International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 4 Ver. IV|| April 2018 || PP 64-70

An Efficient Image Encryption Method Based on Genetic Algorithm

Abhishek Bal[1], Nilima Paul[2]
[1](Department of Computer Science & Engineering, RCC Institute of Information Technology, India)
[2](Department of Computer Science, Dinabandhu Andrews Institute of Technology & Management, India)
Corresponding author: Abhishek Bal

Abstract: *In the area of information technology, the growing of sharing or broadcasting information and transfer it via virtually connected systems or communication networks increases the need for security exponentially. In today's world integrity, non-repudiation, confidentiality, and authentication services are considered as the most important security principle. Throughout the previous few years, the security of digital images growing more vital when images are transmitted through the communication networks or stored in memory. Several image encryption methods are employed in the state of the art of images security. Image encryption is a technique to encode an image to make them non-readable. This paper proposed an efficient approach for image encryption and decryption based on genetic algorithm by using the powerful features of the genetic parameters such as crossover and mutation operations. Genetic algorithm is considered as an optimization algorithm, because it searches a space in a multi-directional way from large and poorly defined space. In this present work, the intermediate cipher is produced by applying the substitution technique on each element of the original image which is encrypted by each element of the key matrix. Then the genetic algorithm is applied to convert the intermediate cipher to the final cipher. The proposed method has been applied to IAM database and USC-SIPI image database over 550 images. Experimental results show that proposed technique achieved a high precision that is fast enough for real-time data security.*

Keywords *-Genetic Algorithm; Optimization; Cryptography; Image Encryption; Image Decryption; Plain Text; Cipher Text.*

Date of Submission: 05-03-2018 Date of Acceptance: 20-04-2018

I. INTRODUCTION

In earlier days, computer data was considered to be useful, but not something to be protected. When computer applications were developed to handle the personal or financial data, then the need of data security was very important. The word cryptography is derived from the Greek word Kryptos means hidden and graphics means write. In a word, cryptography means secret writing. Cryptography encompasses on the following security basis that is confidentiality, authentication, data integrity and non-repudiation. The two main processes of achieving cryptography [2] are encryption and decryption.

When a sender is sending messages (plain text) to the receiver, the encryption process protects the messages by encrypting with an encryption key to make them non-readable (cipher text). On the other side, in the receiver end decryption process, the messages (cipher text) are decrypted into its original form (plain text) by using decryption key.

The cryptographic algorithm can be categorized as symmetric cryptography [3, 4] and asymmetric cryptography [5] based on the number of keys that are applied to encryption and decryption process separately. Symmetric key cryptography encrypts and decrypts the message using the same key. The speed of the symmetric cryptography is very fast, but it suffers from the key exchange. But in asymmetric key cryptography, two key are required. One is the public key for encryption and another distinct key is needed for decryption called the private key. The speed of the asymmetric cryptography is slower than the symmetric key cryptography, but does not suffer from the key exchange. There are two primary ways by which a plain text message can be converted to obtain the corresponding cipher text that are substitution and transposition [6].

Genetic algorithm [1, 7, 22] is considered as a powerful technique [8] because anyone can apply it easily to any domain. Genetic algorithm [1, 8, 9, 10, 11, 12, 13, 14, 15] is the searching process in the way of adaptive heuristic manner that incorporates evolutionary ideas of natural selection and genetics.Genetic algorithm used to solve different types of optimization problems and also useful for searching in random space. Optimization [9, 10] process finds a best or optimal [8] solution for a problem which performs better than traditional artificial intelligence. Unlike older AI systems, the GA's do not fall easily, even if the presence of

Gaussian noise during the image acquisition process or change of input condition. The genetic algorithm can be implemented in any type of data like text messages, images, video etc.

This paper proposed an efficient image encryption algorithm where the operators of GA (crossover and mutation) are used to perform the encryption-decryption procedure. In the proposed method, genetic algorithm was applied to the intermediate cipher image which is produced by applying the substitution technique to original image matrix. Genetic algorithm is built up with the genetic operators or process, i.e. selection, crossover, mutation and reproduction that are performed in a repetitive manner to evaluate the solution until a solution is found as optimal.

