JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-6, Aug 2016 E-ISSN: 2347-2693

Fuzzy-Ga Combined Approach in Image Encryption

Subhajit Das[1*], SatyendraNath Mandal[2], Sunil Karforma[3]

[1] *NayagramBaniBidyapith, Nayagram, India*
[2]*Kalyani Govt. EnggCollege,Dept.of Information Tech. Kalyani,Nadia,India*
[3]Burdwan University,Dept of Computer Science, Burdwan,India

Available online at: www.ijcseonline.org

Received: Jun/29/2016 Revised: July/09/2016 Accepted: July/26/2016 Published: Aug/12/2016

***Abstract*—**: Many algorithms have been developed to encrypt digital image. In this paper Fuzzy set theory in combination with genetic algorithm has been applied to encrypt the image. Genetic algorithm is used for key generation and fuzzy set theory has been used to diffuse original image .The encrypted image is obtained after logical operation between the key set and diffused image. A number of tests have been applied on encrypted image to check the security level of the proposed algorithm.

***Keywords*—**Fuzzy Logic, Genetic Algorithm, Selective Cross Over, Diffused Image, Compression Rule

I. INTRODUCTION

In the age of globalization secure transmission of digital image through internet is a real challenge to the researchers because traditional cryptographic algorithm is not a good idea for image encryption. The main characteristics of image encryption algorithm is that image size is almost grater then text size and for image encryption it is not needed that decrypted image must be fully equal to input image.[1][2] Many branches of sciences have been applied for image encryption. Among them soft computing tools like genetic algorithm, fuzzy logic, artificial neuron network etc. also been applied in image encryption to provide high security, low time requirement, high correlation among pixel and so on.RozaAfarin ,SaeedMozaffari[3]have proposed a Genetic algorithm and binary pattern based image encryption. Their proposed method uses three keys and consists of two phases, substitution phase and modification phase. In substitution phase Local Binary Pattern (LBP) operator and in modification phase Bit Plane Slicing (BPS) operator is used to generate chromosome.Genetic algorithm is applied in both the phases to reduce correlation among adjacent pixel and to encrypt the input image.Jalesh Kumar and S Nirmala demonstrate an image encryption algorithm based on genetic algorithm [4]. In their proposed method pseudorandom key sequence is generated using Linearcongruential generator then crossover operation is performed on input image. Finally mutation operation is performed on the result obtained from the previous stage to obtain cipher image.RasulEnayatifar et al. [5] used genetic algorithm to select best DNA mask among DNA masks that generated by using logistic map and DNA sequence. Fittest DNA mask is used to obtained cipher images.RavinduMadanayake et al.[6] have proposed an encryption algorithm using fuzzy logic. In their proposed encryption algorithm user can get desired security level and processing level by using various keys for the encryption/decryption process. This facility of the algorithm is achieved by fuzzy logic. Most of the authors [1]-[6] used either GA or fuzzy logic to obtain cipher image. But a powerful image encryption algorithm developed in this paper used fuzzy set theory and GA both. Proposed encryption algorithm consists of two phases, in the first phase fuzzy logic has been used to diffused the image and in second phase a bitwise logical operation has been used to encrypt the image. Image diffusion phase cast the image elements into confusion by changing the pixel value so that the input image is not recognizable. The purpose of this phase is to reduce the similarity and high relationship among neighboring pixels and it gives a better encrypted image. To enhance the security level of the encrypted image a logical operation has been performed between diffused image and key value in the second stage of the proposed algorithm. A genetic algorithm based keyword generation method has been used in our proposed algorithm to provide dissimilarity between input key value and effective key value and make confusion to the attacker.

