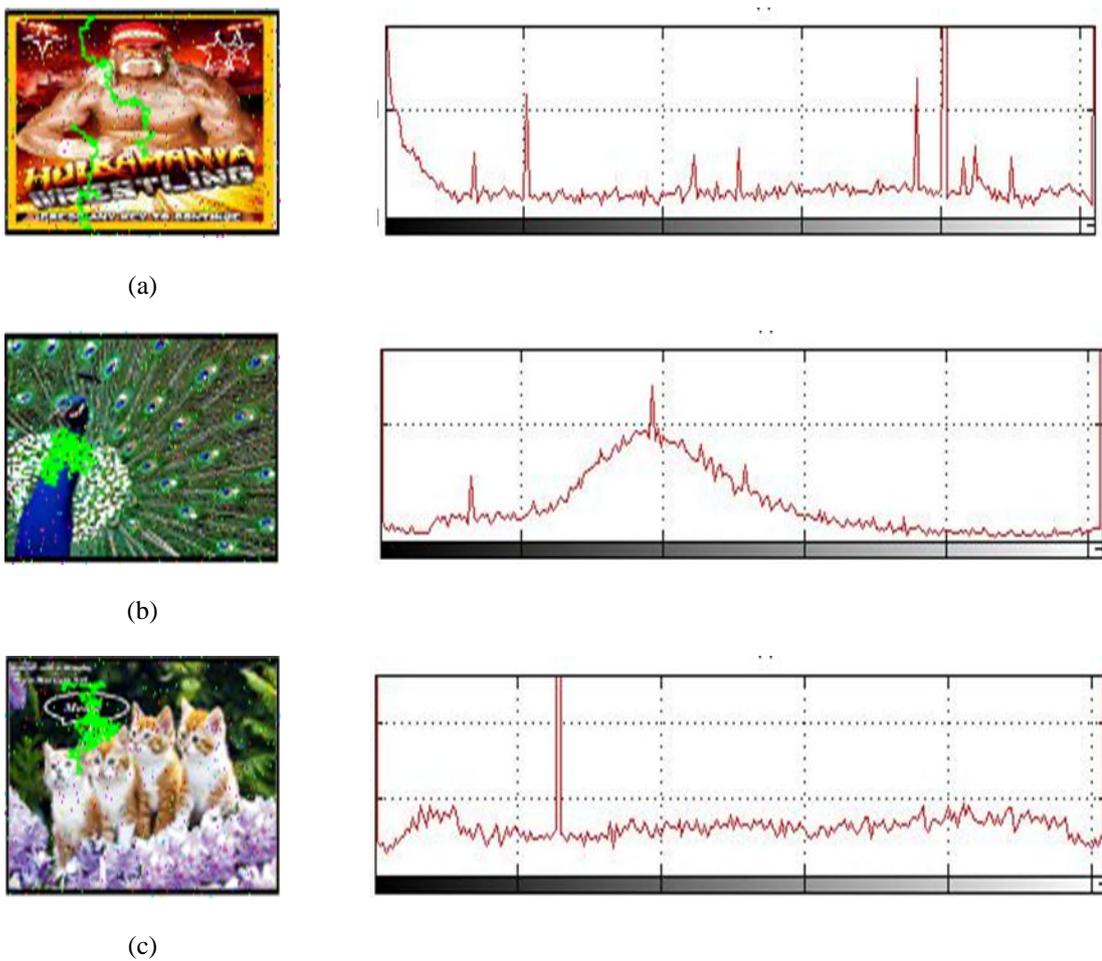


Figure 6. Images (a, b, and c) With Locations under Salt and Pepper Noise

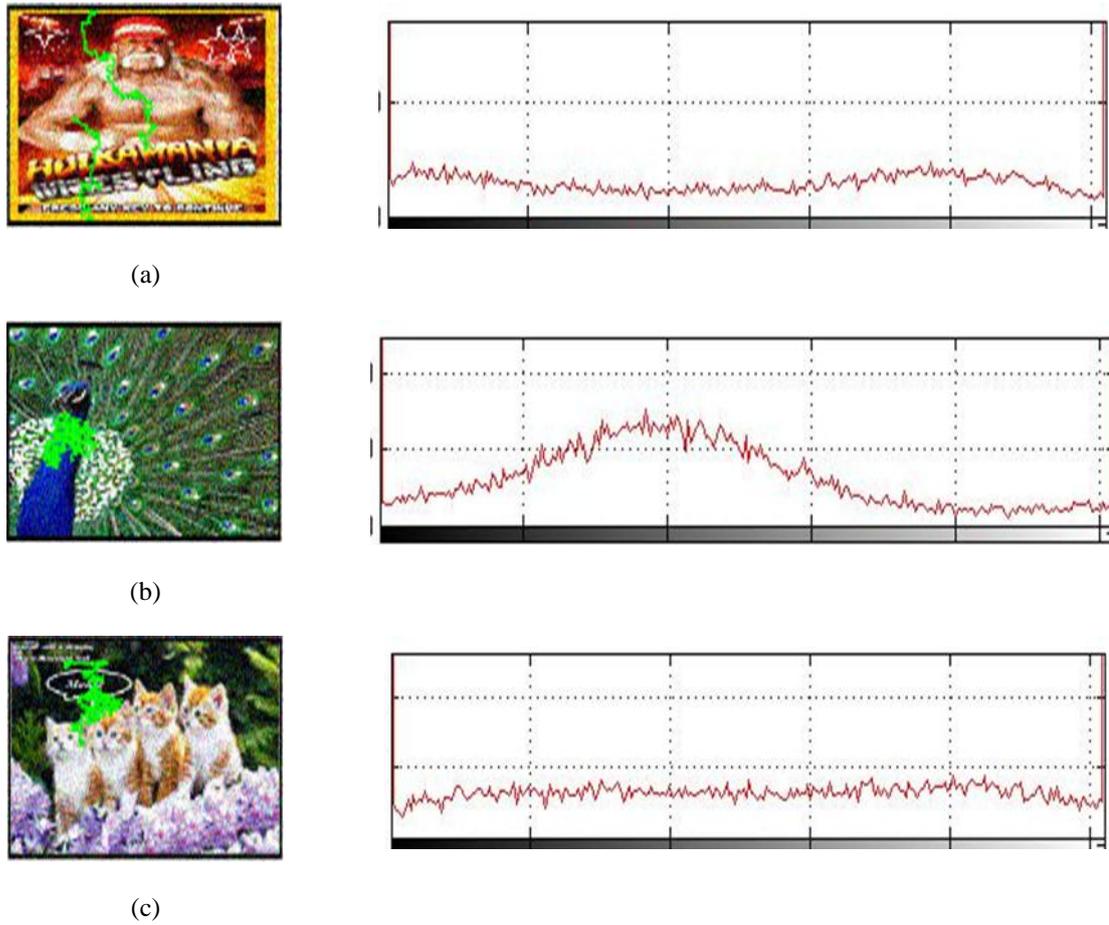


Figure 7. Images (a, b, and c) With Locations under Gaussian Noise

Figure 8 show the final Images after Hiding Process

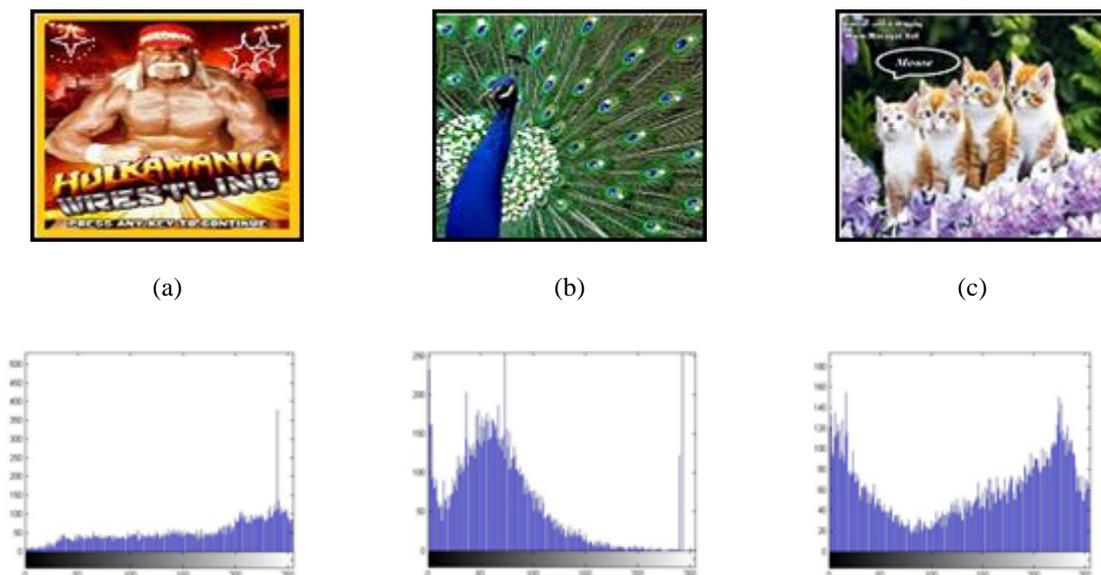


Figure 8. Final Images after Hiding Process

The relationship between number of iterations and required time for each iteration when using the developed PSO algorithm is shown in Table 3.

Table 3. Iteration and Time for Dev. - PSO Algorithm

Iteration No.	Time in sec.
1	3

5. QUALITY METRICS RESULTS

The following figure shows all stego images that contains secret information that embedded based on developed PSO algorithm using LSB technique as shown below, while the quality metric such as MSE and PSNR are computed for the original and cover images as shown at Figure 4(a), Figure 4(c) and Figure 4(e). Values of images quality assessment are shown in Table 4. Furthermore, the stego images exposed to intended attack such as salt and pepper that illustrated in Figure 9, while the resultant stego images under Gaussian noise shows in Figure 10. The objective measurement based on the value of PSNR and Mean Square Error (MSE) illustrated in Table 4.