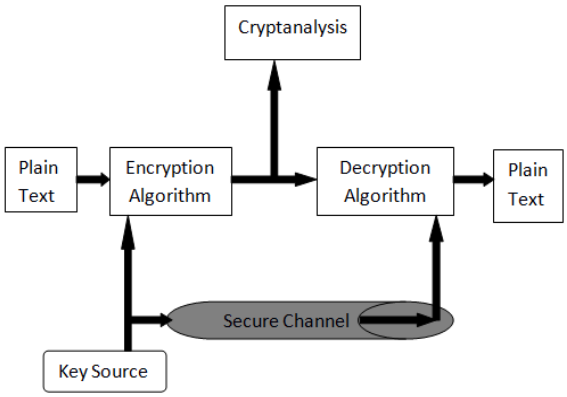


Fig. 1 Model of Secure Communication

II. LITERATURE SURVEY

In 2014, Abhishek Bal, Nilima Paul, Suvasree Chakraborty and Sonali Sen [1] have proposed a method based on genetic algorithm which is used for automatic voice recognition technology. This proposed word also explained the methodology of the genetic algorithm. The results show that such an algorithm able to discover new voices from the existing voices.

In 2012, Ankita Agarwal [17] has proposed a method based on genetic algorithm which is used to produce a new encryption method by exploring the dominant features of the crossover and mutation operations of GA. This proposed genetic-based encryption method satisfied the goals that are required for image encryption.

In 1993, Richard Spillman, Mark Janssen, Bob Nelson and Martin Kepne [18] have proposed a new approach to cryptanalysis based on the application of a directed random search algorithm (GA). The results show that such an algorithm could be used to discover the key for a simple substitution cipher.

In 2006, Tragha A., Omary F., Mouloudi A. [19] have represented a symmetrical block ciphering system by using genetic algorithm. The complexity of their proposed system is o(n) because all operations are very simple and proposed methods are applied randomly in ciphering.

In 1978, Rivest R. L., Shamir A., and Adleman L. [5] have proposed encryption process with the novel approach of exposing the encryption key as public, but not thereby expose the corresponding decryption key.

In 1997, Andrew Clark & Ed Dawson [21] have proposed a new method for attacking the simple substitution cipher which utilizes a parallel version of the genetic algorithm. They also expressed an analysis of the fitness function.

III. PROPOSED METHOD

1. Encryption Process

The encryption process encrypts the original image by the substitution technique with the help of key matrix. Then the genetic algorithm produces the final cipher text from the intermediate cipher text. The proposed method is described below

1.1) key generation: At first, an image is taken as a key. This image is represented here in terms of the key matrix denoted by a 2-D Array ENKEY[ ][ ] whose order is m×n. This ENKEY[ ][ ] is applied in encryption and decryption process. So the key exchange procedure between sender and receiver through the secure channel is required before the encryption process.

1.2) substitution: In this proposed work, polyalphabetic substitution is used for substitution purpose. Let the sequence of the original image is represented as IMG1=$IMG1_{1,1}$, $IMG1_{1,2}$, $IMG1_{1,3}$,…,$IMG1_{m,n}$ and encryption key matrix is represented as ENKEY=$ENKEY_{1,1}$, $ENKEY_{1,2}$, $ENKEY_{1,3}$,…, $ENKEY_{m,n}$.

The sequence of intermediate encrypted image IMG2=$IMG2_{1,1}$, $IMG2_{1,2}$, $IMG2_{1,3}$,…., $IMG2_{m,n}$ is calculated as

$$IMG2(I,J)=(IMG1(I,J)+ENKEY(I,J)) \text{ MOD } 255 \qquad (1)$$

The size of the original image matrix and the encryption key matrix are same that is m×n. If the size of the original image matrix and key matrix are not same, then through resizing function they are converted to the same size. In the substitution operation, 255 is used for mod operation instead of 26 because here proposed work applies the encryption operation on the gray scale image instead of alphabet. The maximum intensity value of 8-bit gray scale image is 255. The substitution techniques for a subset of an image are shown in Table I.

