International Conference on Innovative Trends in Electronics Communication and Applications 2015 [ICIECA 2015]

ISBN	978-81-929742-6-2
Website	icieca.in
Received	02 - April - 2015
Article ID	ICIECA007

VOL	01
eMail	icieca@asdf.res.in
Accepted	15 - November - 2015
eAID	ICIECA.2015.007

A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos

R Ranjith kumar[1], S Jayasudha[1], S Pradeep[2]
[1]Assistant Professor, [2] UG scholars
Department of ECE, P.A. College of Engineering and Technology, India

Abstract: *This paper focuses on a symmetric image encryption scheme that exploits the basis of genetic algorithm and chaos. The proposed scheme employs only one round encryption to achieve the satisfactory level of security. Plain image is converted into bit stream and the cross over operation in GA is used to perform the modification of pixel in bit level and the population for GA is believed to be the bytes in binary format of the plain image. The key generator [18] that employs chaotic maps increases the sensitivity of the external keys. It is the seed to generate the Random number sequence (RNS) and Mask. RNS is used for crossover operation and Mask is used for breaking correlation among the pixels after crossover. The statistical and experimental results prove the robustness of the proposed scheme.*

Keywords: Genetic algorithm, Chaos, Image encryption, Logistic map

INTRODUCTION

The world and the technologies in it are developing in a faster manner, so the threat of secure transmission of the information is essential. The amount of information being transferred in the internet has been increased a lot in these decades. Most of the information is in the form of images. The main question to be asked is that, are these images transferred in a safe manner? The answer for this question is may be or may not be. There is an essentiality that most important information like military and medical images should be transferred with high security. For the transfer of high risk images image processing is a boon. The images have to be modified in a certain way that none could able to access the original information behind it except the sender. This is so called encryption of the image. Many schemes have been proposed in the recent years which are based on many logics. The proposed system is based on GA (Genetic Algorithm) and Chaotic systems.

Genetic algorithms which are commonly called as GA was first developed in order to mimic some of the naturally occurring processes [1]. But in recent days its use has been extended in the processing of images. With the help of GA the encryption of the images can be performed in a better way than many other concepts and it is secure since it is not utilising the natural numbers directly. One of the main notions of the GA is crossover which employs the swapping of data between two points in a byte which is selected by the key given by the user. There are many a type of crossover namely single point crossover, two point crossover, three parent crossover and uniform crossover [2]. The proposed system uses two point crossover techniques, according to which random points are selected and the crossover operation is carried out. Hence the crossover concept of GA plays vital role in the proposed scheme.

The second and the foremost important concept used in the proposed scheme is Chaos [3]. In 1991, thoshiki habutus [4] proposed a system where the cipher image can be obtained by the inverse chaotic mapping concept. Chaos theory has been spread out in many areas where image processing also owns its place [5]-[15] as the system which is built with the chaos has high security and highly sensitive to the conditions which are given at the initial state and the failure of the system is almost rare. Hence the utilisation of the

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. “A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos”. *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

basis of chaos in the field of image processing keeps on growing. The proposed method combines the elements of GA and Chaos to develop a secure image encryption scheme. It utilizes the key generator [18].The plain image is converted into its binary format and the cross over is performed to modify the pixels in the first stage and the Mask generated from the chaotic maps is applied on the output of the first stage to increase the robustness of the scheme. The proposed system achieves the required level of security in single round [16][17].Different analyses performed on the cipher image proves the randomness and robustness of the cipher. The rest of this paper is managed as follows, section 2 depicts proposed method, and section 3 furnishes the results of various analyses and section 4 is the conclusion.

PROPOSED METHOD

Figure 1 shows the block diagram of proposed method. The plain image of size MxN (8 bpp) is primarily converted into its binary format (I_b) of size (MxN)xn, where n represents the number of bits required for representing a pixel (in this case n=8). Each row of resulting I_b will own a single pixel. I_b is believed as the initial population for the basis of GA. The proposed scheme utilises the crossover operation in GA in order to perform the modification in the initial pixels before the application of the mask. The RNS produces two different random sequences to carry out the crossover among the rows of I_b. After performing the crossover, Modified I_b of size (MxN)xn is then converted into MxN image. This image is then fed into the next section where MxN mask is available for performing the XOR operation. The final image after applying the above process is called as the cipher image. The RNS and Mask obtains the initial seed from the key generator.