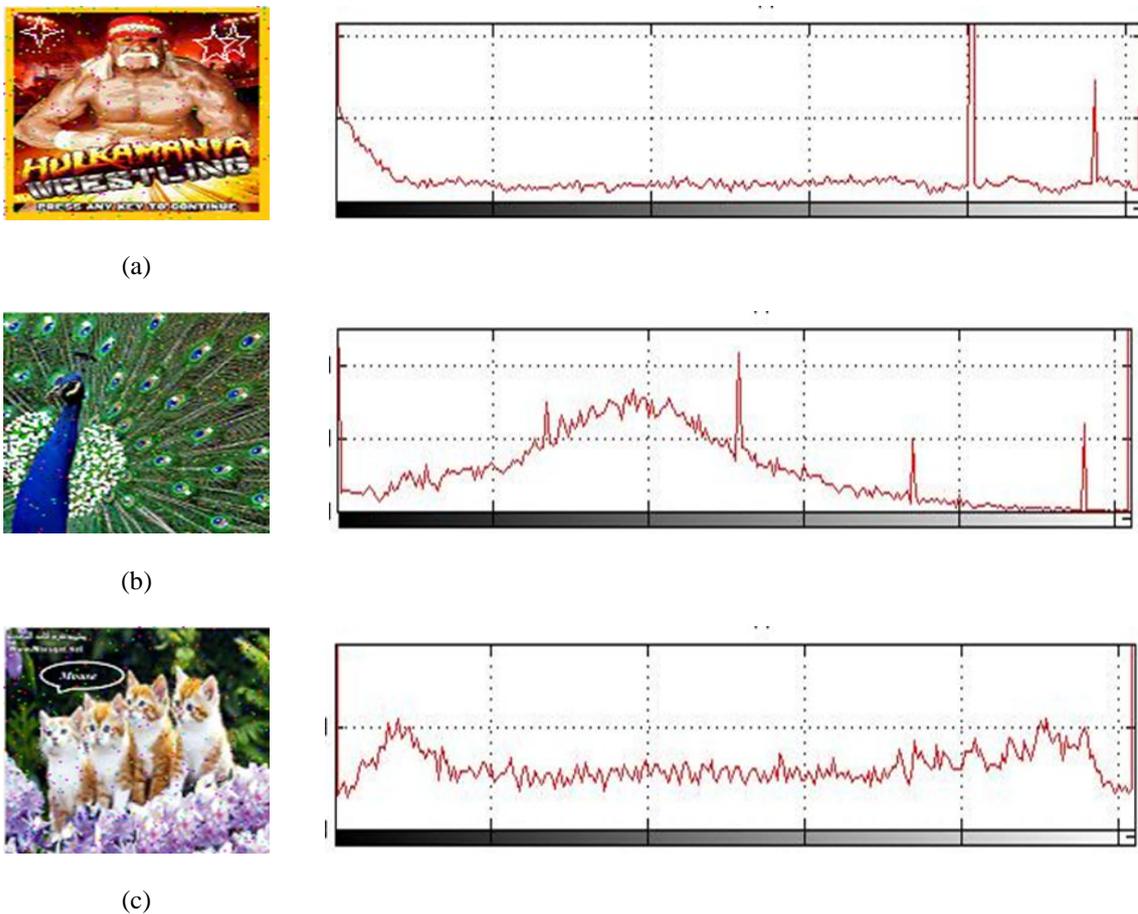


Figure 9. Stego Images (a, b, and c) Under Salt and Pepper Noise

Table 4. Values of Images Quality Assessment

Stego Image	Red		Green		Blue	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
A	0.00659	44.22	0.01749	44.66	0.00989	44.87
B	0.00711	43.60	0.01661	44.23	0.01869	44.45
C	0.00677	42.93	0.02553	43.65	0.02041	43.97

From the results that illustrated in the table above, each color image has three sub-bands know as Red, Green, and Blue, Furthermore, the blue sub-band is less sensitive for any attack, while the red or green sub-bands are more sensitive to any intended attack or mild-processing. Our proposed method hid a secret message in three sub-bands color at the same time to increase the security for the developed PSO and to make the stego image able to survive the secret message from the intended attack, if any sub-band destroyed the secret message can be extracted from other sub-band, while the most methods that based on PSO are used gray image to avoid the distortion that produced after the embedding stage in the quality for the cover image.