Table I. Substitution Table for Encryption

PT	96	254	145	15	77	221	26	254	110
KEY	89	16	248	189	145	45	55	74	69
ADD	185	270	393	204	222	266	81	328	179
CT	185	15	138	204	222	11	81	73	179

In Table I, the first row represents the original image intensity, the second row represents the encryption key matrix, the third row represents the addition of original image matrix and key matrix and values of the fourth row is calculated by the values of third-row mod 255. This substitution process will continue until all the intensity values or elements of the original image (plain text) are encrypted.

The strength of this intermediate cipher is that there is multiple cipher text value for each plain text value, means if one element of the plain text occurs in multiple positions of that plain text then this element value can be converted to multiple cipher text values. Consider the Table I, where the plain text value in third and ninth columnsis 254 but after encryption through substitution technique the plain text value 254 converted to 15 and 73. After getting the intermediate cipher text, then genetic operators are applied to product final cipher text image.

1.3) Genetic Operator: Genetic algorithm is a searching process in adaptive heuristic fashion that incorporates evolutionary ideas of natural selection and genetics. Genetic algorithms are used to solve different optimization problems by searching in random space so that it can give a best or optimal solution.

Genetic operators are executed in such a way so that the genetic diversity is controlled. Genetic diversity or evolution is necessary for producing a new population. GA involves mainly three operators - selection, crossover, and mutation.

1.3.1) Selection: At first, selection operator is applied on population. From the population, individuals are selected based on selection operation. Most important is that how to select these individuals. Most commonly used methods for selection are roulette wheel selection, Boltzmann selection, tournament selection and rank selection, etc. Proposed algorithm does not use selection operator, because the input images for encryption is already given by the user.

1.3.2) Crossover: Crossover is next genetic operation that combines two parents (individuals) to construct new offsprings by taking the best characteristics from the each of two parents and also keeping in mind it would not be duplicate of parents. Most common crossover types are one-point, two-point, uniform and arithmetic crossover etc. In the proposed method uniform crossover operator is performed on the intermediate encrypted image which is the output image of polyalphabetic substitution. Here only one image is taken for crossover instead of two images. Proposed method performs the crossover operation in two fashions. The first crossover is performed in column major fashion, then it performed with row major fashion on the output of the column major fashion. In column-major fashion, the image is treated multiple sections of columns and the crossover is performed among of them, whereas in row major fashion image is treated in multiple sections of rows and the same process is applied among on them. Ultimately crossover operators mixed property of the original image in such way that actual properties of the images are lost.

1.3.3) Mutation: Mutation operator is executed for maintaining genetic diversity from one generation to the next. Mutation operator inverts one or multi gene values in an off from its initial condition. It can produce completely new gene values which are added to the gene pool. With newly created gene values, the genetic algorithm may able to produce a better solution than the previous one. Flip bit, Boundary, Non-uniform, and Gaussian are different types of mutation operators.

In this proposed method flip bit [1, 10] mutation technique is used which simply invert bit value, i.e. 0 goes to 1 and 1 goes to 0. In this proposed method before applying the mutation operator, intensity values of the intermediate encrypted image converted to the binary bit pattern then apply the mutation operation on the bit pattern. After the mutation operation, bit pattern converted to the intensity values to create a final encrypted image.

2. Algorithm for Image Encryption

Image Encryption algorithm is carried out by genetic algorithm as follows
Step 1: start
Step 2: Input the gray image as a plain text and convert it to the image matrix. Consider a 2-D array IMG1[ ][ ] as image matrix.
Step 3: Input another image as a key matrix. Store the key in 2-D array ENKEY[ ][ ]
% Perform the matrix addition and substitution
Step 4: for i←1 to r
Step 5: do
Step 6: for i←1 to c
Step 7: do
Step 8: A←Double(IMG1[i,j])
Step 9: B← Double(ENKEY[i,j])
Step 10: C←A+B
Step 11: IMG2[i,J]←MOD(C,255)
Step 12: end for
Step 13 :end for
Step 14: X1←R/2
Step 15: X2←C/2
% Circular Shift Operation
Step 16: IMG3←Circshift(IMG2,[X1 -X2])
% Cross Over and Mutation Section
Step 17: IMG4←Crossover(IMG3)
Step 18: IMG4←Mutation(IMG4)
Step 19: stop

