Bulletin de la Société Royale des Sciences de Liège, Vol. 85, 2016, *p.* 935 - 951

The production of the initial population and Mandelbrot algorithm by using genetic set to encrypt Image

Elaheh Agha MOHAMMADI[1*], Mehdi Sadegh ZADEH[2]

[1] Graduate Student Artificial Intelligence Computer Engineer, Islamic Azad University, Science and Research of Bushehr, Iran
[2] Department of Computer Engineer, Islamic Azad University of Mahshahr, Iran

Abstract:

Nowadays, finding a way to secure media is common with the growth of digital media. An effective method for the secure transmission of images can be found in the field of visual cryptography. There is a growing interest in the use of visual cryptography in security application. Since this method is used for secure transmission of images, many of the methods are developed based on the original algorithm proposed by Naor and Shamir in 1994. In this paper, a new hybrid model is used in cryptography of images which is composed of Mandelbrot algorithm and genetic algorithm. In the early stages of proposal, a number of encrypted images are made by using the Mandelbrot algorithm and the original picture and in the next stage, these encrypted images are used as the initial population for the genetic algorithm. At each stage of the genetic algorithm, the answer of previous iterations is optimized to get the best encoding image. Also, in the proposed method, we can achieve the decoded image by a reverse operation from the genetic algorithm. The best encrypted image is an image with high entropy and low correlation coefficient. According to the entropy and correlation coefficient of the proposed method compared with existing methods, it is observed that our method gets better results in both of them.

Keywords:

visual cryptography, genetic algorithm, Mandelbrot function, fractal, reversible genetic algorithm.

Introduction:

With the rise of digital media, the need for methods to maintain such data seem necessary. Digital media sources link to the rich source of data which are offered by the internet and the range of the data are increasing day by day. These data can be simple text documents, images of people and so on. Internet provides an easy access to this required knowledge.

The field of visual cryptography is developed during the past few years. The main method was initially proposed by Naor and Shamir for binary images. This method offers a secure system in which secret messages are parts that are separately similar to random noise, but when they are properly placed on each other, their messages can be decrypted only by using the human visual system. While this method provides security for text and binary images, growth of digital media requires the development of these techniques to provide security for color and greyscale images. Through the development of the original method, visual cryptography provides a secure method to store and transfer text, binary images, gray and color images. Since the original method was developed in 1994, many changes and improvements were added to the available collection of visual encryption techniques. Many digital services require reliable security for the transfer and storage of digital images. Due to the rapid growth of the Internet in today's digital world, security of image has attracted a lot of attention. Prevalence of multimedia technologies in our society is caused digital images play a substantial role compared to the old texts which calls for serious protection of users' privacy is for all applications. Digital images' encryption techniques are very important that should be protected against unauthorized access attacks.

Digital images are exchanged on various types of networks that often a large part of these data is confidential or private. Encryption is a preferred technique to protect the transmitted data. There are various encryption systems to encrypt and decrypt data image. Today, images can be regarded as one of the usable forms of information. Image Encryption has various applications in different fields such as internet communications, multimedia systems, medical imaging, telemedicine and military communications and therefore, providing effective and secure protection for image files is one of the main concerns.

In proposed method, at first, the input images are combined with Mandelbrot fractal image then in terms of the size of the images, a series of random numbers is generated and in the next stage, pixel is selected with the use of these numbers in both of the rows and combined dual-point operation is performed on them. And finally, by using random numbers generated in the second step, the row of image pixels of previous step is dislocated that this act is similar to the mutation function in the genetic algorithm and in this way the encrypted image is obtained and if input images to be colorful, these acts are done on all three color components. In the decode step, at first the mutation function conducted at the encryption step is carried out inversely then, the two point combined action is also performed inversely. Finally, in order to achieve the original image, the Mandelbrot fractal image is subtracted from the generated image.