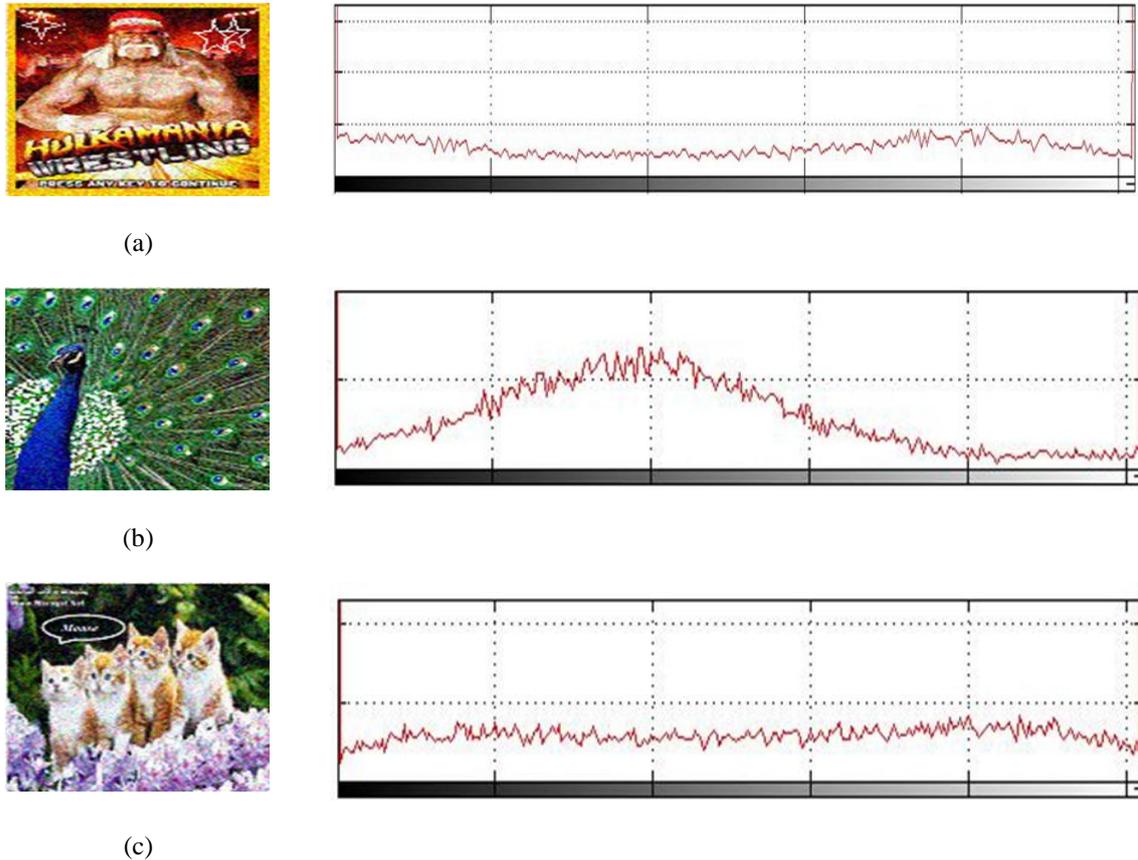


Figure 10. Stego Image (a, b, and c) Under Gaussian Noise

Finally our proposed method compared with other methods that utilized the propertise of PSO and based on LSB, the value of PSNR, MSE befor any intended attack computed according to the blue-sub band color and illustrated in the following table, and Figure 11 shows the curve chart according to Table 5, while the performance for PSNR, MSE after intended attack such as: after salt & pepper noise, Gaussian noise illustrated in the Table 6, and Figure 12 shows the curve chart according to Table 6.

Table 5. Compare the Proposed Method with Other Method before Intended Attack

Stego Image	A		B		C	
	PSNR \ dB	MSE	PSNR \ dB	MSE	PSNR \ dB	MSE
Method 8	43.24	0.06611	43.18	0.09110	42.89	0.09995
Method 9	38.75	0.08420	37.92	0.07994	35.99	0.06993
Method 10	44.90	0.09242	44.78	0.08003	43.32	0.02812
Our Proposed Method	44.87	0.00989	44.45	0.01869	43.97	0.02041

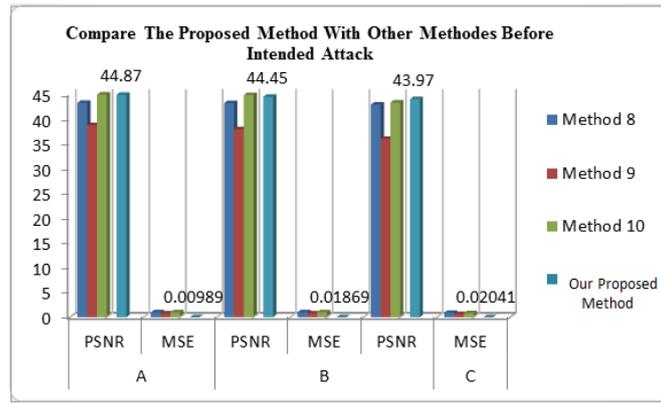


Figure 11. The Value of PSNR, MSE Befor Intended Attack

Table 6. Comparing the proposed method with others after intended attacks

Stego Attacks	A				B				C			
	Salt&Pepper \ dB		Gaussian \ dB		Salt&Pepper \ dB		Gaussian \ dB		Salt&Pepper \ dB		Gaussian \ dB	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Method 8	37.99	0.3421	38.20	0.9531	38.51	0.6643	39.73	0.8815	36.99	0.7743	38.60	0.8001
