

Hiding Information using Secret Sharing Scheme Based on Gene Expression Programming

Marghny H. Mohamed¹, Mahmoud A. Mofaddel², Tarek Y. Abd El-Naser^{3,*}.

¹ Dep. of Computer Science, Faculty of Computers and Information Systems, Assuit University, Assuit, Egypt.

² Dep. of Computer Science and Mathematics, Faculty of Science, Sohag University, Sohag, Egypt.

³ New Cairo Academy, Dep. of Computer Science, Cairo, Egypt.

Received: 22 Nov. 2017, Revised: 22 Dec. 2017, Accepted: 26 Dec. 2017.

Published online: 1 Jan. 2018.

Abstract: Undoubtedly, communication process is considered as one of the most important means which contributed in the technological development. Transfer the data between people rapidly and accurately has been appeared due to the development of the internet. However, these data may be very confidential and important and may be also found by the hackers who can steal, modify and misuse it. Therefore, it is important to transfer the data with ultimate security. Steganography is one of the techniques, which is designed to deal with such type of problems. In this paper, images have been used as a cover file, because of the difficulty of doubt of presence of any hidden data. Gene expression programming (GEP) algorithm has been used with LSB technique (it is based on replacing the LSBs of cover-image with secret-image bits giving a stego-image) for hiding data and secret-sharing scheme for protect it. We have been presented a secret-sharing scheme based on which a user divides the secret-image vertically into parts such that each part is embedded randomly in one cover. Only authorized of parties can reconstruct the secret-image by comparing the variance between the left edges of the selected part of secret-image with the right edges of the other parts of secret-image and vice versa. The results of the comparison guide us to obtain the parts again of the secret image. The hiding of data needs a powerful and sophisticated method such as GEP where it chooses the best places to hide the secret-image in the cover-image through a set of processes to reduce attention of presence of confidential data by reducing the distortion and also besides hiding data we need strong protection method such as the SSC method where preventing hackers From easy access to the complete secret-image.

Keywords: Steganography, Data hiding, Parallel Method, Security Method, LSB, Secret Sharing Scheme, Gene Expression Programming(GEP).

1 Introduction

Today, communication networks are the backbone of the knowledge world, which is the mean of exchanging information. Communication have evolved according to the evolution of civilizations, this information may be text, image, audio, and video. Technological development and the information revolution have created a digital society that relies heavily on the transmission of information over the Internet, and it has been necessary to develop information hiding techniques, to protect from unauthorized persons to create a secure electronic environment. There are two ways to keep data outreach. The first way is the encryption in which data are converted to meaningless information, but displayed to any one, so encryption has not

achieved the desired objectives enough to secure confidential information [16,17,18,19,20,21]. The second way is data hiding. Therefore, there is an urgent needing to look for techniques to hide the secret information. LSB is one of the most famous techniques which it makes modifications to the cover image by simply substituting each bit of secret-image by the last bit of each byte of the cover image and the secret image is hidden in such a way that the observer cannot detect any distortion[23] in the original image. Hence, researchers have resorted to develop algorithms to support and improve this technique such as the Genetic algorithm, gene algorithm expression programming (GEP) algorithm, etc. [11,12,13,14,15]. After hiding the data it needs a protection, here we will protect the information using the SSC technique that relies on

*Corresponding author e-mail: Tarekyahia2000@gmail.com

splitting the secret image to parts and embedding it in more than one cover, the main example of this technique was described in [1,2].

(SSC) refers to distribute [22] secret message among group t of n participants, the secret-image can be reconstructed if a sufficient number of shares are combined together, the SSC method works to protect the secret image, so if a part fell into the hands of unauthorized people, it would have no meaning and not understood.

Many of techniques have been proposed using (SSC). Lin and Tsai [3] proposed method of secret image sharing with steganography and authentication, they depended on Polynomial interpolation technique based on image sharing, but when they reconstruct the secret-image the little distortion of secret-image may happen. Yuan in [4] proposed a method to hide secret bits among textured regions with different covers. A multi-secret image sharing scheme has been proposed in [5], it shares n secret images among n shared images. In this technique, there are n stego-images are used together to recover n parts of secret images, if there are any losing in stego images it will not be able to recover the secret image. Nasrollah proposed algorithm depends on hierarchical threshold secret image sharing (HTSIS) scheme for sharing a secret image among a set of participants with different levels of authority has been proposed. [6].

In this work we proposed a method to split the secret image to vertical parts, because in most languages in the world the typing direction is horizontal from left-to-right and right-to-left, so if one part fall in hand of unauthorized person it will be meaningless and not understandable [14] after splitting. Each part will be embedded randomly in each cover by using the LSB technology supported by the gene expression programming (GEP) algorithm which selects the best possible places to hide data in the cover-image to get the highest quality and the least distortion of the stego-image, then send it to the other side, and the idea of combining the parts of the secret image is based on measuring the variance between the edges of the parts of secret image. This distribution gives more protection to the secret-image.