Cryptography:

Cryptography is the science of codes and ciphers and an ancient art and it is used for centuries to protect the messages that were exchanged between the commanders, spies, lovers and others to make their messages confidential. When data security is discussed, it is necessary to prove the identity of the sender and receiver of the message and also, to be sure not to change the content of the message. The three issues of confidentiality, authentication and integrity are at the heart of modern data communications security and can use encryption (8). This issue should be ensured that a message can only be read by those for whom the message was sent, and others are not allowed. Cryptography is the provider of this issue.

Cryptography is the art of writing in an encrypted format so that no one except the intended recipient cannot read the message content. Cryptography has two main components including algorithm and key. The algorithm is a converter with mathematical formula. The key is a string of binary digits (one and zero) which in itself is meaningless (7). Modern cryptography assumes that algorithm is known or can be discovered. It is the key that should be kept secret or varies at each stage of implementation. Decryption may use the same pair of algorithm and key or different pair (1, 2).

Areas of Cryptography

Issues related to the field of cryptography can be proposed and considered at different levels (7). At the first level, a number of the paradigm such as symmetric cryptography, asymmetric cryptography and mixture exist and at the second level, a number of algorithms such as RSA and DES exist and protocols and standards are established at the third level. At the fourth level, applications or other protocols are created on these protocols. Maybe algorithm to be good, the protocol to be well-defined and established, but at the level of implementation of the application not to be good. Therefore, every level requires a degree of quality, performance, and confidence and creating influence on the systems may naturally return to each of these levels (2).

The terms used in Cryptography

Cryptology: The science of the study of cryptography and decryption

Password device: a system that is created to encrypt and decrypt data.

Cryptography: It is the art and science of mathematical techniques related to the concepts of data security like confidentiality, data integrity, authentication, non-repudiation.

Decryption: The study of methods that are used to break the encryption techniques.

Cryptographer: A person who is studying the systems and versions of encryption.

Decrytor: A person who is malicious at decoding and analysis of codes.

Cryptography: The encryption process of messages in a way that it's content to be hidden from foreigners.

Decryption: The process of recovering plaintext from the ciphertext.

Symmetric encryption algorithm: symmetric encryption algorithms or private key encryption use a key to encrypt and decrypt of data.

Asymmetric cryptography algorithm: Asymmetric Cryptography algorithm or public key cryptography algorithm uses different keys to encrypt and decrypt of data and decryption key cannot be derived from the encryption key (1,3).

DES, Triple-DES, SHA-1, RSA are the public key algorithm and RSA is the most famous public key algorithm that is used for encryption and digital signature. RSA calculations are done with integers n = p * q for large prime numbers p and q. To encrypt the message of m, it reaches to the view of a public small view of e.

To decrypt, the receiver of cipher text of C = me (mod n), calculates reverse of d = e-1 (mod (p-1) * (q-1)) and obtains the amount of Cd = me * d. The private key includes m (mod n) e, q, n, p, d. The public key only includes e, n (1, 13).

Cryptography methods

Symmetric method: In this method both sender and receiver of information have a common key for encryption and decryption. In this state, the encryption and decryption of information are two reverse process. Key transition between each other by intranet or physically is somewhat safe. But its transmission by internet is not correct (4). In such systems, the keys for encryption and decryption are same or have very simple relationship with each other. Symmetric encryption is used to encrypt large amounts of data. When it is used with a digital certificate, the confidentiality of information is protected. When electronic signature is used, the message integrity is guaranteed (2).

Advantages: High speed during the encryption, key generated randomly and fast.

Disadvantages: a plurality of keys for the members of each connection, key distribution among communicating parties.

Asymmetric method: This method was created to solve the problem of key transfer in symmetric method. In this method, instead of a shared key a pair of public and private key is used. In this method, the public key is used for encryption of information. The one who intends to transfer information in an encrypted form, encodes information and sends to the person who is the owner of the key pair. The

owner of key maintains the private key for himself in a confidential form. In this method, the encryption and decryption keys are distinct (2).