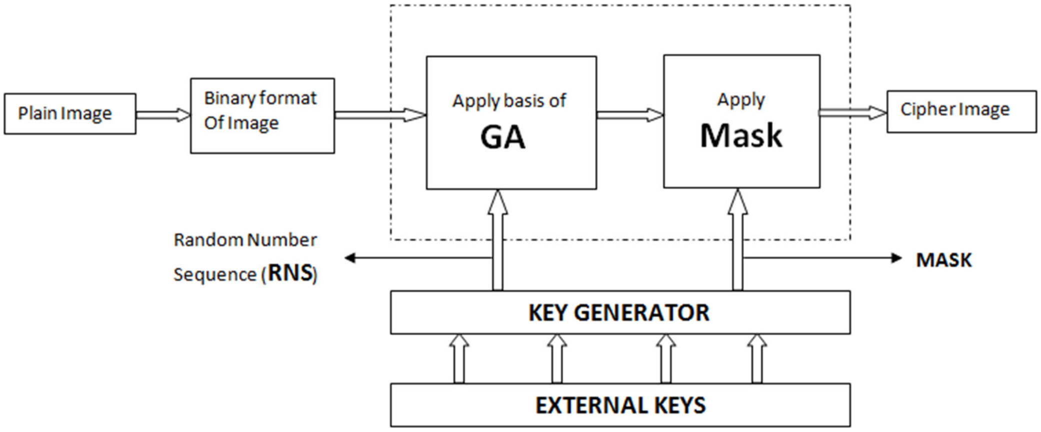

Figure 1 Proposed method

RNS and MASK GENERATION

The proposed system gives rise to 4 keys, each of 53 bits in size. These external keys are fed as the input for key generator [18] in order to increase the sensitivity of keys. The generated external keys are then seeded to generate RNS and apply the mask to it.

RNS

Let the seed from the key generator be X_{i1}, then two random number sequence are generated with respect to this seed.

RNSS (random number sequence for selection): This sequence will be in the order of 1 to (MxN).it is generated by chaotic logistic map of the equation,

$$Y_{i+1}=by_i(1-y_i) \tag{1}$$

where b is greater than 3.7 to get chaotic behaviour. RNSS is used for random selection in I_b,

$$\text{RNSS} = (Y \text{ x } 10^{14} \bmod (\text{MxN})) + 1 \tag{2}$$

RNSS will be a 1x(MxN) vector.Pseudo code 1 shows the procedure for generating RNSS.

RNSCO (random number sequence for crossover): This sequence will be in the range of 2-5, since the cross over is performed on 8 bits. Chaotic tent map is used for the generation of RNSCO,

$$Z_{i+1} = \left\{\begin{matrix} \mu Zi & Zi \leq 0.5 \\ \mu(1-Zi) & Zi > 0.5 \end{matrix}\right\} \tag{3}$$

where μ>1.9 for chaotic behaviour. The range 2-5 can be achieved by the following equation.

$$\text{RNSCO} = (\text{Z x } 10^{14} \bmod 4) + 2 \tag{4}$$

RNSCO will be a 1x((MxN)/2) vector.pseudo code 2 shows this process.

MASK GENERATION

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. "A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

The size of the mask is as same as the size of the plain image (i.e., MxN). The internal key from the key generator X_{i2} is used as the seed for the generation of the mask. The values in the mask are in the range of (0-255). Both the logistic and the tent map are used for the generation of the mask. ie., LT [18] system is used by which the total space is divided into two. For the odd places, the logistic map is used and for the even places, tent map is used.

$$\text{Mask}_{i+1} = b \text{ x } \text{mask}_i \text{ x } (1\text{-mask}_i), \quad \text{for i= 1,3,5,7,........ (MxN)-1}$$

$$\text{Mask}_{i+1} = \begin{cases} \mu \ x \ maski & maski \leq 0.5 \\ \mu(1 - maski) & maski > 0.5 \end{cases} \quad \text{for i= 2,4,6,8................(MxN)} \qquad (5)$$

Finally the mask is reshaped from 1x(MxN) to MxN. The generated values are then modified into the range (0-255) using,

$$\text{Final\_mask} = (\text{Mask x } 10^{14} \text{ mod } 256) \qquad (6)$$

Refer pseudo code 3 for this process.