The rest of this paper include: in section 2 steganography using LSB Substitution in section 3 explaining the idea of Parallel hiding method (secret sharing scheme), in section 4 explaining of gene expression programming algorithm, in section 5 the proposed algorithm with shared scheme method, in section 6 Experimental results.

2 Hiding Data Using Simple LSB Substitution Method

In principle, hiding data using simple LSB substitution method is described as: Let C is the original 8-bit gray scale cover-image of $M_c \times N_c$ pixels, represented as:

$$c = \{X_{ij} | 0 \leq i \leq M_c, 0 \leq j \leq N_c, X_{ij} \in \{0, 1, 2, \dots, 255\}\}, \quad (1)$$

M is the n -bit secret message represented by:

$$M = \{m_i | 0 \leq i \leq n, m_i \in \{0, 1\}\}, \quad (2)$$

suppose that the n -bit secret message M is to be embedded into the k -rightmost LSBs of the cover-image C .

Firstly the secret message M is rearranged to form a k -bit virtual image M' , represented as:

$$m' = \{m'_i | 0 \leq i \leq n', m_i \in \{0, 1, \dots, 2^k - 1\}\}, \quad (3)$$

where $n' = M_c \times N_c$. The mapping between the n -bit secret message $M = \{m_i\}$ and the embedded message $M' = \{m'_i\}$ can be defined as follows:

$$m'_i = \sum_{j=0}^{k-1} m_i \times k + j \times 2^{k-1-j}. \quad (4)$$

We get the sub-set of n' pixels $\{x_1, x_2, \dots, x_n\}$ of cover-image C on series. Then, the k -LSBs of x_i will be replaced by m'_i , mathematically the pixel value x_i is represented by:

$$X'_i = x_i - x_i \bmod 2^k + m'_i. \quad (5)$$

And to extract the embedded message using same sequences the set of pixels $\{x'_1, x'_2, \dots, x'_n\}$, the pixels which contain secret message bit are selected from stego-image and k -rightmost LSBs are extracted and put on series of bits of secret message [13].

Mathematically, the embedded message bits m'_i can be recovered by $m'_i = X'_i \bmod 2^k$.

In addition, the quality of the stego-image using LSB technique may be Unacceptable and it is possible to attract attention, to solve that problem we divide the secret image into smaller parts using (SSC) method, to achieve high quality and provide higher protection for stego-image.

3 Secret Sharing Scheme Method

The idea of Secret sharing Scheme Method is to distribute the secret image among group t of participant's p each one is allocated the share of the secret part. The secret image can be reconstructed only when all shares are combined, this case is called sufficient combination, in secret sharing scheme there is one main player who gives the n player the shares, players can get there shares if conditions are achieved, secret sharing scheme called (t, n) -threshold scheme, t group of players, n number of players, so any group of t can reconstruct the secret image, but no group

fewer than t .

4 Gene Expression Programming

GEP is an algorithm that represents relations between variables in sets of data and then design models to explain the whole image about these relations. GEP algorithm is one of the evolutionary algorithms that solves various problems like simulating networks of neurons and others simulating evolution through natural selection [8,24].

Gene expression programming (GEP) is like genetic algorithms (GAs) and genetic programming (GP), a genetic algorithm as it uses populations of individuals, selects them according to fitness and introduces genetic variation using one or more genetic operators. The main difference between three algorithms based on nature of each individual with (GAs), the individuals are arranged in strings with fixed length (chromosomes) and with GP individuals are arranged in nonlinear objects of different sizes and shapes (parse trees) and with GEP the individuals are arranged in strings with fixed length then are expressed as nonlinear objects with different sizes and shapes [9].

There are two main factors in GEP (chromosomes) and (expression tree), as shown in Fig.1.

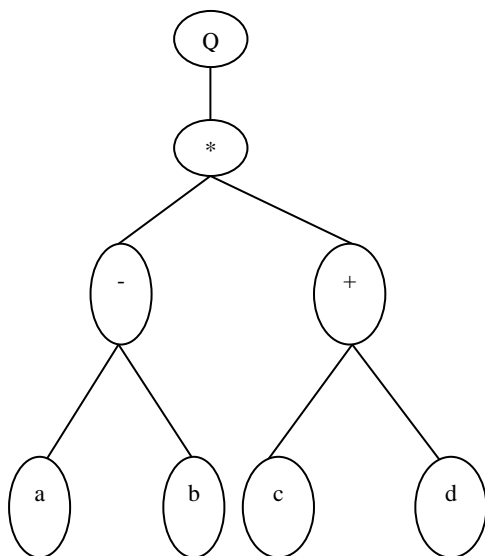


Figure 1. Expression Trees of $\sqrt{(a-b)(c+d)}$

Where “Q” represents the square root function, this type of diagram representation is called the **phenotype** in GEP. And the **genotype** can be easily inferred from the phenotype as follows:

0	1	2	3	4	5	6	7
Q	*	-	+	a	b	c	d

The GEP algorithm starts with creating random generation of the chromosome each chromosome is evaluated by

fitness function, then select the best chromosomes and they reproduce with some (modifications) to get new offspring with new traits, the process will be repeated again and again until specified number of generations or when you get the best solution.