Advantages: No need to distribute and send key.

Disadvantages: low speed in high volume of data, the complexity of key generation.

Digital Signature

The digital signature is used to approve the identity of the sender of document and also to ensure that the document has not been altered during the transmission to the recipient. The whole or part of the document can be signed (7, 8).

The reasons for using digital signatures including: using public key allows everybody to send his key to the information sender and then the receiver after receiving the information decodes it by his private key therefore, digital signature allows the sender or receiver to be sure that the information is received by the intended person or place.

Information during the transition period may be altered by others. The need for a digital signature is felt to insure the accuracy of information received. Rejection of the information sent, the recipient of information to ensure that the sender of information does not reject its sending, requests a signature from the sender as a witness to the claim. In fact, electronic signature is possible by using asymmetric cryptography to prove a document belongs to its owner and lack of distort of the contents.

RSA algorithm

In 1777, in MIT university three American mathematician established the foundations of the algorithm. Three stages can be imaged for this algorithm (5): that document is done and generally, it can be said that the electronic signature is built based on the private key of individuals (5).

• Generating public and private keys for encryption

• Encoding information by public key

• Decrypting information by private key

Image

For image processing, we should be familiar with the way of registration and using images on computer or common digital processors. By knowing how to register and review images on a computer, programs can be made that by using these data, image file can be read and in this way we can access to all components of the image and the necessary processes are done on the image. Also, after processing the operation results can be recorded and stored on the computer (3, 6).

There are two ways to display graphic images that including the viewing image method which is also known as pixel image and vector method.

The function of chaos

Until a few decades ago, scientists knew the world as a set of systems that moves according to the algebraic rules of the nature in completely clear and predictable way but with the development of science many other natural events were not justifiable by previous algebraic ideas. Efforts of scientists to describe such events lead up to the advent of theories of quantum and relativity in physics and chaos theory in mathematics (9).

Chaos literally means clutter and disarray and in everyday conversation is usually a sign of irregularity and disorganization which has negative aspect. But today, with the advent of scientific attitude disorder and chaos is not regarded as the concept of irregularity, disorganization and inefficient but it is considered as a kind of order in disorder or regular irregularity. The key and main motivation of chaos theory refers to the concept of regularity in irregularity (5).

Chaos Theory

Chaos theory deals with the study of chaotic dynamical systems. Chaotic systems are nonlinear dynamical systems that are very sensitive to their initial conditions. Slight changes in initial conditions of such systems will lead to the great changes in the future. This phenomenon in chaos theory is well known as the butterfly effect (4, 3).

The Butterfly Effect is the name of a phenomenon that is created because of the sensitivity of chaotic systems to initial conditions. This phenomenon points out that small changes in the chaotic system like Earth's atmosphere can cause drastic changes in the future. Chaos is a phenomenon that occurs in definable nonlinear systems that shows extreme sensitivity to initial conditions and random-like behavior. In the event that such systems meet the requirements of Lyapunov exponential equation, they will remain stable in the chaos fashion. An important feature that puts this phenomenon at the center of attention refers to system’s definability at the same time of pseudo-random behavior that causes output of system seems random from the perspective of attackers while from the point of view of decoder of system is definable and therefore, is decipherable. The benefits of this type of functions include (10, 11):

Extreme sensitivity to initial conditions: It means that any slight change in initial values creates a significant difference in the next values of function.

Seemingly random behavior: Compared with manufacturers of numbers, natural random in which the string of generated random numbers cannot be reproduced, methods used for random numbers generation in algorithms based on chaos functions make it possible that random numbers can be reproduced if the original value and the mapping function to be existed.

Certain performance: Chaos functions have random appearance, but they are absolutely certain.

Image encryption based on logistic chaos signal.