In the above algorithm, Circshift() method is used to perform the right or left shift operation depending on the argument. Crossover() method is used to perform the crossover operation and Mutation() method is used for mutation operation after crossover is done. In the above algorithm, at first intensity values of the original plain text image and encryption key image are added then perform the modulus operation with value 255 over the newly calculated value and store into A 2-D array called IMG2[ ][ ]. After that circular shift operation is performed on IMG2[ ][ ]then the genetic operators- crossover and mutation are applied to the shifted image to produce the final encrypted image.

3. Decryption Process

The decryption process is a reversal process of encryption. In the decryption process, we first apply the GA operator (crossover and mutation) on the encrypted image to get the intermediate image. Then circular shift operation is performed in reverse order and at last reverse substitution function is applied to the intermediate to get the original image.

3.1) Key Generation: in the decryption process, the decrypted key is generated by subtraction of ENKEY (encryption key matrix) from the 255 stored in DEKEY matrix. That is

$$DEKEY(I,J) = 255 - ENKEY(I,J) \qquad (2)$$

3.2) Substitution: Let the sequence of the encrypted image is represented as$IMG2=IMG2_{1,1}$, $IMG2_{1,2}$, $IMG2_{1,3}$, … , $IMG2_{m,N}$ and decryption key matrix consist of the sequence of $DEKEY=DEKEY_{1,1}$, $DEKEY_{1,2}$, $DEKEY_{1,3}$, … , $DEKEY_{M,N}$. Let the sequence of decrypted image $IMG1=IMG1_{1,1}$, $IMG1_{1,2}$, $IMG1_{1,3}$, …. , $IMG1_{m,N}$ is calculated as

$$IMG1(I,J)=(IMG2(I,J)+DEKEY(I,J)) \text{ MOD } 255 \qquad (3)$$

The size of the encrypted image matrix and decryption key matrix is same that is m×n. In the substitution operation, 255 is used for mod operation instead of 26 because here proposed work applies the

decryption operation on the image instead of alphabet. So, the maximum intensity of 8-bit gray scale image is 255. The substitution processes for a subset of an image are shown in Table II.

Table II. Substitution Table for Decryption

CT	185	15	138	204	222	11	81	73	179
KEY	166	239	7	66	110	210	200	181	186
ADD	351	254	145	270	332	221	281	254	365
PT	96	254	145	15	77	221	26	254	110

In Table II, the first row represents the encrypted image intensity, the second row represents the decryption key matrix, the third row represents the addition of encrypted image matrix and key matrix and at last, the values of the fourth row are calculated by the values of third row mod 255 to get the original image matrix. This process continues until all of the encrypted image (cipher text) sequence is decrypted. From the output of the last row of Table II, It is proved that the plain text value after decryption is same as the plain text value before encryption.

4. Algorithm for Decryption

Image Decryption algorithm is carried out by genetic algorithm as follows
Step 1: start
Step 2: The name of the cipher file is stored in a 2-D Array IMG4[ ][ ], the encryption key is stored in a 2-D array ENKEY[ ][ ]
% Decryption Key Generation
Step 3: Decryption key is generated by subtraction each element of ENKEY from 255 and stored in DEKEY array
% Cross Over and Mutation Section
Step 4: IMG4←Mutation(IMG4)
Step 5: IMG5←Crossover(IMG4)
Step 6: X1←r/2
Step 7: X2←c/2
%Circular Shift Operation
Step 8: IMG6←Circshift(IMG5,[-X1 X2])
% Perform the Matrix Addition and Substitution
Step 9: for i←1 to r
Step 10: do
Step 11: for j←1 to c
Step 12: do
Step 13: A←Double(IMG6[i,j])
Step 14: B←Double(DKEY[i,j])
Step 15: C←A+B
Step 16: IMG6[i,j]←MOD(C,255)
Step 11: end for
Step 12: end for
Step 13: return Decrypted Image (original image) to the calling function.
Step 14: stop