BASIS OF GA and MASKING

The 'apply basis of GA' block will perform the cross over operation on I_b. A pair is selected from I_b based on RNSS values and crossover is applied on the selected pair. The modified values will be placed on the locations where the pair was taken. The following steps explain this process.

Step 1: Get RNSS vector of size 1x(MxN) that has values in the range(1 to MxN). For each pair of value in RNSS get the corresponding values of I_b in A and B.

$A = I_b(\text{RNSS(i)})$ i.e.. i^{th} row of I_b

$B = I_b(\text{RNSS(i+1)})$ i.e.. $i+1^{th}$ row of I_b

Step 2: Get RNSCO vector of size 1x((MxN)/2).Each value in RNSCO determines the cross over point for the pair A,B.

Let A = [0 0 0 0 1 1 1 1] , B = [1 1 1 1 0 0 0 0] and RNSCO = 4

Then cross over is applied as shown below,

$A = [\ 0\ 0\ 0\ 0\ \underline{1\ 1\ 1\ 1}]$ $B = [1\ 1\ 1\ 1\ \underline{0\ 0\ 0\ 0}]$

A_modified = [0 0 0 0 0 0 0 0] B_modified = [1 1 1 1 1 1 1 1]

Step 3: Replace existing values of A and B in I_b with modified values(i.e.. update I_b).

Step 4: Increment i and repeat step 1 – 3 until i reaches the end of RNSS.

Step 5: Convert the updated I_b into pixels and resize the result to MxN.

Even though this modification of pixels breaks the correlation among the pixels, there is a possibility of unchanged pixels in plain image after the application of GA. If A and B are same then cross over will not modify the value of pixel according to the steps explained above. To completely break the correlation among the pixels, one more technique called masking is employed. The block named 'apply mask' will perform this operation. The Mask generated by the LT system is applied to the output from the GA block. The resulting image is called cipher image which is completely random in nature. Single round is enough for the cipher is enough to attain the required level of security and is proved using various statistical and differential analyses in section 3.

Pseudo code 1:

```
        Initialize i =1;
        y[i] = X_i1;
  // X_i1 is initial seed from key
//generator
        for i=1: M*N-1
        y[i+1] = 4*y[i]*(1-y[i]);  //
y is a vector of 1 x (MxN)
          end
  RNSS = mod ( y*10^14 , MxN) + 1
```

Pseudo code 2:

```
          Initialize i =1;
        z[i] = X_i1;
  // X_i1 is initial seed from key
//generator
        for i=1: M*N / 2
        if z[i] <= 0.5
        z[i+1] = 2*z[i];
  // z is a vector of 1 x (MxN / 2)
        else
         z[i+1] = 2*(1-z[i]);
          end
          end
   RNSCO = mod ( z*10^14 , 4) + 2
```

Pseudo code 3:

```
        Initialize i =1;
        Mask[i] = X_i2;
// X_i2 is initial seed from key //generator
         for i=1: M*N
           if  i+1 is even:
         if Mask[i] <= 0.5
         Mask[i+1] = 2*Mask[i];
   // z is a vector of 1 x (MxN)
         else
           Mask[i+1] = 2*(1-Mask[i]);
           end
           if i+1 is odd:
     Mask[i+1] = 4*Mask[i]*(1-Mask[i])
            end
Mask = mod ( Mask*10^14 , 256)
Mask = reshape(Mask,[M N])
```

PERFORMANCE ANALYSIS

KEY SPACE ANALYSIS

A key space of 2^{212} is used in the proposed scheme which is much more sufficient for security. The two important aspects that are contained by the key are exhaustive search that characterise the ability to withstand any type of brute force attack and non-recovery property that specifies how strong the key is infeasible to the attacks. To maintain the system in its high secure state the minimum value of R (number of rounds) can be obtained from the relation [11],

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. "A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

$$R = floor\left[\frac{128}{\log_2 L}\right] + 1 \tag{7}$$

since L = 212 in this system, R = 1.From the NPCR,UACI,NBCR and MAE values which are in Table 2., it can be seen that the system has much more resistance and can withstand any kind of brute-force attacks and requires just an one round encryption

STATISTICAL ANALYSIS

These are the tests which are mainly employed to investigate the robustness of the system which can be calculated by histograms and correlation coefficients of both the plain image and cipher image.