In the image encryption method with the help of chaos functions a 08-bit external secret key hidden in irregular logistic map is used. The initial conditions for both logical map are obtained by applying foreign key that provides different weights for all the bits. Therefore, in this process the encryption of 0 is used for different implementation type to encrypt the pixels of an image and each of them for a certain pixel which is considered by the logistic map and to strengthen the password against any aggression the hidden key is changed after encrypting each block of 11 pixels image.

The results of various experiments, statistical analysis and sensitivity tests show that this method of image encryption provides an effective and mysterious method to transfer and encrypt the image immediately.

Chaotic encryption techniques for practical use are interfered well because these techniques provide a good combination of speed, high security, complexity, reasonable calculations for computing time and so on. Digital images have certain features including data redundancy, strong constant between adjacent pixels and having low sensitivity compared to textual data (12).

The smallest change in the character of a pixel of the image do not reduce image quality, image size, etc. As a result, common passwords such as IDEA, AES, DES and RSA are not suitable for immediate encryption of image because their passwords require high computation time and high computing power.

For immediate encryption of image, only passwords are preferred that need less time and at the same time reduce the amount of security and have attracted the attention of encoders. In the image encryption an external secret key bit and two irregular logical maps are used. The primary mode for each logical map is obtained by applying external secret key along with different weight preparation in its bits. In this algorithm, the first logical map is used to produce numbers ranging from 1 to 24. The initial state of the second logical map is changed by numbers produced in the first logical map and by variation of the initial state, the movements of the second logical map become random in this way. In suggested encryption process of 0 type, different actions are used for encrypting the pixels of an image

and operator that is used for a particular pixel is determined by the output of the second logical map. Thus, the second irregular map increases the turbulence of relation between encrypted image and its original version. To strengthen the code against the aggression after every encryption, the 11 pixel block of cipher key is modified.

The suggested process for image encryption in this method

The need for image encryption to securely transmit images over communication channels such as internet networks and wireless communications networks is increasing and due to the high volume of image and video data the traditional encryption algorithms do not enjoy the necessary efficiency in this regard (53). In this study, a new method is proposed based on a combination of Mandelbrot fractal image and genetic operators with the ability to encrypt images with minimal correlation coefficient and maximum entropy. In Figure 1, the overall chart of image encryption stages of the proposed method is displayed. Then, the stages of image encryption system are completely explained.

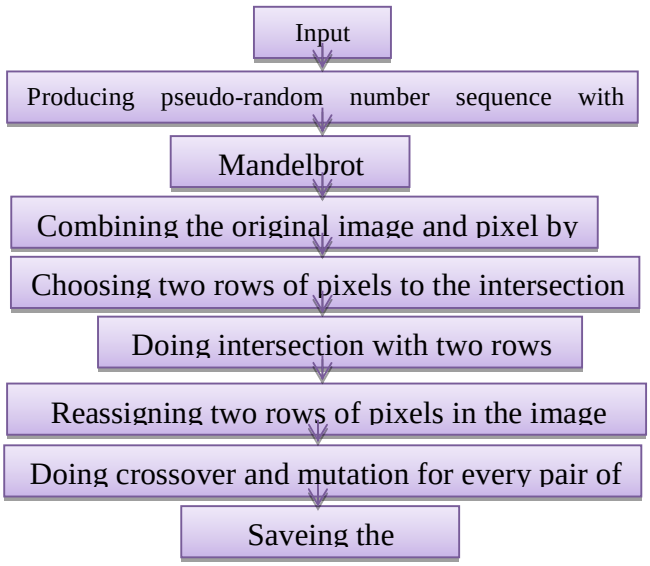

Figure 1: The overall chart of the encryption system of the proposed system

Combining the original image with the image of Mandelbrot

At this stage, the input images with Mandelbrot fractal image that have the same size are gathered pixel by pixel and the remaining pixel of original image with pixel of Mandelbrot image is calculated to number of 255 for each pixel of output image. And for color images, these actions are calculated for triple RGB colors.