4.1 Encoding

Gene expression programming algorithm is implemented over a number of steps initially; the data should be encoded to the form which the algorithm works on it, and each formatting according to the nature of the problem.

To design the chromosomes there is a technique called Multigene families (MGFs), These MGFs consist of clusters of related genes and each gene has the length $g=1$ and exclusively composed of one terminal $t=1$. This kind of genes we get it when the length of head h equal zero. Where the terminal t evaluated by the equation:

$$T = (n-1)h + 1 \quad (11)$$

And n denotes the largest argument of the functions used in the gene's head.

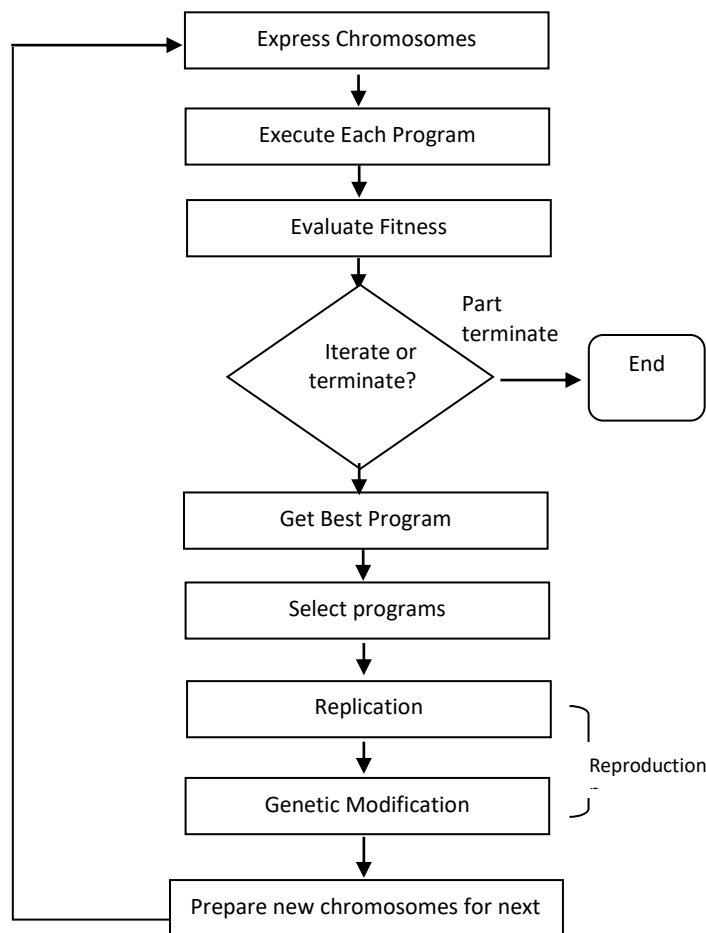


Figure 2. The flowchart of a GEP [8].

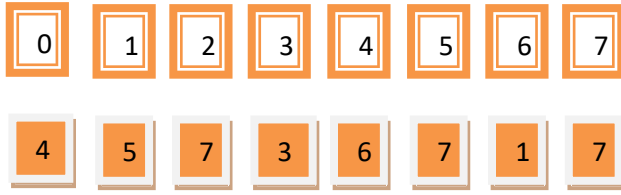


Figure 3. A GEP chromosome composed of one MGF with 8 genes.

4.2 Initial population

We get chromosomes of individuals of an initial population are generated randomly by some functions, these initial individual are the first set they are not used in any environment and not suitable solutions.

4.3 Fitness Function

The fitness functions measure the quality of the current solution, the fitness function is defined in this work as the mean square error MSE; calculate differences between the original cover image and the stego-image [7].

The role of fitness function is to achieve the minimum distortion and high capacity of stego image.

The measurement of high capacity and minimum distortion can be evaluated by maximum PSNR: which means minimum MSE, so that our goal is to select a solution with maximum PSNR values. The PSNR Is estimated in decibel (dB), defined as:

$$\text{PSNR} = 10 * \log_{10} \left(\frac{255*255}{\text{MSE}} \right), \quad (6)$$

and MSE is defined as:

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (x_{ij} - y_{ij}), \quad (7)$$

where, x_{ij} refers to the original pixel value, and y_{ij} refers to the processed pixel value, and m and n denote the width and height of the image respectively.