HISTOGRAM ANALYSIS

Histograms are the graphs which are drawn between pixel intensity and their number of occurrences. Each image possesses its own histograms which are widely different from one another. Here image encryption schemes modify the histogram to avoid known plain text attacks. Figure 2 (a) and (b) shows the original image and its corresponding encrypted image. Figure 2(c) and (d) shows their respective histograms. The proposed scheme completely flattens the histogram which shows the encrypted image has pixels that are having approximately equal number of occurrences. It proves the randomness of the cipher image.

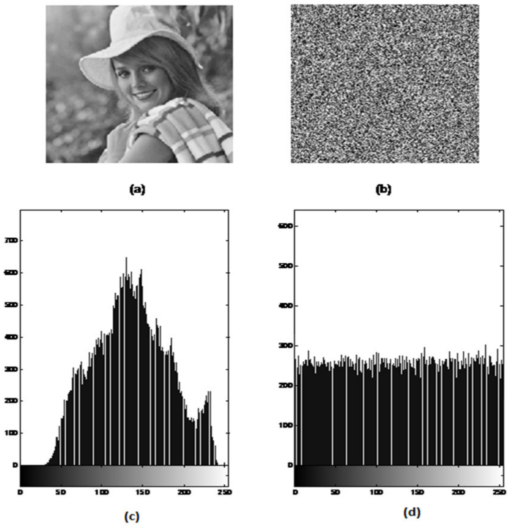

Figure 2 Histogram analysis (a) Plain image (b) Encrypted image (c) Histogram of plain image
(d) Histogram of Encrypted image

CORRELATION COEFFICIENT ANALYSIS

Correlation between the pixels of the image must also be analyzed to check the robustness of the system. Generally the correlation between the adjacent pixels in the original images is high but for a good encrypted image it has to me minimised. This analysis is carried out by selecting 10,000 pairs randomly in the manner that they are horizontally, vertically and diagonally adjacent. The correlation can be calculated by using the formula,

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x,y)\sqrt{D(y)}}} \tag{8}$$

where,

$$\mathrm{cov}(x,y) = E\{(x - E(x)) - (y - E(y))\}$$

where, x and y denotes the two adjacent pixels in the image and E(x) and D(y) denotes the mean and standard deviation of corresponding grey levels. Correlation coefficients are compared with different algorithms and tabulated in Table 1.From Table 1, the correlation which is nearly 1 for the plain image is broken nearly to 0 which means that the encrypted image is highly uncorrelated.

INFORMATION ENTROPY ANALYSIS

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. "A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

Information entropy is generally to describe the degree of uncertainty that is present in a system and can be calculated by using the formula,

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)} \tag{9}$$

where, m and p (m_i) represents the total number of symbols and probability of occurrence of the symbol respectively. In practical, the information entropy generates random messages but is expected to have a value which is less than ideal one (in this case 8).Entropy must be same as ideal for cipher image so that the enemy cannot guess any part of the image. Table 2 proves the above statement, which the entropy values of the cipher nearly equal to 8 (ideal).

DIFFERENTIAL ATTACK

NPCR and UACI: When a system must resist all kind of attacks it should always be sensitive even a fraction change in the plaintext and key. NPCR and UACI which have been proposed by the NIST [19] are the mostly used methods for testing the sensitivity.

$$NPCR = \frac{1}{n} \| \{ i \mid x_i \neq y_i, i = 0,1,\ldots n-1 \} \| \tag{10}$$

$$UACI = \frac{1}{n} \sum_{i}^{n-1} \frac{| x_i - y_i |}{255} \tag{11}$$

Given two images $x = \{x0, x1, \ldots, xn\text{-}1\}$ and $y = \{y0, y1, \ldots, yn\text{-}1\}$, the NPCR and UACI are defined in Eq.(8) and Eq.(9) [18]. For two random images, the average NPCR is about 0.9961, and the average UACI is about 0.3346 [19]. The NPCR and UACI values for various images are calculated and tabulated in Table 2.

MAE: Mean Absolute Error is an another method to perform the tests on the system against differential attacks[16]. Let C(i, j) and P(i, j) be the gray level of the pixels at the i^{th} row and j^{th} column of a M×N cipher and plain-image, respectively. Then the mean absolute error can be calculated using the formula,

$$MAE = \frac{1}{M \times N} \sum_{j=0}^{N} \sum_{i=0}^{M} | c(i,j) - p(i,j) | \tag{12}$$

The values for various images are calculated and are tabulated in Table 2. Larger value of MAE indicate better security[16].