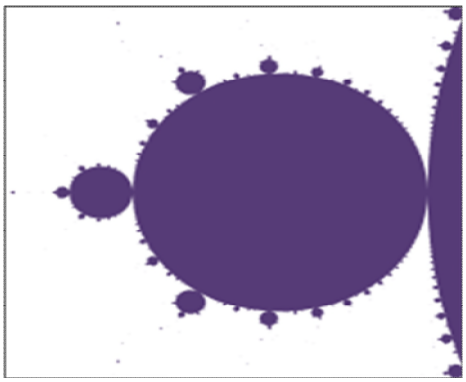

Figure 2: Self-resemblance in Mandelbrot collection.

Numerical code generation for encryption and decryption

At this stage, a series of Fibonacci random numbers are produced in relation to the size of the input images and the golden key that these numbers are used in the later stages.

Fibonacci series

In mathematics, Fibonacci series are a sequence of numbers that are defined as follows:

$$F(n) := \begin{cases} 0 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ F(n-1) + F(n-2) & \text{if } n > 1. \end{cases}$$

In which except the two prime numbers, the next numbers are obtained from sum of their previous two numbers. The first numbers of the series are: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584.... These numbers are named to the name of Italian mathematician Leonardo Fibonacci.

Double point crossover operator on rows of output images

At this stage, by using the code generated in previous stage, at first, two rows of pixels as two chromosomes become ready for crossover action and to determine the crossover pixel, at first, the number of row of each chromosome is divided to 255 and is multiplied in the number of pixel of each row (the number of genes) and the number of pixel is achieved for double point crossover action. This is achieved for all pixel rows and for each three RGB color channels.

Mutation operator on the output images

At this stage, by using the code generated in the second stage, the row of pixels of images of previous step is dislocated and this is obtained for all row of pixels and for three RGB color channels. In Figure 3, an example of mutation operator is shown on the two rows of pixels of the image.

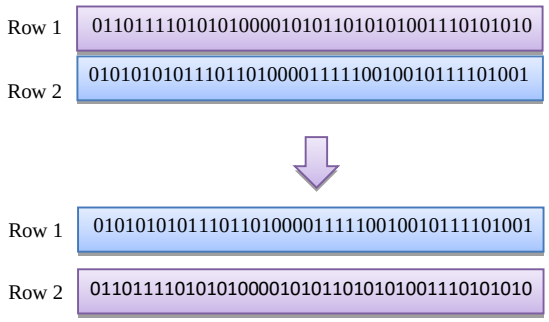

Figure 3: An example of mutation operator on two rows of pixels of the image

Finally, the encrypted image is created by using a combination of input images with Mandelbrot fractal image and operators of genetic algorithm. Figure 4 shows an example of the input image and the encrypted image.

Figure 4: An example of the input image and the encrypted image

Decoding image

In this section, all the steps and processes in the encryption are performed inversely. At first, the encrypted image is loaded and the sequence of Fibonacci random numbers are created by using the golden code, then the Mandelbrot fractal image is created. In the next stage, based on the sequence of produced numbers, mutation operation is inversely applied and contrary to the encryption part on encrypted image. Then, the crossover practice is also applied in reverse form on pixel rows of encrypted image and this is applied to all the rows of pixels of the images. Finally, in order to achieve the main image the Mandelbrot fractal image should be subtracted from encrypted image and this action is done by pixel by pixel subtraction. Figure 5 shows the overall chart of steps involved in images decoding. In the following the details of each section are explained.