II. 'S' SHAPED MEMBERSHIP FUNCTION

To obtain membership value of each pixel S shaped membership function has been used where this spline-based curve is a mapping on the vector x, and is named because of its S-shape. The parameters *a* and *b* locates the extremes of the sloped portion of the curve, as given by:

$$(x; a, b) = \begin{cases} 0 & x \le a \\ 2\left(\frac{x-a}{b-a}\right)^2 & a \le x \le \frac{a+b}{2} \\ 1 - 2\left(\frac{x-b}{b-a}\right)^2 & \frac{a+b}{2} \le x \le b \\ 1 & x \ge b \end{cases}$$

Value a and b have been used as a boundary value of each group in which the considering value is lying.

III. Selective Crossover

Selective crossover is very much like “dominance without diploidy”[7].In this type of crossover each gene associated with a dominance value. During recombination two parents are selected and their fitness is recorded .Here ‘Parent 1’ is considered as the contributor. The dominance value of each gene in both parents is compared linearly across the chromosome. The gene that has a higher dominance value contributes to ‘Child 1’ along with the dominance value. If both dominance values are equal then crossover does not occur at that position. Fig. 1 gives an example of selective crossover.

1	1	1	0	0	0	1	1
0.2	0.5	0.1	0.4	0.5	0.7	0.7	0.4

(a)

1	0	0	0	1	1	0	0
0.1	0.6	0.1	0.3	0.51	0.6	0.8	0.5

(b)

1	0	1	0	1	0	0	0
0.2	0.6	0.1	0.4	0.51	0.7	0.8	0.5

(c)

1	1	0	0	0	1	1	1
0.1	0.5	0.1	0.3	0.5	0.6	0.7	0.4

(d)

Fig 1:- a) and b) parent1 and parent 2 with dominance value c) and d) child 1 and child 2 after selective crossover.

IV. Proposed Algorithm

In this paper, images are encrypted by number of steps. The proposed algorithm has been divided into five parts key generation, image fuzzification, encryption, decryption and image defuzzification. First the image pixels have been altered by a set of predefined and compression rules. The key is generated and it has been applied on the altered image pixels for encryption of image .Same key has been used for decryption that prove proposed algorithm is a symmetric key algorithm. Total 256 types of grey values have been divided into 16 groups, group ‘0’ consists of value ranging from 0 to 15 ,group ‘1’ consists of value ranging from 16 to 31, group ‘2’ consist of values ranging from 32 to 63 and so on. These rules are furnished in table no 1.Membership value of each element have been calculated using ‘S’ shaped membership function .Input image has been converted into a fuzzy set where each element consist of its value and its corresponding membership value .In key word generation method ASCII value of each keyword character has been taken as its dominance value and genetic algorithm has been applied on them to generate effective key word.

A. Key word Generation

Genetic algorithm with selective crossover has been used to generate effective key value. In this method each individual chromosome has associated with a real valued vector, and thus each gene has an associated dominance value. The dominance values of each gene in both parents are compared linearly. The gene which has higher dominance value contributes to a child along with the dominance value and lower dominance value contributed to another child along with its dominance value. If both dominance values are equal, then no crossover occurs at that position. After crossover value of gene at last position is incremented by 1 and its corresponding variance value has been calculated. A fitness function has been applied to each chromosome to compute its fitness value.

1. To take a keyword containing at least 16 characters and total number of characters should be multiple of 8.
2. To divide all characters into equal length chromosomes(c_h) and each containing with 8 genes(g) (characters).

   $$c_h = \{g_1, g_2, \ldots\ldots\ldots.., g_8\}$$
3. To take 8 bit ASCII value of each gene.
4. To take ASCII value of each gene as their dominance value.
5. For each generation do
   - 5.1 To compare dominance value of each gene at specified position linearly.
   - 5.2 Higher dominance values contribute to child1.
   - 5.3 Lower dominance values contribute to child2.
   - 5.4 To perform mutation ASCII value of last gene (g_8) increased by 1if the value is 256 then it has been taken as zero.

5.5 To compute fitness value(f_{c_h}) of each chromosome.

$$f_{c_h} = \frac{tatal\ no\ of\ 1's\ in\ c_h}{length\ of\ c_h\ in\ bits\ .}$$

5.6 To comparefitness of parent with their child if fitness value of child is grater then the fitness value of their parent then decrease the dominance value of those genes that was not exchanged by basing factor (b_k)during crossover.