Strict Avalanche Criterion: The strict avalanche criterion (SAC) is intended to examine the changes in bit-level. According to SAC a single bit change in input will lead to an inundation change in the output. The Number of Bit Change Rate (NBCR) is defined in [20] and is used to measure the SAC performance using Eq.(13).The ideal NBCR is 50% in average [20]:

$$NBCR = \frac{H_m[s_1, s_2]}{L_b} \times 100 \tag{13}$$

H_m[.] calculates the Hamming distance between two encrypted bit streams(s_1 and s_2) obtained by slight difference in the key. L_b is length of the bit stream. The NBCR values listed in Table 2 shows that the system performs efficiently against the differential attacks in bit level.

Randomness test with sp800-22 test suite: The two main strategies which are recommended by the NIST [23] to perform the analysis on the system are checking the P-values that are uniformly distributed over the interval [0, 1] and comparison of the expected value with the value that are calculated from the proportion of the sequence. A large sequence of the binary number has been employed in checking the uniform distribution of the P-value in each test that has been performed. The computation is as follows:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - N/10)}{N/10} \tag{14}$$

Where F_i represents the number of occurrences that the P-value contains in i^{th} interval and N denotes the size of the sample. The P-values can be calculated from the following Eq.

$$P - Value = igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right) \tag{15}$$

Here, igmac is the incomplete Gamma function. When the P-values are greater than or equal to 0.0001 then it shows that the encrypted image has P-values that are distributed uniformly. The outcomes are tabulated in Table 3. The encrypted image given by the proposed system has passed all the tests and also proved that its distribution is uniform. Hence from the NIST test it can be concluded that the encrypted image from the proposed system is highly random in nature.

Table 1. Comparison of correlation coefficients.

Scheme	Horizontal	Vertical	Diagonal
Original Lena image	0.9882	0.9856	0.9669
AES[19]	0.0770	0.0660	-
Algorithm[21]	0.0845	0.0681	-
Algorithm[22]	0.0965	-0.0318	
Algorithm[18]	-0.0094	-0.0003	-0.0039
Algorithm[17]	0.0015	0.0069	0.0018
Proposed method	-0.0006	-0.0021	0.0022

Table3. NIST Test results

Statistical Test		P-Value	Result
Frequency		0.6065	Success
Block Frequency		0.5502	Success
Runs		0.0852	Success
Statistical test		0.5322	Success
Long runs of one‘s		1.0000	Success
Binary Matrix Rank		0.4015	Success
Spectral DFT		1.0000	Success
No overlapping templates		0.7312	Success
Overlapping templates		0.9983	Success
Universal		0.6642	Success
Serial	P – Value 1	0.8526	Success
	P – Value 2	0.4029	
Approximate Entropy		0.5816	Success
Cumulative sums		0.5753	Success
Random excursions		0.7725	Success
Random excursions variant		0.4959	Success

CONCLUSION

The proposed encryption scheme utilizes the basis of GA and Chaos to develop a secure image encryption scheme. A mixture of analyses has been carried out to prove the security level of proposed encryption scheme. The proposed method uses crossover operation in GA to perform pixel modification in bit level. Chaotic maps are utilized to generate random number sequences for the assist of crossover and Mask generation. It has a superior sensitivity to the little change in the key due to the structure proposed for key generation and has single round to achieve the necessitated security. The results of various tests like NPCR, UACI, MAE and NBCR proves that the system is robust and can survive against any security attack.

Table 1. Differential and Entropy analysis

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. “A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos”. *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

