IMAGE ENCIPHERMENT USING GENETIC ALGORITHM

S. Arunpandian[1], Prof. Dr.K.Mahesh[2]
Department of computer science, Alagappa university, Karaikudi , India
[1] spandiyan01@gmail.com
Department of computer science, Alagappa university, Karaikudi , India
[2] mahesh.alagappa@gmail.com

***Abstract* – Cryptography gets an essential role for secure the information's. In Every second, Enormous data is swap over through the communication channel, at this level the information security is required to digital data transaction. Without using the cryptography technique, the data sharing is inadequate. However, crypto method is extremely essential rather than the transaction speed. Even data as encrypted format, that data may steal in-between the communication. The embezzle technique has been threatening in mounting technology world. Security needs unbreakable cryptography mechanism better than the convention. Genetic algorithm is the powerful impartial optimization method and helps to encrypt the information in elegant way, which has some properties like selection, crossover, and mutation. The novel encryption method called image en-cipherment using genetic algorithm (IEGA). Which provides data security and it is propagated by the combination of cryptography and genetic algorithm. The images are encrypted and decrypted using IEGA method and results were compared in this paper by using some existing methods. The quality metrics such as SNR, PSNR, and MSE is used to justify the quality of our proposed IEGA methodology.**

Keyword — Cryptography, Genetic Algorithm, Security, Cross-over, Mutation

I. INTRODUCTION

A. *Cryptography*

Cryptography is the cram of information hiding and substantiation. It consist the algorithms, strategies and protocols to secure prevent or impediment unauthorized access to perceptive information and enable the verifiability of each component in a communication. Secret value is in cryptography, which can be identified as key. In addition to an algorithm which has a key that is difficult to maintain devising new fangled algorithm .which can be agree to reversible scramble of information. Cryptography is classified into two types such as Secret Key and Public Key. Secret key algorithms are used mainly for the core encryption of data. Huge number of probable keys and tremendously fast is to be in these algorithms. The vital symmetric key algorithm offer admirable secrecy. Already the information is encrypted with specified key there is no prompt way to decrypt the data without possessing the identical key. Mutually the dispatcher and the intentional receiver have to agree upon the key earlier than any communication begins [3] .Symmetric key algorithm could be divided into two phases: Stream and Block. Block algorithm are encrypt the data as distinct block at a time, whereas stream algorithm encrypt byte by byte or even bit by bit. Generally, encryption is a one of the methods to provide high security, which is well known that image encryption has extensively applications in internet communication, telemedicine, multimedia system etc[2].An efficient well-built and consistent encryption scheme is mandatory for surmount a secure communication of secret data over the network[6].

B. *Genetic algorithm Basics*

The genetic algorithm is a method for resolve the both constraint and unconstraint optimization tribulations, which is based on the selection; the process moves a biological evaluation. The genetic algorithm mutates a population of individual elucidation repetitively.

1) *Selection:* To select the some "individuals" from the parent population, it is done by the selection operation. The genetic selection process can be generated as follows: Each individual is evaluated by the fitness intention, provide the suitability values which are them normalized.
2) *Crossover:* The crossover operative plays the mid role in the genetic algorithm, which is the main way to initiate new individuals. The essential scheme of the crossover operator is performed by alternate a segment of the genes between two individuals to produce new individuals. This operators have single, two, multi-point, uniform crossovers.
3) *Mutation:* Mutation is a small random twist in the chromosome to get new solution, which can be used to maintain and diversity in the genetic population, it is equivalent to biological mutations

II. LITERATURE SURVEY

The following literature review, consist of methods applied by the research worldwide and recent developments.

In author xinyuvan-Dahaixupresented the new image encryption method generated by genetic algorithm properties which is based on the recent cryptography from the phase of genetic mechanism. Through the logistic map of intertwining method has been used to propagate the chaotic sequences remaining its advantages. Every pixel of the image takes as an “individual” each bits of its gene. In selection phase, the Monte Carlo method used to arbitrarily pick two individuals according to the chaotic sequences, cross, swap their genes using the particular crossover operator in the second phase. Selection and Crossover operations are help to perplex the image and to diffuse the image using the mutation operator. Finally modify the genes of individual arbitrarily for the mutation. The logistic map of intertwining is analyzed from the phase of the allotment of the sequences and Lyapunov exponents compared it with logistic map. The result of the intertwining logistic map could overcome the inadequacy of logistic map. Security and experiment analysis shows the new structure fully satisfies the functional requirement of modern cryptography[1].