Here

$b_k = next\ higher\ value\ such\ that\ total\ no\ of\ 1\ in\ ASCII\ sequence\ is\ not\ changed.$

5.7 To take two chromosome having highest fitness value as two parent for next generation. End of for.

6. To take all the chromosomes form 1 to n generation collectively and treated as an effective key value (K).

B. Image fuzzification

Fuzzy set theory has been used to represent each pixel of input image. Fuzzy sets are sets whose elements have degree of membership. A fuzzy set is a pair (*U*,*m*) where *U* is a set and *m:U*[0,1] .For each $x \in U$, the value of *m(x)* is called the grade of membership of x in *(U,m).* The grade of membership i.e membership value of each *x* has been obtained by using several membership functions.

Input: Plane image

Output: Defused image

Step 1. The gray scale image is a set of pixels represented by matrix $\mathbb{M}$

$$\mathbb{M} = \{a_{ij}\}_{m\times n}$$

Step 2. A set of predefined rule have been applied to each a_{ij} to obtain b_{ij} .

Each b_{ij} has been used to represent both value and membership value of each a_{ij}.

Value of each a_{ij} has been lies between 0 to 255 i.e. $0 \le a_{ij} \le 255$.

Total 256 types of value have been divided into 16 groups group ‘0’ consists of value ranging from 0 to 15 ,group ‘1’ consists of value ranging from 16 to 31, group ‘2’ consist of values ranging from 32 to 63 and so on. In our proposed encryption algorithm these group values are useful for both fuzzification and also for defuzzification.Binary equivalent of the elements b_{ij} can be represented as

$b_{ij} = b_8^{ij} b_7^{ik} \dots\dots..b_1^{ik}$Where b_1^{ij},…,b_1^{ik},…..=0 or 1.

Group value of each a_{ij}has been represented by bit stream $\{\ b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\ \}$.

Membership value has been represented by bit stream $\{b_8^{ij}b_7^{ij}b_6^{ij}b_5^{ij}\ \}$.

Step 3. Sets of rule have been used to represent each a_{ij} has been described below.

Rule 1: If $(a_{ij} \ge 0\ and\ a_{ij} \le 15)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0000\ end.$

Rule 2: If $(a_{ij} \ge 16\ and\ a_{ij} \le 31)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0001\ end$

Rule 3: If $(a_{ij} \ge 32\ and\ a_{ij} \le 47)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0010\ end$

Rule 4: If $(a_{ij} \ge 48\ and\ a_{ij} \le 63)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0011\ end$

Rule 5: If $(a_{ij} \ge 64\ and\ a_{ij} \le 79)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0100\ end$

Rule 6: If $(a_{ij} \ge 80\ and\ a_{ij} \le 95)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0101\ end$

Rule 7: If $(a_{ij} \ge 96\ and\ a_{ij} \le 111)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0110\ end$

Rule 8: If$(112\ and\ a_{ij} \le 127)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0111\ end$

Rule 9:If$(a_{ij} \ge 128\ and\ a_{ij} \le 143)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1000\ end$

Rule10:If$(a_{ij} \ge 144\ and\ a_{ij} \le 159)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1001\ end$

Rule11:If$(a_{ij} \ge 160\ and\ a_{ij} \le 175)then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1010\ end$

Rule12:If$(a_{ij} \ge 176\ and\ a_{ij} \le 191)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1011\ end$

Rule13:If$(a_{ij} \ge 192\ and\ a_{ij} \le 207)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1100\ end$

Rule14:If$(a_{ij} \ge 208\ and\ a_{ij} \le 223)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1101\ end$

Rule15:If$(a_{ij} \ge 224\ and\ a_{ij} \le 239)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1110\ end$

Rule16:If$(a_{ij} \ge 240\ and\ a_{ij} \le 255)\ then\ \{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 1111\ end$