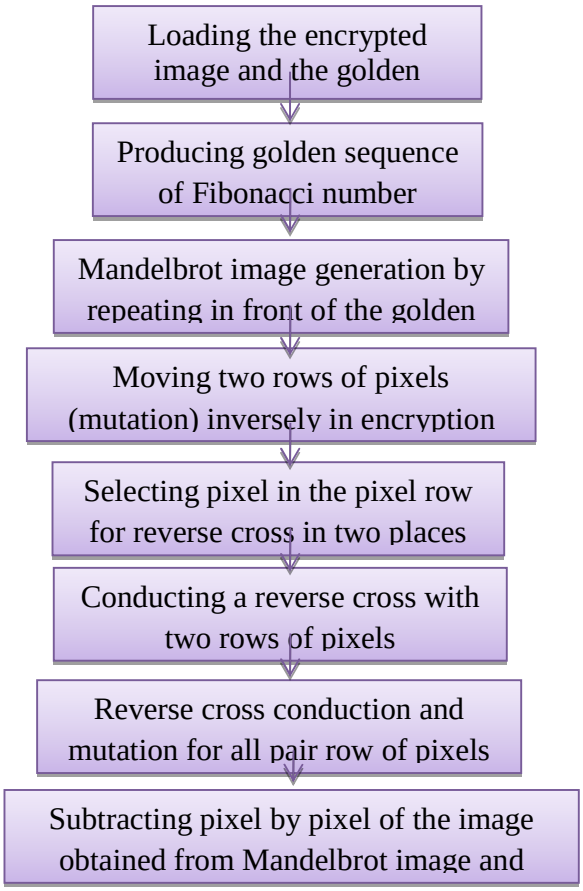

Figure 5: The overall chart of decoding system of the proposed system.

The production of the sequence of Fibonacci random numbers

At this stage, after loading the encrypted image and the golden number, such as the encryption section, the sequence of Fibonacci random numbers is produced.

Reverse mutation operator on encrypted images

At this stage, by using a series of randomly generated code, the pixels' row of encrypted images is displaced that this operation causes the row of pixels returns to its own true location. Also, this action is performed for all rows of pixels of images and for each of the three RGB color channels.

Reverse double point crossover operator on rows of encrypted images

By using randomly generated code sequence, at first, two rows of pixel as two chromosomes become ready for crossover action and in order to determine the crossover pixel, the number of row of each chromosome is initially divided to 255 and is multiplied in the number of pixel of each row (the

number of genes) and the number of pixel is achieved for double point crossover action. This action is achieved for all rows of pixels and for each three RGB color channels.

Discretization of the original image from the Mandelbrot image

At this stage, the original image is subtracted from the Mandelbrot image that are at the same size and the decoded image is obtained by combining the Mandelbrot fractal image with genetic algorithm operators. Figure 6 displays an example of the encrypted image and decrypted image.

Figure 6: An example of the encrypted image and decrypted image

The performance and efficiency of proposed system are tested by using different parameters and criteria and the results obtained in each part are discussed and analyzed.

Collection of images

To evaluate and test the performance of the proposed system and also to compare with other methods the known images in this area are used. These images are being used in most of the articles and are suitable to evaluate the performance of systems. Images used in the gray area include Lena, Peppers, Baboon, House, Boat and Photographer and color images include Peppers, Baboon, Lena and Airplane. In Figure 7 the gray images used in the experiments of proposed system and in Figure 2 the color images are shown.

Figure 7: The gray images used in the experiments of proposed system

Evaluating the proposed system

Among the important criteria in images cryptographic operations can point to the calculation of the amount of entropy of encrypted images, correlation coefficient of the original image and encrypted image, the amount of PSNR original image and the decrypted image and also, histogram of the encrypted image. The proposed system is evaluated based on the mentioned criteria and on the gray and color images' levels. In the following the details of the results of the proposed system are presented.

Entropy of the encrypted images

Information entropy in theory of the information is in connection with the fact that a signal or a random event to what extent is random. In fact, information entropy reports the randomness rate as a mathematical evaluation. One of the goals of the image encryption topic is data encryption in a way that the encrypted image contains maximum entropy. In other words, the more entropy amount, the more chaos or randomness of pixels of images. This causes the information of the original image not to be recognizable from encrypted image and access to the original image by using statistical analysis to be minimized. In Table 1, the entropy rate of encoded images is shown in the sample images.