In authors ”RasulEnayatifar, Abdul Hanan Abdulla” presented the chaotic function is used for create the hybrid model of the genetic algorithm and image encryption also predictable formation. This method helps to build the various numbers of encrypted images from the original input and encrypted images are employed as the initial population for initiating the operation of the genetic algorithm. Outcomes are obtained for correlation coefficients and the entropies of the images also prove the high effectiveness of this method, compared with other methods in image encryption. Moreover, this method has a higher stability in the face of attacks common in this area[2].

In authors “Girish R. Naik and Poornima G. Naik[3]” presented the en-cipherment of a text file using symmetric key and genetic operation techniques. In this method made an attempt to exploit the randomness involved crossover and mutation process for generating a secure single time secret key encryption and decryption message. The number of crossover points and mutation points, both are used to transmit the measurement lengthwise of the secret key and hence the strength of the algorithm and emphasis by create it complicated to break by permutation the secret key. A permutation of predefined factor agreed upon by both the dispatcher, intended receiver. The arbitrariness together with incarnation makes the algorithm; it might strong and hard to break. This methodology is common, which can apply any text file for secure transmission of the data[3].

In authors “Rosa Afrain**”** presented a novel method for image encryption which has completed by genetic algorithm. The input image of the rows and columns are dislocated randomly and acquired images are divided into four equal size sub-images. After that one of these sub-image is selected accidentally. Two pixels are chosen from that sub-image as genetic algorithm initial population. Both, the mutation and crossover operations are applied in the binary value of the chosen pixel value. Then reconstruct the image in reverse manner. Even the image entropy is increased that the current sub-images is utilized for the next procedure. Entropy, correlation, coefficient and histogram analysis is used to measure the randomness of an encrypted image. This accession is sensitive to the keys and small warp in them [4].

In author **“**ShubhanginiP.Nichat” presented the chaotic and secret key methods are used to create the different number of encrypted images. Algorithm of genetic moreover used to get the optimal result and in the last stage finest cipher image is selected as best; cipher image is protected on computation of the co-relation, co-efficient and entropy. The image has lowest correlation coefficient and maximum entropy is selected as the best cipher image[5].

III.IEGA METHOD

A. Architecture Diagram

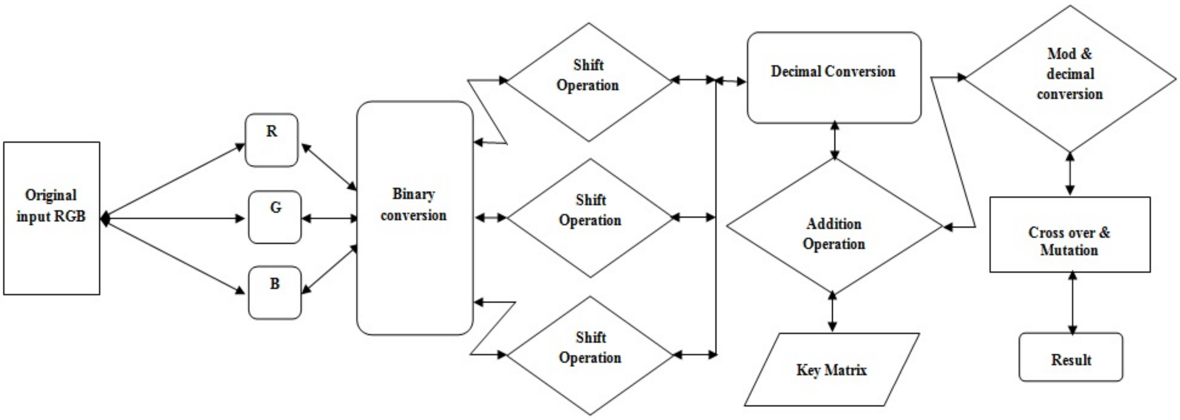


Fig. 1.Architecture model of IEGA method.

B. IEGA method steps

In this paper new image encryption method is proposed based on improved genetic algorithm and also uses symmetric key encryption

*Walk 1***:** Get the original RGB image as an input. To obtain the pixel values use row and column based on the height and width of [X,Y co-ordination] of IRGB.