Step 4. S shaped membership function has been applied to each a_{ij}.Boundary values of each group in which a_{ij} lies have been taken as lower and upper limit. As each membership value lies between 0 to 1 i.e $\mu_{a_{ij}} \longrightarrow$ [0,1] for simplicity only one bit after decimal point has been consider to represent each membership value.For each b_{ij},$\{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\}$ have been used to represent value and remaining bits of b_{ij} i.e $\{b_8^{ij}b_7^{ij}b_6^{ij}b_5^{ij}\}$ have been used to represent membership value of each a_{ij}. Representation of membership value for all group elements along with their considering value have been furnished in table no 1.

Membership value	Considering value	$b_8^{ij}b_7^{ij}b_6^{ij}b_5^{ij}$
0.00	0	0000
0.0089	0	0000
0.0356	0	0000
0.0800	0	0000
0.1422	.1	0001
0.2222	.2	0010
0.3200	.3	0011
0.4356	.4	0100
0.5644	.5	0101
0.6800	.6	0110
0.7778	.7	0111
0.8578	.8	1000
0.9200	.9	1001
0.9644	.9	1001
0.9911	.9	1001
1	1	1111

Table 1:- Membership value and its representation

Step 5: The gray scale imageM is now converted in to diffused imageN

$$N= \{b_{ij}\}_{m\times n}$$

Example let value of a_{ij} be 123. So according to Rule 8 $\{b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij}\} = 0111$. 'S' shaped membership function has been applied to obtain the membership value of 123 with boundary value 112 and 127. So *m(123)*= 0.8578 .For presentation simplification 0.8578 has been taken as 0.8. According to table 1 $\{b_8^{ij}b_7^{ij}b_6^{ij}b_5^{ij}\} = 1000$.

Hence 123 can be represented as {1 0 0 0 0 1 1 1}.

C. Image Encryption.

Input: - Diffused image(N), Effective key value (K)Output: - Encrypted Image.

Method:

At this point logical XOR operation has been performed between each b_{ij} and each element of *K*starting from left corner of the plain image, to obtain an encrypted image. If total number of b_{ij} is grater then the number of elements *K* then *K* taken as circularly.

D. Image Decryption

Input: - An Encrypted image, Effective key value (K)

Output: - Diffused image(N).

Method:

To perform bitwise XOR between elements of set *K* and grey value of pixels starting from left corner of the encrypted image. If the number of pixels > number of elements of *K* then the elements of the *K*has to be taken circularly.

E. Image reconstruction

Input: - Diffused image

Output: - Plain Image.

Method: Following steps have been done on each pixel of diffused image to obtain the plain pixel value(a_{ij}).

Step1. To obtain the value of lower 4 bits of diffused image (group value).

$$x = val\ (b_4^{ij}b_3^{ij}b_2^{ij}b_1^{ij})$$

Step 2. To obtain the value of upper 4 bits of diffused image (membership value).

$$y = val\ (b_8^{ij}b_7^{ij}b_6^{ij}b_5^{ij})$$

Step 3.If y =15 then $a_{ij} = 16 \times x + 15$ Else $a_{ij} = 16 \times x + (4 + y)$.

Step 4. Do steps 1 to 3 for all (a_{ij})

V. Experimental Result

To test the performance of the proposed algorithm, it has been applied to some images in Fig 2 and the encrypted images are furnished in Fig 3. A stepwise implementation for our proposed algorithm also furnished in Fig. 4

Fig 2:- a)Lena b)Babun c)Monalisa d)Flower

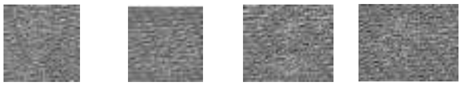


Fig 3:-:-a)Lenab)Babunc)Monalisa d)Flower

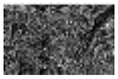
Input image	
Image after fuzzification	
Image after encryption.	