S.NO	IMAGE	ENTROPY		NPCR	UACI	MAE	NBCR
		Plain	Cipher				
1.	5.1.09.tiff	6.7093	7.9967	0.9963	0.3335	67.1615	49.8772
2.	5.1.11.tiff	6.4523	7.9971	0.9962	0.3350	85.6294	49.9851
3.	aerial.bmp	6.9940	7.9971	0.9959	0.3339	80.3379	49.9743
4.	airfield.bmp	6.8303	7.9967	0.9960	0.3352	82.1247	50.0040
5.	bananas.png	7.1883	7.9968	0.9966	0.3342	92.985	49.9851
6.	almonds.png	7.3286	7.9965	0.9965	0.3333	77.8629	49.9847
7.	apples.png	7.6688	7.9965	0.9960	0.3328	85.0347	49.8781
8.	baloons.png	7.6934	7.9966	0.9955	0.3347	78.3416	50.0355
9.	barbara.bmp	4.4858	7.9968	0.9959	0.3347	107.439	50.0502
10.	billiard_ball.png	7.8777	7.9971	0.9963	0.3334	86.9552	49.9750
11.	boat..tiff	7.1914	7.9964	0.9960	0.3334	68.4918	49.8974
12.	bridge.bmp	5.7056	7.9972	0.9962	0.3336	80.381	49.8699
13.	building.png	7.4974	7.9967	0.9962	0.3348	81.6513	50.0507
14.	cameraman.bmp	6.9046	7.9969	0.9954	0.3345	88.3031	49.9626
15.	cards.png	7.7015	7.9966	0.9956	0.3339	89.4539	50.0629
16.	carrots.png	7.2489	7.9966	0.9961	0.3341	83.1118	49.9954
17.	chairs.png	7.0077	7.9968	0.9958	0.3343	77.0681	49.8800
18.	clips.png	7.8975	7.9965	0.9963	0.3339	87.1048	50.0389
19.	clown.bmp	5.3684	7.9972	0.9959	0.3338	94.5873	50.1364
20.	coins.png	7.4779	7.9966	0.9964	0.3356	81.8701	50.0628
21.	couple.bmp	7.0572	7.9964	0.9957	0.3331	68.3726	50.1125
22.	crowd.bmp	6.7893	7.9975	0.9959	0.3341	78.1304	50.0637
23.	cushions.png	7.8200	7.9969	0.9961	0.3353	85.7439	50.1371
24.	dollar.bmp	6.9785	7.9967	0.9963	0.3350	85.6641	50.0174
25.	ducks.png	7.7216	7.9968	0.9962	0.3350	76.9442	49.9933
26.	fence.png	7.5103	7.9968	0.9960	0.3340	81.5195	49.9041
27.	finger.bmp	7.1075	7.9970	0.9964	0.3336	71.5721	49.9588
28.	flowers.png	7.9327	7.9966	0.9961	0.3350	84.1959	49.9222
29.	garden_table.png	7.5886	7.9971	0.9956	0.3344	77.1007	49.9699
30.	girlface.bmp	7.0818	7.9968	0.9964	0.3348	82.3625	50.0423
31.	goldhill.bmp	4.5028	7.9971	0.9961	0.3352	107.701	49.9784
32.	guitar_bridge.png	7.2723	7.9970	0.9959	0.3346	84.7575	50.0929
33.	lighthouse.bmp	7.4486	7.9970	0.9960	0.3353	73.0076	49.9535
34.	houses.bmp	7.6548	7.9971	0.9960	0.3350	79.1343	50.0881
35.	trucks.bmp	6.5632	7.9964	0.9964	0.3341	71.2126	49.9289
36.	keyboard.png	6.5977	7.9966	0.9962	0.3355	84.3599	50.0332
37.	kiel.bmp	6.9589	7.9964	0.9961	0.3367	70.2597	50.0151
38.	snails.png	7.6659	7.9970	0.9963	0.3350	86.0029	49.9506
39.	lena.tif	7.4451	7.9967	0.9961	0.3347	68.3637	50.0689
40.	lion.png	7.1707	7.9974	0.9960	0.3348	90.2793	49.9369
41.	livingroom.tif	7.2952	7.9969	0.9962	0.3350	68.4693	50.0715
42.	mandril_gray.tif	7.2925	7.9969	0.9965	0.3350	71.3210	50.0198
43.	mountain.bmp	4.7981	7.9974	0.9966	0.3351	105.637	50.0263
44.	pencils.png	7.8439	7.9968	0.9959	0.3335	79.1839	50.0656
45.	guitar_head.png	7.4193	7.9964	0.9965	0.3338	82.3748	49.9245
46.	woman_blonde.tif	6.9542	7.9964	0.9956	0.3336	70.8953	49.9054

REFERENCES

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. "A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.

[1] S. N. Sivanandan, S. N. Deepa, “Introduction to Genetic Algorithm”,Springer Verlag Berlin Heidelberg, 2008.

[2] M. Mitchell, “An Introduction to Genetic Algorithms,” The MIT Press, Cambridge,USA, 1999.