Method 9	31.90	1.9997	33.60	0.3877	31.61	1.9003	32.99	0.9694	30.38	0.3399	31.81	0.2003
Method 10	37.16	0.7783	38.90	0.9958	48.60	0.2015	40.11	0.1811	37.33	0.8855	38.85	0.9913
Our Proposed Method	37.09	0.6899	38.66	0.9147	48.48	0.2289	40.01	0.8813	37.31	0.7865	38.96	0.8944

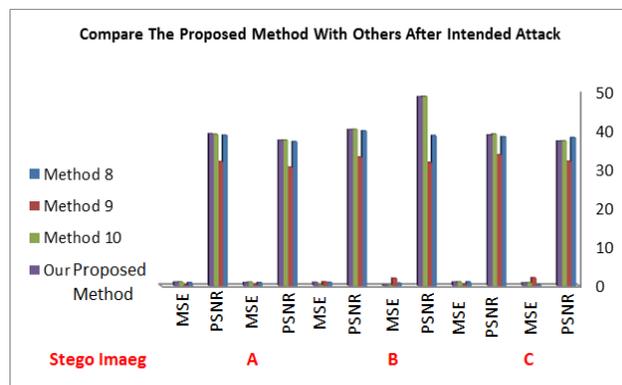


Figure 12. The Value of PSNR and MSE after Intended Attacks

5. CONCLUSIONS

The PSO algorithm is developed to determine an optimal solution from search space of problem. After using the developed PSO algorithm on three images, notice these images does not affected by a prominent distortion or noising that applied over the stego image on it as shown in Figure 9 and Figure 10, the experimental results of the developed PSO algorithm and hiding process by using LSB technique are accepted and good since the quality of these images is good as shown in Table 4 that describes the relationship between PSNR and MSE. Furthermore, the stego image results after exposed it to several types of intended attacks tabled and compared with other method. The indicates that the developed PSO algorithm has good performance and high efficient in hiding a secret message in the digital color images depending on the value of PSNR and MSE that illustrated in Table 5 and Table 6. The selecting accuracy of the best location when using the developed PSO algorithm is shown in Table 2 and Figure 5, notice that there are no