Fig 4:- A stepwise output of proposed algorithm

VI. Testing

A. Correlation Coefficient

Correlation issued to find out the degree of similarity between two variables .It is an important parameter to find the quality of image encryption algorithm .Any image encryption algorithm is said to be good if it hides all the attribute of plain image from its cipher image. If any cipher image and its corresponding plain image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. For two identical images correlation coefficient is equal to 1.To test the correlation between two adjacent pixels in plain-image and ciphered image, the following procedure was carried out. First, randomly select 2000 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels have been selectfrom an image. Then, calculate the correlation coefficient of each pair by using the following formulas:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))2$$

$$COV(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))$$

$$r=\frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

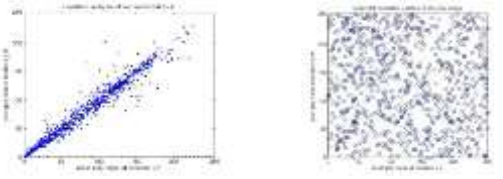
Where x and y are grey-scale values of two adjacent pixels in the image. N is the total number of pixels [1][4] .The correlation coefficients of horizontal, vertical and diagonal pixels of plain and encrypted images are shown in Table 3 and Table 4. The correlation distribution of two horizontally adjacentpixels and two vertically adjacent pixels of the plain image(Babun) and encrypted image(Babun) has been furnished in Fig.5 and Fig. 6 respectively. These correlation analysis prove that the proposed encryption algorithm satisfy zero co-correlation.

Table 3:- Correlation coefficient of two adjacent pixels in Plain image.

Image name	Plain image		
	Vertical	Horizontal	Diagonal
Lena	0.9374	0.9692	0.9107
Babun	0.9833	0.9823	0.9109
Monalisa	0.9809	0.9792	0.966
Flower	0.9544	0.9587	0.9287

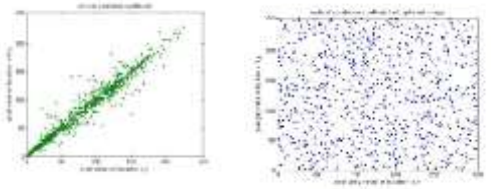
Table 4:- Correlation coefficient of two adjacent pixels Encrypted image.

Image name	Encrypted image		
	Vertical	Horizontal	Diagonal
Lena	0.0055	0.0012	0.0035
Babun	0.0008	0.0032	0.0027
Monalisa	0.0005	0.0045	0.0017
Flower	0.0055	0.0011	0.0063



(a) (b)

Fig 5:-a) The correlation analysis of two horizontallyadjacent pixels of Babun
b) The correlation analysis of two horizontally adjacent pixels of encrypted Babun.



(a) (b)

Fig 6:-a) The correlation analysis of two vertically adjacent pixels of Babun b) The correlation analysis of two vertically
adjacent pixels of encrypted Babun.

B. Compression Friendliness

Compression friendliness is one of the important properties in cryptography. An encryption algorithm is said to be compression friendly if it has small impact on data compression efficiency. In other words, it can be said if the size of encrypted image is same with the size of input image then the algorithm is said compression friendly. Size of input image and encrypted image-generated by our proposed algorithm have been showed in table4 and result prove that our proposed algorithm is compression friendly.

Table 4:- Input and encrypted image size.

Image name	Input image size(kb)	Encrypted imagesize (kb)
Lena	2	2
Babun	1	1
Monalisa	1	1
Flower	1	1