[3] Jiri Fridrich, “Image Encryption Based on Chaotic Maps”, Proceeding of IEEE Conference On Systems, Man, and Cybernetics, pp. 1105-1110, 1997.

[4] Habutsu T et al. “A secret cryptosystem by iterating a chaotic map” Eurocrypt 1991:127-40.

[5] Frank Dachselt and Wolfgang Schwarz, “Chaos and Cryptography”, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 48, No. 12, pp. 1498– 1509, 2001.

[6] K.W. Wong, “A fast chaotic cryptographic scheme with dynamic look-up table”, Physics Letters A, Vol. 298, No. 4, pp. 238–242, 2002.

[7] Wai-kit Wong, Lap-piu Lee and Kwok-wo Wong, “A modified chaotic cryptographic method”, Computer Physics Communications, Vol. 138, No. pp. 234-236, 2001.

[8] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps”, International Journal of Bifurcation Chaos, Vol. 8, No. 6, pp. 1259-1284, 1998.

[9] S. Lian, J. Sun and Z. Wang, “A block cipher based on a suitable use of chaotic standard Map”, Chaos, Solitons and Fractals, Vol. 26, No. 1, pp. 117–129, 2005.

[10] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law, “A Fast Image Encryption Scheme based on Chaotic Standard Map”, Physics Letters A, Vol. 372, No. 15, pp. 2645– 2652, 2008.

[11] M. Francois, T. Grosges, D. Barchiesi and R. Erra, “A new image encryption scheme based on a chaotic function”, Image Communication, Vol. 27, No. 3, pp. 249–259, 2012.

[12] A. Ahmed, Abd El-Latif, Li Li, Tiejun Zhang, Ning Wang, Xianhua Song and Xiamu Niu, “Digital image encryption scheme based on multiple Chaotic systems”, Sensing and Imaging, Vol. 13, No. 2, pp. 67–88, 2012.

[13] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao and Tao Xiang, “A block cipher with dynamic S-boxes based on tent map”, Communications in Nonlinear Science and Numeric Simulation, Vol. 14, No. 7, pp. 3089–3099, 2009.

[14] Yang Tang, Zidong Wang and Jian-an Fang, “Image encryption using chaotic coupled map lattices with time-varying delays”, Communications in Nonlinear Science and Numeric Simulation, Vol. 15, No. 9, pp. 2456–2468, 2010.

[15] T.S. Parker and L.O. Chua, “Chaos: a tutorial for engineers”, Proceedings of the IEEE, Vol.75, No. 8, pp. 982–1008, 1987.

[16] Benyamin Norouzi, Sattar Mirzakuchaki, Seyed Mohammad Seyedzadeh and Mohammad Reza Mosavi, “A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process”, Multimedia Tools and Applications,Vol. 71, No. 3, pp. 1469-1497, 2014.

[17] R. Ranjith Kumar, B.Saranraj and S.Pradeep, “A new one round image encryption algorithm based on multiple chaotic systems”, ICTACT Journal on Image and Video Processing, Vol.5, No. 4, pp. 1017-1023, 2015

[18] R. Ranjith Kumar and M. Bala Kumar, “A New Chaotic Image Encryption Using Parametric Switching Based Permutation and Diffusion”, ICTACT Journal on Image and Video Processing, Vol. 4, No. 4, pp. 795-804, 2014.

[19] J. J. Buchholz, “Matlab implementation of the Advanced Encryption Standard”, http://buchholz.hs-bremen.de/aes/aes.htm, 2001.

[20] R. Forre, “The strict avalanche criterion: spectral properties of boolean functions and an extended definition”, Proceedings on Advances in Cryptology, pp. 450–468, 1990.

[21] Hongjun Liu and Xingyuan Wang, “Color image encryption based on onetime keys and robust chaotic Maps”, Computers & Mathematics with Applications, Vol. 59, No. 10, pp. 3320–3327, 2010.

[22] Nooshin Bigdeli, Yousef Farid and Karim Afshar, “A robust hybrid method for image encryption based on Hopfield neural network”, Computers and Electrical Engineering, Vol. 38, No. 2, pp. 356–369, 2012. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

Cite this article as: R Ranjith kumar, S Jayasudha, S Pradeep. “A Novel Image Encryption Scheme on the Basis of Genetic Algorithm and Chaos”. *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 41-48. Print.