Here also, Circshift() method is used to perform the right or left shift operation. Crossover() method performs the crossover operation and Mutation() method performs the mutation operation. In the decryption algorithm, the decryption key DEKEY[ ][ ] is generated by substitution of encryption key ENKEY[ ][ ] from 255. Then the genetic operators (crossover and mutation) are applied on the encrypted image matrix in reverse order, then circular shift operations are performed and stored in a 2-D array called IMG6[ ][ ]. After that intensity values of the intermediate decrypted image and intensity values decryption key image are added to perform the modulus operation with value 255 and stored in a 2-D Image matrix called IMG6[ ][ ]. At last, receiver get the original plain text image as IMG6[ ][ ] from the cipher text image.

IV. EXPERIMENTAL RESULT

This section illustrates proposed encryption and decryption approach with the use of genetic algorithm by showing the results of some input image as test cases. The proposed work implemented in MATLAB on was tested IAM database and USC-SIPI image database over 550 images. The proposed algorithm can work on gray scale images with any size and achieves more than 96% accuracy.

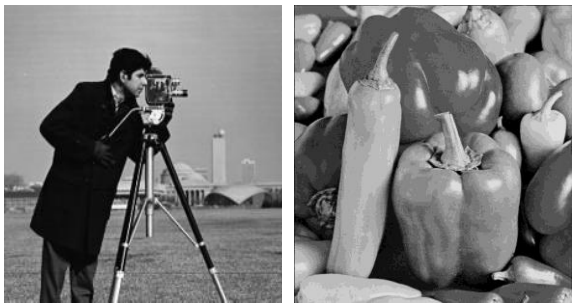
The actual original image which is the input of the encryption process is shown in Fig. 2(a) and 4(a) and key images for encrypting are shown in Fig. 2(b) and 4(b). After applying the proposed method on the original image, the encrypted results of the original images are produced that are shown in Fig. 3(a) and 5(a). After that, encrypted image is sent to the receiver end with key matrix through secure channels to produce the original image. The decrypted images of the corresponding encrypted images are shown in Fig. 3(b) and 5(b).

(a) (b)

Fig 2. (a) Original Image; (b) Key Image

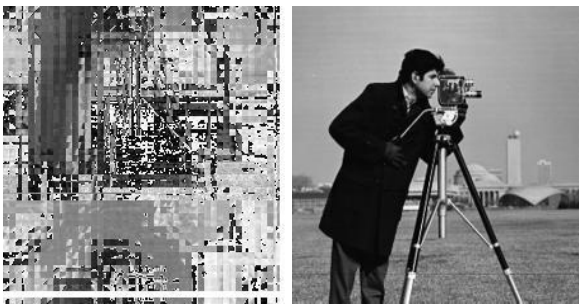
(a) (b)

Fig 3. (a)Encrypted Image; (b) Decrypted Image



(a) (b)

Fig 4. (a) Original Image; (b) Key Image



(a) (b)

Fig 5. (a) Encrypted Image; (b) Decrypted Image

V. CONCLUSION

This paper has proposed an algorithm to implement image encryption based on the secret key matrix using the genetic algorithm. Key matrix and intermediate cipher provide good security for image transmission through networks. The substitution method ensures the confidentiality of image through networks as it is using genetic algorithm which adds more security. From the experimental results, it is observed that the proposed Genetic algorithm (GA) based encryption method is satisfying our goals and a very good result is achieved during recognition. It is also suited to work with pictures and music. Due to parallelism, it makes the genetic algorithm more advantageous and effective. The main advantage of the evolutionary algorithm is that they do not have a lot of statistical measurements about the optimization problems. In the future work, our target is to design a sophisticated software based on this proposed technique which will be targeted to use in highly secure multimedia applications to support both data encryption and image encryption.

REFERENCES

[1] Abhishek Bal, Nilima Paul, Suvasree Chakraborty, Sonali Sen. Voice Matching using Genetic Algorithm. In: International Journal of Advanced Computer Research, Volume-4 Number-1 Issue-14 ;2014.

[2] Douglas, R.Stinson.Cryptography – Theory and Practice. In: Crc Press;1995.