*Walk 2***:** mine the RGB color value from the input image, which has 256 pixel values.

$$I_{RGB}=\begin{bmatrix}(20,40,60) & (60,20,70) & (20,20,80)\\ (30,50,40) & (75,65,55) & (25,25,40)\\ (25,45,35) & (15,45,55) & (75,65,85)\end{bmatrix}$$

*Walk 3***:** Extracted RGB color components values are split in matrix fashion.

$$R_i=\begin{bmatrix}20 & 60 & 20\\ 30 & 75 & 25\\ 25 & 15 & 75\end{bmatrix} G_i=\begin{bmatrix}40 & 20 & 20\\ 50 & 65 & 25\\ 45 & 45 & 75\end{bmatrix} B_i=\begin{bmatrix}60 & 70 & 80\\ 40 & 55 & 40\\ 35 & 55 & 85\end{bmatrix}$$

*Walk 4***:** R_i, G_i, Bi matrices are converted as binary matrix with the help of BCD conversion.

$$R_{Bi}=\begin{bmatrix}00010100 & 00111100 & 00010100\\ 00011110 & 01001011 & 00011001\\ 00011001 & 00001111 & 01001011\end{bmatrix}\quad G_{Bi}=\begin{bmatrix}00101000 & 00010110 & 00010100\\ 00110010 & 01000001 & 00011011\\ 00101101 & 00101101 & 01000001\end{bmatrix}$$

$$B_{Bi}=\begin{bmatrix}00111100 & 01000110 & 01010000\\ 00101000 & 00110111 & 00101000\\ 00100011 & 00110111 & 01010101\end{bmatrix}$$

Walk 5: Shift Right 2 bits from R_{Bi}, G_{Bi}, B_{Bi}.

$$R_{Si}=\begin{bmatrix}00000101 & 00001111 & 00000101\\ 10000111 & 11010010 & 01000111\\ 01000110 & 11000011 & 11010010\end{bmatrix}\quad G_{Si}=\begin{bmatrix}00001010 & 00000101 & 00000101\\ 10001100 & 01010000 & 01000111\\ 01001011 & 01001011 & 01010000\end{bmatrix}$$

$$B_{Si}=\begin{bmatrix}00001111 & 10010011 & 00010100\\ 00001010 & 11001101 & 00001010\\ 11001000 & 11001101 & 01010101\end{bmatrix}$$

Walk 6: Convert into equivalent decimal values of R_{Si}, G_{Si} and B_{Si}.

$$R_{1i}=\begin{bmatrix}5 & 15 & 5\\ 135 & 210 & 34\\ 70 & 195 & 210\end{bmatrix}\quad G_{1i}=\begin{bmatrix}10 & 5 & 5\\ 140 & 80 & 35\\ 75 & 75 & 80\end{bmatrix}\quad B_{1i}=\begin{bmatrix}15 & 145 & 20\\ 10 & 205 & 10\\ 200 & 205 & 85\end{bmatrix}$$

Walk7: Let produce the matrix arbitrarily with the size of input image size then transpose rows and columns values consider as a key matrix(K_m).for example

$$K_m=\begin{bmatrix}50 & 70 & 40\\ 40 & 15 & 25\\ 25 & 15 & 75\end{bmatrix}$$

Walk8: Addictive matrix operation is applied on the R_{1i},G_{1i}, B_{1i} with Km. Here, the mod operation is also performed. Because pixel value should be within the 0-255

$$R_{2i} = (R_{1i}+K_m) \bmod 256$$

$$G_{2i} = (G_{1i}+K_m) \bmod 256$$

$$B_{2i} = (B_{1i}+K_m) \bmod 256$$

$$R_{2i} = \begin{bmatrix} 55 & 85 & 45 \\ 175 & 225 & 59 \\ 95 & 210 & 29 \end{bmatrix} G_{2i} = \begin{bmatrix} 60 & 75 & 45 \\ 180 & 95 & 60 \\ 100 & 90 & 155 \end{bmatrix} B_{2i} = \begin{bmatrix} 65 & 215 & 60 \\ 50 & 220 & 35 \\ 225 & 220 & 160 \end{bmatrix}$$

Walk 9: Change as Binary Value from R_{2i},G_{2i} and B_{2i} Matrix

$$R_{2i} = \begin{bmatrix} 00110111 & 01010101 & 00101101 \\ 10101111 & 11100001 & 00111011 \\ 01011111 & 11010010 & 00011101 \end{bmatrix} \qquad G_{2i} = \begin{bmatrix} 00111100 & 01001011 & 00101101 \\ 10110100 & 01011111 & 00111100 \\ 01100100 & 01011010 & 10011011 \end{bmatrix}$$

$$B_{2i} = \begin{bmatrix} 01000001 & 11010111 & 00111100 \\ 00110010 & 11011100 & 00100011 \\ 11100001 & 11011100 & 10100000 \end{bmatrix}$$