information missing, this result indicates to level of accuracy in selecting the best location, also the selected locations are almost serially, and this give us pointer that the developed PSO algorithm is fast. If the bird has predetermined for starting point then all birds follows it, patchwork technique used in the proposed method to hide a secret message inside the cover image in spatial domain in the three color sub-band at the same time to make able to survive the stego image from intended or un-intended attack, therefore if one of an sub-band distroed, the secret message can be extracted from other sub-ban. Our proposed method take three samples during the testing process and take into consideration image texture, and the diffirents results that tabled shows that the proposd method has ability to hide a secret message inside the cover image under spatial domain by using LSB technique (LSB substitution).

REFERENCES

- [1] Nidhi Sethi and Sandip Vijay, "A New Cryptographic Strategy for Digital Images", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 4, No. 3, pp. 456~462, June 2014.
- [2] P. Kumar and V. K. Sharma, "Information security based on steganography and cryptography techniques: A review" *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 10, October 2014.
- [3] R. Gupta, S. Gupta, and A. Singhal, "Importance and techniques of Information Hiding," *International Journal of Computer Trend and Technolog (IJCTT)* - volume 9 number 5- Mar 2014
- [4] T. Morkel, J.H.P Eloff and M. S. Olivier, "An Overview of Image Steganography" Information and Computer Security Architecture (ICSA), Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.
- [5] M. Junej, P.S. Sandhu, "Improved information security using Steganography and Image Segmentation during transmission", Computer Science and Engineering Department, Rayat and Bahra Institute of Engineering and Technology (RBIEBT), Sahauran (Punjab), India
- [6] D. Bhowmik, "Robust Watermarking Techniques For Scalable Coded Image And Video", PhD thesis, Department of Electronic and Electrical Engineering, The University of Sheffield, p.13-34, 2010.
- [7] S. Patel, A. Katharotiya, M. Goyani, "A Survey on Digital Video Watermarking", *IJCTA* | NOV-DEC 2011.
- [8] Champakamala B.S, Padmini. K, Radhika D.K., "Least Significant Bit algorithm for image steganography", *International Journal of Advanced Computer Technology (IJACT)*, Department of TCE, Don Bosco Institute of Technology, Bangalore, India, ISSN:2319-7900
- [9] Chang CC, Chan CS, Fan YH. Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels. *Pattern Recognit* 2006;39:1155–213.
- [10] Bajaj R, Bedi P, Pal SK. "Best hiding capacity scheme for variable length messages using particle swarm optimization" In: Proc SEMCCO 2010. LNCS 6466. p. 237–44.
- [11] Bedi P, Bansal R, Sehgal P, "Using PSO in image hiding scheme based on LSB substitution", In: Proc international conference on advances in computing and communications (ACC 2011); CCIS 192; 2011. p. 259–68.
- [12] Kennedy J. and Eberhart R. C., "*Particle Swarm Optimization*", Proceedings of the 1995 IEEE International Conference on Neural Networks, volume 4, PP: 1942–1948, Australia, IEEE Service Center, 1995.
- [13] N. Ramesh Raju and P. Linga Reddy, "Robustness Study of Fractional Order PID Controller Optimized by Particle Swarm Optimization in AVR System", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 6, No. 5, pp. 2033~2040, October 2016.
- [14] Ismail Khalil Ali, "Intelligent Cryptanalysis Tool Using Particle Swarm Optimization", Ph.D. Thesis, University of Technology, Department of Computer Science, 2009.
- [15] Nor Azlina Ab Aziz, Zuwairie Ibrahim, Marizan Mubin, Sophan Wahyudi Nawawi and Nor Hidayati Abdul Aziz, "Transitional Particle Swarm Optimization", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, No. 3, pp. 1611~1619, June 2017.