Table 1: The results of the proposed system based on the selected criteria

Entropy	Input Image
7.8938	Peppers
7.9057	Lena
7.7937	House
7.8940	Baboon
7.8944	Boat
7.9004	Photographer

Correlation between the original image and encrypted image

The correlation coefficient is statistical tools to determine the relevance of a quantitative variable with another quantitative variable. The correlation coefficient is one of the criteria used to determine the correlation between two variables. It displays the intensity of correlation and this coefficient is between 1 and -1 and in the case of the lack of relationship between two variables is zero. The correlation coefficient of two images is used to investigate the relationship between the encrypted image and the original image. In our study, the aim is to reach a value close to zero and this proves the lack of connections and similarities between the two images. The correlation coefficient close to zero indicates that the encrypted images do not have the features of the original image and by using statistical analysis the original image data cannot be achieved. Table 2 displays the correlation coefficient data of the selected gray level images.

Table 2: Results of the proposed system based on selective criteria

Correlation Coefficient	Input Image
0.0010	Peppers
0.0198	Lena
0.0163	House
0.0111	Baboon
0.0097	Boat

The simulation results

Finally, the outputs images of proposed system include encoded images and decoded images which are shown in Figure (12).

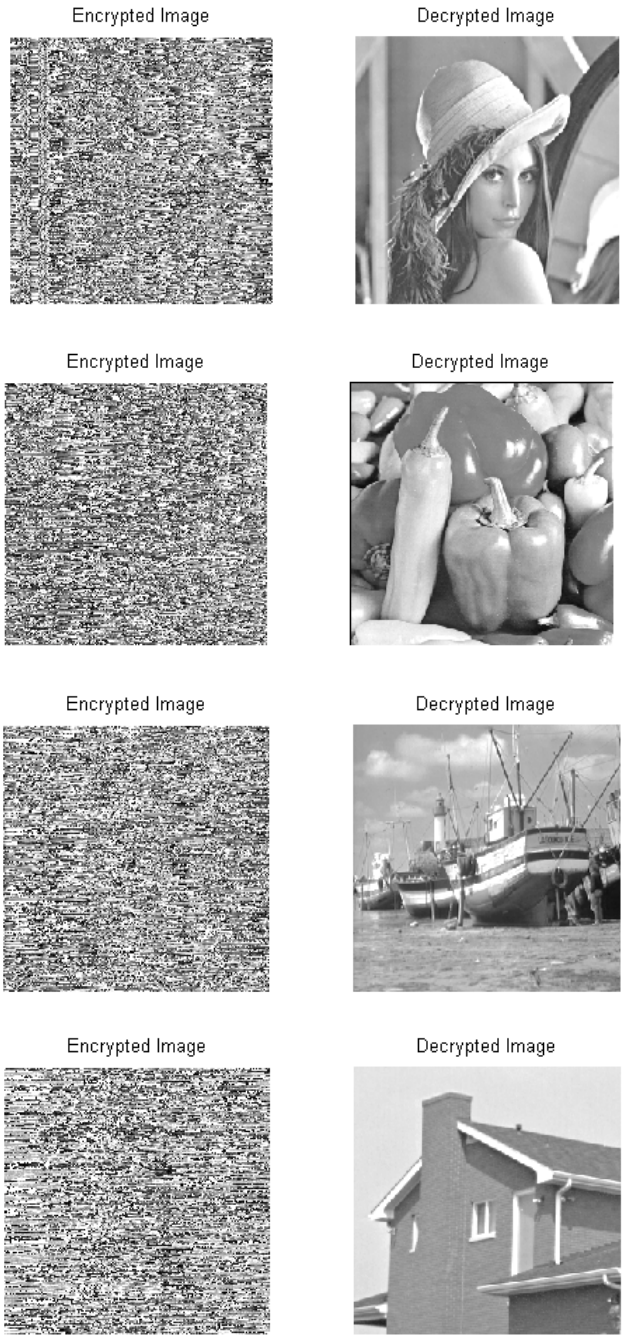

Figure 12: The outputs images of proposed system

A comparison of the proposed method and other methods

In order to investigate the tests results of the proposed system compared to the former provided systems, the test results of previous methods are obtained based on the listed criteria. The results of the proposed system and the system (35) are displayed in the Tables 3 and 4 according to the correlation coefficient and entropy for images of Lena and Baboon.