[3] Daemen J., Rijmen V. The Design of Rijndael, Advanced Encryption Standard. In: Springer-Verlag, Berlin, Isbn 3-540-42580-2;2002.

[4] National Bureau Standards.Data Encryption Standard (Des) . In: Fips Publication 46; 1977.

[5] Rivest R. L., Shamir A., and Adleman L. A Method For Obtaining Digital Signatures and Public Key Cryptosystems. In: Comm. Acm Vol. 21(2), Pp. 120-126;1978.

[6] William Stallings. Cryptography and Network Security,6th Edition.

[7] David E. Goldberg, Addison-Wesley.Genetic Algorithms In Search Optimization and Machine Learning,Chapter 1-8, Page 1-432;1989.

[8] Sastry, K.. Evaluation-Relaxation Schemes For Genetic and Evolutionary Algorithms. In: Master's Thesis, General Engineering Department, University of Illinois At Urbana-Champaign, Urbana, Il;2001.

[9] Randy L Haupt. Practical Genetic Algorithm, John Wiley and Sons Inc, Chapter 1-7, Page 1-251;2004.

[10] Artificial Intelligence: Course Content, Lecture Hours – 42, Rc Chakraborty, June 01, 2010. Available: Http://Www.Myreaders.Info/Html/Artificial_Intelligence.Html.

[11] Georges R. Harik, Fernando G. Lobo, David E. Goldberg . The Compact Genetic Algorithm. In: University of Illinois At Urbana-Champaign Urbana,Il 61801,Illigal Report No. 97006;August 1997.

[12] K. F. Man, Member, Ieee, K. S. Tang, S. Kwong. Genetic Algorithms: Concepts and Applications. In: Ieee Transaction On Industrial Electronics, Vol-43, No-5; October 1996.

[13] Kumara Sastry(2), David Goldberg(2), Graham Kendall(3). Genetic algorithms. In: Springer, 2. University of Illinois, Usa, 3.University of Nottingham, Uk;2005.

[14] Davis, L. D. (Ed).Genetic Algorithms and Simulated Annealing, Pitman Publishing.London;1987.

[15] Srivastava, R.Goldberg, D. E., Verification of The Theory of Genetic and Evolutionary Continuation. In: Proc. Genetic and Evolutionary Computation Conf., Pp. 551–558;2001.

[16] Sindhuja K , Pramela Devi S. A Symmetric Key Encryption Technique Using Genetic Algorithm'. In: International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 414-416; 2014

[17] Ankita Agarwal. Secret Key Encryption Algorithm Using Genetic Algorithm'. In: International Journal of Advanced Research In Computer Science and Software Engineering,Volume 2, Issue 4; April 2012

[18] Richard Spillman, Mark Janssen, Bob Nelson ,Martin Kepne. Use of Genetic Algorithm In Cryptanalysis of Simple Substituion Cipher. In: Cryptologia, Vol.17, No.4, Pp. 367-377; 1993.

[19] Tragha A., Omary F., Mouloudi A. Iciga:Improved Cryptography Inspired by Genetic Algorithms. In: Proceedings of The International Conference on Hybrid Information Technology (Ichit'06), Pp. 335-341; 2006.

[20] Clark A., Dawson Ed. , Nieuwland H. Cryptanalysis of Polyalphabetic Substitution Ciphers Using A Parallel Genetic Algorithm. In: Proceedings of Ieee International Symposium on Information and Its Applications, Pages 17-20,;1996.

[21] Andrew Clark, Ed Dawson. A Parallel Genetic Algorithm for Cryptanalysis of The Polyalphabetic Substitution Cipher. In: Cryptologia,Vol. 21, Issue2, Pages 129-138;1997.

[22] Abhishek Bal, Nilima Paul, Sonali Sen. Automatic Fault Identification of a Mechanical System using Genetic Algorithm. In: International Journal of Computer Applications(0975 – 8887) Volume 104 – No.9; October 2014.

Abhishek Bal and Nilima Paul, "An Efficient Image Encryption Method Based On Genetic Algorithm"International Journal of Engineering Science Invention (IJESI), vol. 07, no. 04, 2018, pp 64-70