4.4 Selection (Roulette - Wheel)

In GEP individuals are chosen depending on fitness by using roulette-wheel sampling. This means that each individual has a slice of the roulette-wheel, which is fit to its fitness then, the roulette is spun as many times as there are individuals in the population so that the population size

is maintained from generation to generation. Obviously, the bigger the slice the higher the probability of being selected [8, 10].

4.5 Inversion Operator

The inversion operator is the most efficient combinatorial specific genetic operators. It randomly selects the chromosome, the multi gene family to be modified, the inversion points in the MGF, then inverts the sequence between the two selected points.

4.6 Elitism Selection

Allow the fittest chromosome to pass to next generation without being altered by a genetic operator(s) [10].

4.7 Reproduction

In the cloning process, the second generation has been created from the first generation that underwent selection processes (the roulette wheel) coupled with elitism, for each new solution to be produced. This process continues on the number of times is that was specified. Indeed, the average fitness will be increased by this operation for the population. Although inversion is the only combinatorial-specific genetic operators selected points. Where each chromosome can only be modified once by this operator [10].

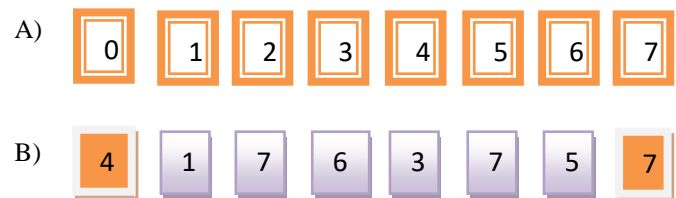


Figure 4. Gene 1 and 6 are randomly chosen in the chromosome, of MGFs as the inversion points.

Inversion operation is applied on a selected chromosome, not all and according to the inversion percentage [10].

5 Proposed Algorithm

Our proposed method has two phases, as follows:

First phase: The secret image is hidden randomly in more than one cover image with two basic conditions first, the secret image must be divided into equal vertical parts in length and width. Second the number of cover images must be equal to the number of parts of the secret image that has been previously divided.

For example

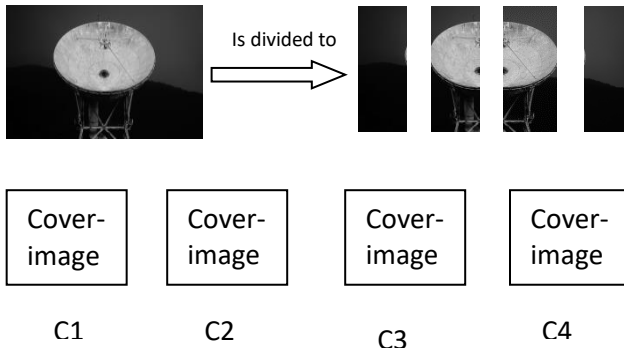


Figure 5. dividing the secret image into four parts each part has one cover-image.

the secret-image S_i is divided into parts $s_1, s_2, s_3, \dots, s_n$, with multi cover-images $c_1, c_2, c_3, \dots, c_n$. If the number of parts of a split secret image is two, you should use 2 cover images and if the number of divided parts is 4, we need 4 cover images and so on. The embedding process is done by using the LSB technology supported by the gene expression programming (GEP) algorithm. (GEP) is Looking for the best possible embedding places in the cover image, (GEP) has multiple parameters are used for achieving the least distortion and higher quality, at the ending of embedding process we get the stego-image.

The operation of ciphering data of each secret part S_i with C_i cover-image is obtained by bitwise XOR operating between them as: $\text{Cipher} = C_i \oplus S_i$. Then all parts are ready to be sent to the other end [13].

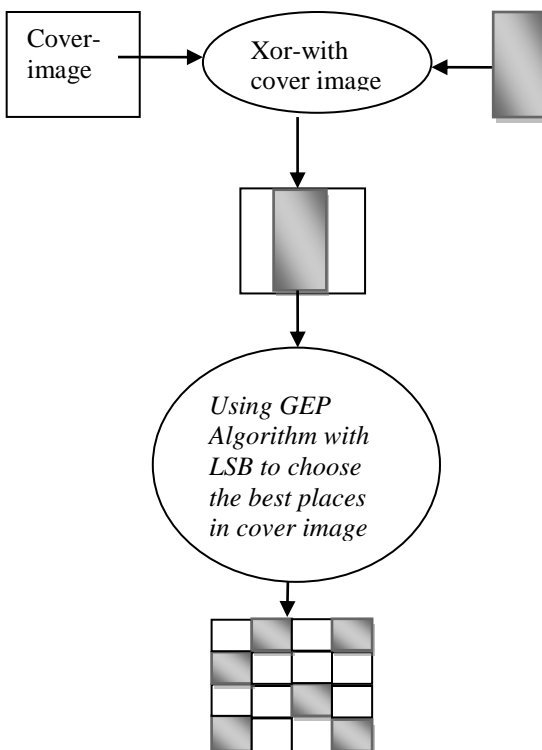


Figure 6. Processing of hiding one part of secret-image
Second phase:

To get secret parts which are randomly distributed in multi cover images:

- Extract the position of data from K-LSB of each stego $\text{stego}_1, \text{stego}_2, \dots, \text{stego}_n$, this done by

$$\text{Position} = \text{extract}(\text{stego}_1, K). \quad (8)$$

- Ciphered data from each stego-image is obtained from the position of data

$$\text{Cipher} = \text{key}(\text{position}). \quad (9)$$

- Operation of deciphering: to get the secret part S_i through Xoring cipher-data with C_i cover-image

$$S_i = \text{cipher } C_i. \quad (10)$$

- Final step collect the parts using the variance (variance of image's edges through the difference of pixels at edges of each secret-part), as follows.

After extracting all parts of secret-image s_1, s_2, s_3, s_4 :

We will focus on the left and right edges of each part of the secret image that we want to collect.

Table 1. Lpx last pixel, 1 part 1, L left, R right

Lpx1 L				Lpx1 R
Lpx1 L				Lpx1 R
Lpx1 L				Lpx1 R
Lpx1 L				Lpx1 R

Then we select random part of secret image and through this part the left edges and right edges are compared to the rest of the parts and the contrast is calculated between last pixels at edge of selected-part and last pixels at edge of rest parts, for example if we have four secret parts, we consider the selected part is number 1:

Get difference between the pixels at right side of selected part with the pixels at left side of rest parts as:

$$r1 = \text{Lpx}2_L, -\text{Lpx}1_r$$

$$r2 = \text{Lpx}3_L, -\text{Lpx}1_r$$

$$r3 = \text{Lpx}4_L, -\text{Lpx}1_r$$

and the vice versa: Get difference between the pixels at left side of selected part with the pixels at right side of rest parts as:

$$r4 = \text{Lpx}2_r, -\text{Lpx}1_L$$

$$r5 = \text{Lpx}3_r, -\text{Lpx}1_L$$

$$r6 = \text{Lpx}4_r, -\text{Lpx}1_L$$

in case of four parts we will get six results, ($r1, r2, r3, r4, r5, r6$). The best result is the lowest value, if the lowest

value was r_4 , then
 $r_4 = L_{px2r} - L_{px1L}$

Here we will merge the left side of selected part with the right side of part number 2. After merging we will get 3 parts, and then we repeat the previous operation until get the whole secret image.

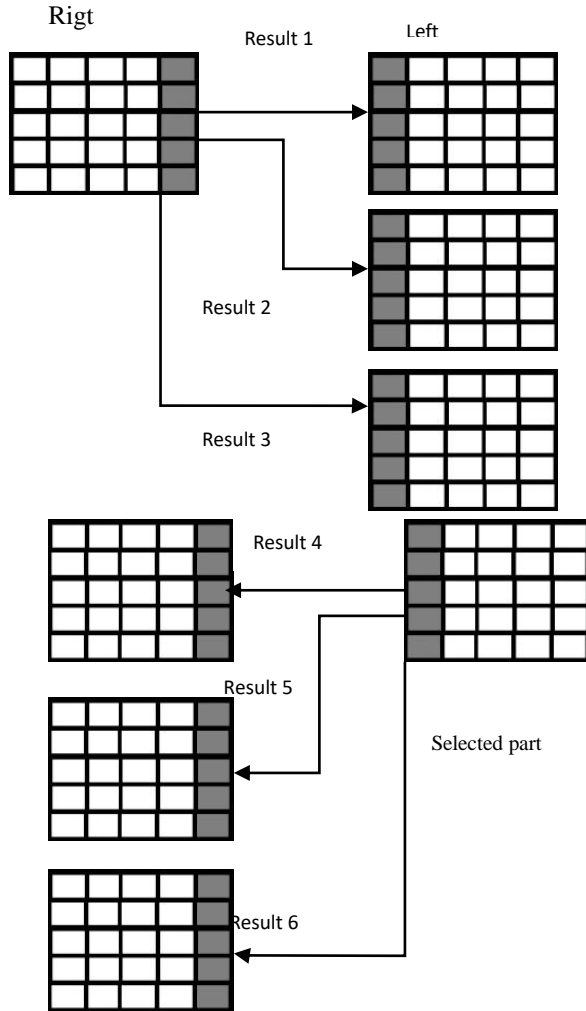


Figure 7. Comparing between parts

In case of two values of results are equal here we will select the last two pixels at edges of parts, and get the summation then calculate the difference as previous as shown:

Ex: If the value of r_3 equals the value of r_4 :

$$r_3 = \sum_{i=1}^2 (L_{px1R})i - \sum_{i=1}^2 (L_{px4L})i, \quad (11)$$

$$r_4 = \sum_{i=1}^2 (L_{px1L})i - \sum_{i=1}^2 (L_{px2R})i. \quad (12)$$

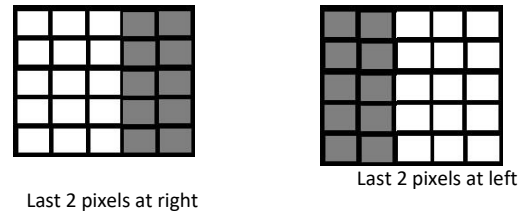


Figure 8. get next pixel to calculate the variance again

If the values of r_3 , r_4 are equal again we repeat the previous operation using last three pixels and so on.

6 Results and Discussions

Twelve experiments with $k = 1, 2$, and 4 LSB Insertion, and 2, 4, 8, 16 covers have been implemented using the proposed algorithm; the parameters of GEP are as follows:

- Maximum of generation = 50,
- Population size = 100,
- Inversion rate = 0.3,
- No. of MGFs=1,
- No. of genes per MGF=2, 4, 16 for $k=1$ -LSB, 2-LSB and 4-LSB insertion respectively.

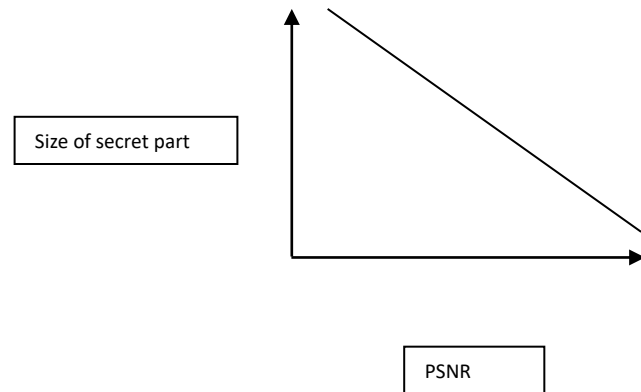


Figure 9. Inversely proportional between the size of secret part and the PSNR

Table 2. the multi cover images and the secret image with different sizes.


				
Babbon	Lena	Boat	cameraman	copule
				
Girl	House	Lake	man	Pepper
				
Birds	Fruits	Car	fish	Cat
				
wife	256 X 128 pixels Secret image	256 X 256 pixels Secret image	512X 128 pixels Secret image	

Table 3. Compare between proposed scheme and other methods (Marghny et al. method And Nasrollah et al. method).

Cover image	Marghny et al. method			Nasrollah et al. method	Proposed Method		
	k-lsb	Simple-LSB	Optimal-LSB	Average Psnr With 2 –k lsb	k-lsb	Simple-LSB Average Psnr	Optimal-LSB Average Psnr
Baboon	1	51.1380	51.1723	51.23	1-k 2 covers Baboon - Lena	54.1616	53.6539
	2	44.0526	44.2475				
	3	-	-		2-k 2 covers Baboon - Lena	46.0193	51.1417
	4	31.4595	32.5326				
				51.01	4-k 2covers Baboon - Lena	33.24525	48.13075
Lena	1	51.1471	51.1681				
	2	44.0656	44.3714				
	3	-	-				
	4	31.4258	32.2161				
Boat	-			51.93	1-k 4 covers Baboon – Lena Boat-cameraman	57.15845	57.15958
Camera men	-			50.93	2-k 4 covers Baboon – Lena Boat-cameraman	49.03375	54.16738
Couple	-			50.90	4-k 4 covers Baboon – Lena Boat-cameraman	36.30575	51.14205
Girl	-			52.29	1-k 8 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake	60.275325	60.16995
House	-			51.11	2-k 8 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake	51.1904875	57.13511
Lake	-			51.11	4k 8 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake	39.34525	54.1082
Man	-			51.13	1-k 16 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake- Man-Peppers-Wife-Cat- Fruits-Birds-Car-Fish	63.152	62.98271875
Peppers	-			51.06	2-k 16 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake- Man-Peppers-Wife-Cat- Fruits-Birds-Car-Fish	55.8259875	60.24425813
Wife – Cat – Fruits- Birds- Car- Fish	-			-	4-k 16 covers Baboon – Lena Boat-cameraman Couple-Girl-House-Lake- Man-Peppers-Wife-Cat- Fruits-Birds-Car-Fish	43.2286875	57.28604375