C. . Information Entropy Analysis

Imageentropy is a quantity which is used to describe the amount of information which must be coded by a compression algorithm. An image that is perfectly flat will have entropy of zero. Consequently, they can be compressed to a relatively small size. An image has a great deal of contrast from one pixel to the next, has high entropy value and consequently cannot be compressed as much as low entropy images. Low entropy images, have very little contrast and large runs of pixels with the same or similar DN values.Entropy value of an image defined as

$$H(m) = \sum p(m_i)\log_2 \frac{1}{p(m_i)}$$

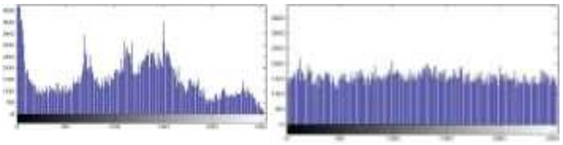
Where $p(m_i)$ represents the probability of the pixel value m_i .Theoretically, a true random system should generate 2^8 symbols with equal probability. Therefore, according to equation of H(m) entropy of the system willbe $H(m) = 8$ [5].Entropy value of plain image and its correspondent cipher image have been furnished in Table 5. The result proves that our proposed algorithm has the ability against entropy attack.

Table 5:- Entropy analysis of plain image and cipher image

Image name	Input image entropy	Encrypted image entropy
Lena	7.746	7.9952
Babun	7.4812	7.9985
Monalisa	7.4069	7.9933
Flower	7.2549	7.9744

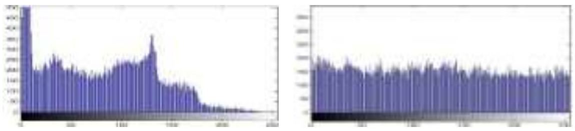
D. Histogram Analysis

An image-histogram describes how the image-pixels are distributed by plotting the number of pixels at each intensity level. The histogram represents the statistical characteristics of an image. If the histograms of the encrypted image are similar to the random image, the encryption algorithm has good performance. It is very difficult for an attacker to extract from the statistical nature of pixels the plain image out of the encrypted image. The histogram of plain and encrypted images has been furnished in fig 7



(a) (b)

Fig 7 :- a)Lena :histogram b)Encrypted lena: histogram



(c) (d)

c) Babun : histogram d) Encrypted Babun: histogram

VII. Conclusion

In this paper, a hybrid image encryption and decryption algorithm based on fuzzy set has been proposed. The correlation coefficient of adjacent pixels of the ciphered image obviate that the proposed algorithm has a good ability of diffusion and confusion and highly resistive against the statistical attack. Entropyvalue of every cipher image proves that information leakage is negligible.

References

[1] Nidhal K. El Abbadi, 2Adil Mohamad and 2Mohammed Abdul-Hameed, "Image Encryption Based on Singular Value Decomposition", Journal of Computer Science, 10 (7),Page No**(1222-1230) 2014**.

[2] HaojiangGao ,Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption" , Chaos,Solitons and Fractals ,ELSEVIER Page No.**393-399**,**2006.**

[3] RozaAfarin ,SaeedMozaffari, "Image Encryption Using Genetic Algorithm and Binary Pattern".

[4] Jalesh Kumar and S Nirmala, "Encryption of Images Based on Genetic Algorithm-A New Approach", Advances in Computer Science, Eng. & Appl., AISC 167.© Springer-Verlag Berlin Heidelberg, **Page No 783–791** , **2012.**

[5] Rasul Enayatifar , Abdul Hanan Abdullah, Ismail FauziIsnin, " Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence",Optics and Laser in Engineering 56 ELSEVIER, **Page No-83-93,2014.**

[6] Ravindu Madanayake, NikilaPeiris, GayanRanaweera and UthpalaJayathilake, "Advanced Encryption Algorithm Using Fuzzy Logic", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012) ACSIT Press, Singapore,2012.

[7] KantaVekaria and Chris Clack, "Selective Crossover in Genetic Algorithms: An Empirical Study".

[8] Cao Guanghui,Hu Kai, Zhang Yizhi, Zhou Jun, and Zhang Xing:Chaotic Image Encryption Based on Running-Key Related to Plaintext, Scientific World Journal Volume **2014**, Article ID 490179, 9 pages.

[9] M. El-lskandarani, S. Darwish, and S. Abuguba :A robust and secure scheme for image transmission over wireless channels in Security Technology,2008.ICCST 2008.42nd Annual IEEE International Carnahan Conference on. IEEE, ,**Page No 51–55, 2008.**