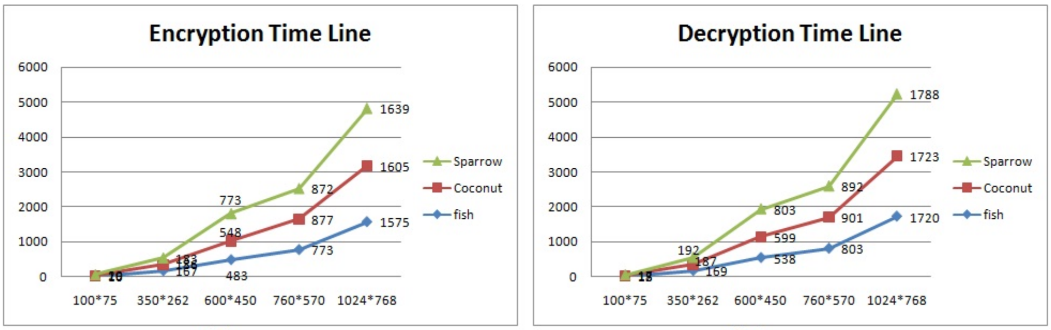
Walk 10: Cross-Over and Mutation

001101110101010100101101001111000100101100101101101101000101111100111100011001000101101010
0110111010111111110000100111011010111111101001000011101010000011101011100111100001100101101
11000010001111110000011101110010100000

1) *Cross-Over:* 0011011101010101001011010011110001001011001011011011010001011111001111000110 01000101101010011011101011111110
2) *Mutation:* 001001110110101111111010010000111010100000111010111001111000011001011011100001 0001111110000011101110010100000

IV.RESULT AND DISCUSSION

IEGA method, flow of process works as efficient. This method has taken the input as various types of resolution and image (1024*768, 760*570, 600*450, 350*262, 100*75) for the experimental work. Outcome of the encryption and decryption progression is dependent on the image size. Different Resolutions of the image size, which could get the too large dimensions, will be slight variation in result. Based on the experimental result IEGA method progression is direct proportional and get the less consumption time in Mille-Second (ms) for en-chiperment process.



(a) (b)

Fig. 2 (a) Encryption Time (b) Decryption Time

The above fig 2 demonstrates IEGA method encryption and decryption time scaling respectively

V. CONCLUSION

Data security is most essential to transfer the tenable data in the network system. Every day, new innovations have been inventing till now by the cryptography mechanism. But it's requirement is needed to be in recent trends of technology and even the data gets more security to data transfer rather than process of data security has also more significant. For that reason the novel approach has derived for image encryption, which is called Image En-cipherment using Genetic Algorithm (IEGA). This method extracts the RGB value from the original input image and converts it into the binary value. Various types of images and its resolutions have taken as the input values. Based on the experimental result this method is reduced the time complexity of image encryption.

REFERENCES

[1] Xingyuan Wang and DahaiXu, “ImageEncryption using genetic operator and intertwinging logistic map”, Nonlinear Dynamics, Vol.78, issue.4, page(s): 2975-2984, 2014.
[2] EnayatifarRasul and Abdul Hanan Abdullah, “Image security via genetic algorithm”, International Conference On Computer and Software Modeling Vol 14, 2011.
[3] NaikPoornima G and Girish R Naik, “ Asymmetric Key Encryption using Genetic Algorithm.” International Journal of Latest Trends in Engineering and Technology (IJLTET) issue.3.3, page(s):118-128, (2014).
[4] AfarinRoza and SaeedMozaffari, “Image encryption using genetic algorithm” Machine Vision and Image Processing (MVIP), 8th Iranian Conference on IEEE, 2013.
[5] NichatShubhangini P and S SSikchi“ Image encryption using hybrid genetic algorithm” IJARCSSE Vol:3.1, 2013.
[6] Dwivedi, Neha, Rishi Kumar Gupta, and ShafaliAgarwal. "Image Encryption using Curved Scrambling and Diffusion."IJETVol: 8 No. 6, 2016

AUTHOR PROFILE

Arunpandian S received the Master’s Degree in Computer Applications from the Bharathidhasan University, Trichy, Tamilnadu, India, in 2015, and currently pursuing the M.phil degree at Alagappa University, Karaikudi, Tamilnadu, India.Who has Research interest in Cryptography and Big Data & Analytics

Dr. K. Mahesh, who is a faculty member in Department of computer Applications at Alagappa University, Karaikudi, India, he has published many papers in the national and international journals and who has 25 years of experience in teaching. His research interest is video segmentation, video processing and image processing.