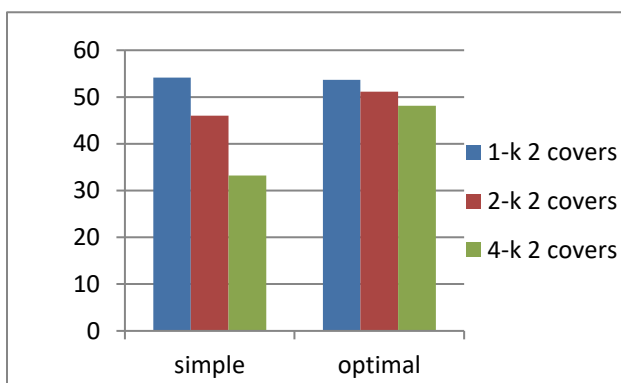


Figure 10. Comparing between simple LSB and optimal LSB with 2 cover-images.

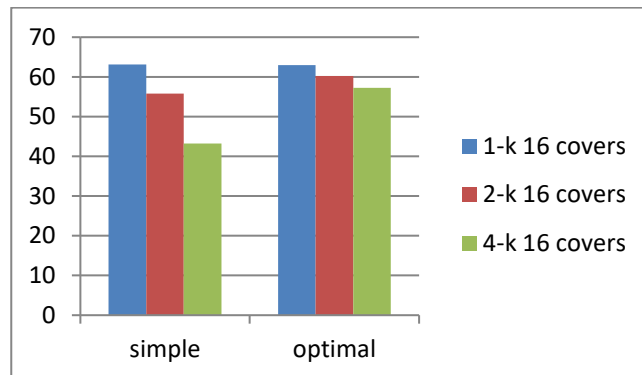


Figure 13. Comparing between simple LSB and optimal LSB with 16 cover-images.

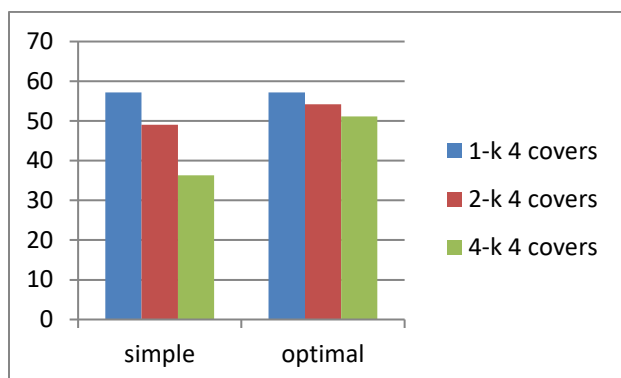


Figure 11. Comparing between simple LSB and optimal LSB with 4 cover-images.

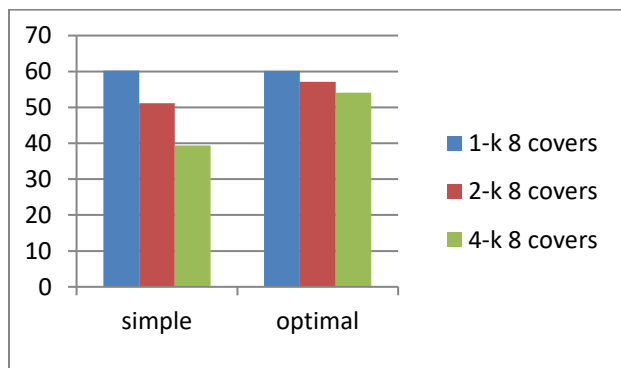


Figure 12. Comparing between simple LSB and optimal LSB with 8cover-images.

7 Conclusions

We notice that when the size of secret part decreases the PSNR of stego-image increase there is inversely proportional relation between them.

References

- [1] A. Shamir., "How to share a secret, Communications of the Association for Computing Machinery" . , **22(11)** 612–613, 1979.
- [2] G.R. Blakley., "Safeguarding cryptographic keys", in Proceedings of the National Computer Conference". , **48**, 313–317,1979.
- [3] C.-C. Lin, W.-H.Tsai., "Secret image sharing with steganography and authentication", J. Syst. Software . , **73 (3)** ,405–414, 2004.
- [4] Hai-Dong Yuan., " Secret sharing with multi-cover adaptive steganography", Information Sciences . , **254** ,197–212,2014.
- [5] Chien-Chang Chen, Wei-Jie Wu., "A secure Boolean-based multi secret image sharing scheme", The Journal of Systems and Software. , **92**, 107–114, 2014.
- [6] NasrollahPakniat, et MahnazNoroozi, et ZibaEslami., " Secret image sharing scheme with hierarchical threshold access structure." ELSEVIER . , **25**, 1093-1101, 2014.
- [7] Ferreira, Cândida., "Function Finding and the Creation of Numerical Constants in Gene Expression Programming" 7th Online World Conference on Soft Computing in Industrial Applications, 2002.
- [8] Ferreira, Cândida., "Gene Expression Programming in Problem Solving." WSC6 tutorial, 2001.
- [9] Ferreira, Cândida., " Gene Expression Programming, Mathematical Modeling by an Artificial Intelligence", 2nd Edn. Berlin Heidelberg: Springer-Verlag, 2006.
- [10] Ferreira, Cândida., "Combinatorial Optimization by Gene Expression Programming: Inversion Revisited." In J. M. Santos and A.Zapico, eds, Proceedings of the Argentine Symposium on Artificial Intelligence. ,160-174,2002.