Table 3: The results of the proposed system and system based on the selected criteria on the Lena image

The method used	Correlation Coefficient	Entropy
The proposed method	0.0198	7.9057
Method (56)	0.0135	7.9822

Table 4: The results of the proposed system and system based on the selected criteria on the Peppers image

The method used	Correlation Coefficient	Entropy
The proposed method	0.0010	7.8938
Method (56)	0.0119	7.9873

As can be seen in Tables 5-3 to 5-4, the results of proposed system compared to the articles (56) and (57) have achieved better results in relation to the mentioned criteria.

Conclusion

In this paper, a method was presented based on fractal theory and operators of genetic algorithm to encrypt images. At first, in the proposed method the input images are combined with Mandelbrot fractal image then, according to the size of the images, a series of random numbers are generated that in the next stage, by using these numbers in each step two rows of pixel are selected and double point combined operations are performed on them. Finally, by using random numbers generated in the second stage, the row of pixels of the image of previous step is dislocated that this act is as mutation practice in genetic algorithm and the encrypted image is obtained in this way. If input images to be colored, this act is done on all three color components. In the decode step at first, the mutation practice conducted at the encryption step is done reversely then the double point combined operation is done in

reverse form. Finally, in order to achieve the original image, Mandelbrot fractal image is subtracted from the generated image. The proposed system was evaluated by using the criteria used in these areas and also was compared with similar systems and according to various criteria, the proposed system can obtain the acceptable and appropriate values based on various criteria and compared with previous similar methods, the proposed method could also get better results based on the mentioned criteria.

References :

[1] J. Weir, W. Yan, "A comprehensive study of visual cryptography", Transaction on DHMS V, LNCS, Springer, pp. 70-105, 2010.

[2] A. Campbell, The Designer's Lexicon. Chronicle Books, San Francisco, 2000.

[3] W. Qiao, H. Yin, H. Liang, "A Kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395, 2009.

[4] J. S. Lee, T. H. Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1- 4244-4568-4/09, IEEE, 2009

[5] P. S. Revenkar, A. Anjum, W. Z. Gandhar, "Survey of visual cryptography schemes", International Journal of Security and Its Applications, Vol, 4, No. 2, 2010.

[6] R.J. Chen, W.K. Lu, J.L. Lai, "Image encryption using progressive cellular automata substitution and SCAN", In: IEEE international symposium on circuits and systems, 2005.

[7] R. Enayatifar, "Image encryption via logistic map function and heap tree", Journal of the Physics Science, pp. 221–8, 2011.

[8] Z. Liu, L. Xu, C. Lin, J. Dai, S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains", Optics and Lasers in Engineering 49, pp.542–6, 2011.

[9] H. Li, Y. Wang, "Double-image encryption based on discrete fractional random transform and chaotic maps", Optics and Lasers in Engineering 49, pp.753–757, 2011.

[10] Z. J. Liu, Q. Guo, L. Xu, "Double image encryption by using iterative random binary encoding in gyrator domains", Optics Express 18, pp.12033–12043, 2010.

[11] J. Koljonen, "Comparison of nearest point algorithms by genetic algorithms", Expert Systems with Applications 38, pp.10303–10311, 2011.

[12] D. Ashlock, J. Alexander Brown, "Fitness functions for thee Mandelbrot set", IEEE Transaction, 2011.

[13] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," AEU - International Journal of Electronics and Communications, vol. 66, pp. 806-816, 10// 2012.