- [11] H. Marghny, Mohamed, M. N. Al-Aidroos, and A. M. Bamatraf, "Data hiding technique based on LSB matching towards high imperceptibility," *MIS Review*, 57-69, 2012.
- [12] M. Mohamed, F. Al-Afari, and M. A. Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation," *Int. Arab J. e-Technol.*, **2**, 11-17, 2011.
- [13] M. H. Mohamed and H. I. Abul-Kasim, "Data Hiding by LSB Substitution using Gene Expression Programming," *extraction.*, **10**, p. 5, 2012.
- [14] M. H. Marghny, S. E. El-Gendi, F. Al-Afari and M. El-Melegy, "Steganography for Secure Data Communication" Msc Thesis, Faculty of Science, Assiut University., pp. 120, 2009.
- [15] H. Marghny Mohamed, M. Naziha AL-Aidroos and A. Mohamed Bamatraf, "A combined image Steganography technique based on edge concept and dynamic LSB," *International Journal of Engineering Research and Technology.*, **1**, 2012.
- [16] M. H. Mohamed and L. M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method," *Applied Mathematics & Information Sciences.*, **10**, p. 259, 2016.
- [17] M. Mohamed, A. Al-Mehdhar, and M. Bamatraf, "SOM PAD: Novel Data Security Algorithm on Self Organizing Map," *Computer Science and Information Technology (CS and IT)*, 2012.
- [18] M. Mohamed, A. A. Al-Mehdhar, M. Bamatraf, and M. R. Girgis, "Enhanced Self-Organizing Map Neural Network for DNA Sequence Classification," *Intelligent Information Management.*, **5**, p. 25, 2013.
- [19] M. H. Mohamed, Y. B. Mahdy, and W. A. E.-W. Shaban, "Confidential Algorithm for Golden Cryptography Using Haar Wavelet," *arXiv preprint arXiv:1501.03617*, 2015.
- [20] M. H. Mohamed, N. M. Al-Aidroos, and M. A. Bamatraf, "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference".
- [21] Ferreira, Cândida., "Gene Expression Programming: A New Adaptive Algorithm for Solving Problems." *Complex Systems.*, **13(2)**, 87-129, 2001.
- [22] Mansouri, Mahdi, et al. "A review of single phase power factor correction AC-DC converters." *Clean Energy and Technology (CEAT)*, 2013 IEEE Conference on. IEEE, 2013.
- [23] Sebtahmadi, S. Sina, et al. "A PSO-DQ Current Control Scheme for Performance Enhancement of Z-source Matrix Converter to Drive IM Fed by Abnormal Voltage." *IEEE Transactions on Power Electronics.*, **2017**.
- [24] Saghafinia, Ali, and S. HrKaboli. "Online Adaptive Continuous Wavelet Transform and Fuzzy LogicBased High Precision Fault Detection of Broken Rotor Bars for IM.", 2012.



M. H. Marghny Is a Professor of Computer Science, Vice Dean of Faculty of Computers and Information, Assiut University. He received his Ph.D. degree in computer science from the University of Kyushu, Japan, in 2001, his M.Sc. and B.Sc. from Assiut university, Assiut, Egypt, in 1993 and 1988, respectively. He is currently a professor in

the Department of Computer Science, and Vice Dean for Education and Student Affairs of the Faculty of Computers and Information, University of Assiut, Egypt. His research interests include data mining, text mining, and information retrieval, web mining, machine learning, pattern recognition, neural networks, evolutionary computation, fuzzy systems, and information security. Prof. Marghny is a member of the Egyptian mathematical society and Egyptian syndicate of scientific professions. He is a manager of some advanced research projects in Faculty of Computers and Information, University of Assiut, Egypt.



Mahmoud A. Mofaddel

Received his B. Sc. And M. Sc. Degrees from ASSIUT University in 1985 and 1991 respectively, and his Ph. D. degree from Rostock University, GERMANY in 1999. He authored and co-authored more than 23 scientific papers. His research interests include high performance computing, and image processing.



Tarek Y. Abd El-Naser

Received his B. Sc. Degrees from Sohag University in 2005, he received certified in software development from ITI (Information Technology Institute) in 2008, he is teaching assistant in department of computer science at New Cairo Academy.