International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.205-216
http://dx.doi.org/10.14257/ijsia.2016.10.2.19

A Novel Lossless Image Encryption Method using DNA Substitution and Chaotic Logistic Map

Shouvik Chakraborty[*1], Arindrajit Seal[2], Mousomi Roy[3], Kalyani Mali[4]

[1,2,3]*P.G. Student, Department of Computer Science & Engineering, University of Kalyani, West Bengal, India*
[4]*Professor and Head, Department of CSE, University of Kalyani, Nadia, WB, India*
[1]*shouvikchakraborty51@gmail.com*, [2]*arindrajit.seal@gmail.com*, [3]*iammouroy@gmail.com*, [4]*kalyanimali1992@gmail.com*,

Abstract

Presently, there is a growth in the transmission of image and video data. Security becomes a main issue. Very strong image cryptographic techniques are a solution to this problem. There is a use of a randomly generated public key and based on that there is an application of DNA algorithm. In the proposed method DNA algorithm based substitution is used for spatial domain bit permutation. Here the chaotic logistic map is used for generating a pseudorandom bit sequence. We have generated 48bit length sequences for every pixel. After the substitution operation, a final layer of security is imposed to make this process more fault tolerant. The For checking the strength of the work a series of tests are performed and various parameters are checked like Correlation Coefficient Analysis, analysis of NPCR and UACI values etc.

Keywords*: Image cryptography, DNA Substituion, Lossless encryption, Logistic map.*

1. Introduction

Information security plays an important part in every field, especially fields related to confidential business and/or military affairs. Keeping data safe from unwanted access is Data Security. Encryption works by jumbling up the information data into unreadable form and then uses a key to right it for reading. Traditional image encoding algorithms are generally not suited for image encoding due to their slow speed in real-time processing and also handling various data formatting. Many chaos-based digital image encoding algorithms have been suggested. The concept of chaos is mostly used for image encoding because of its excellent cryptography characteristics. Various algorithms provide different degrees of security and it is based on how hard they are to break. If the cost required to decode an algorithm is more than the value of the encoded data then the algorithm probably is thought to be safe. Modern high quality image encoding methods have several errors and are exposed to heavy attacks by expert cryptanalyst. Thorough study and analysis between these techniques are needed to ensure the performance and to choose the better one for the intended application. For certain applications speed of encryption may be the main concern and for some other cases the security will be important. There are three types of encoding schemes namely substitution, transposition and permutation and techniques which include both transposition and substitution. Substitution schemes change the pixels while permutation just shuffles the pixels based on the algorithm. In some cases both the methods are combined to improve security. Chaos theory has proven to be a very good alternative to provide a fast and quite reliable image encoding scheme. The method in [1] is chaos based using bit level permutation. Permutation at the bit level

Shouvik Chakraborty is the corresponding author.

ISSN: 1738-9976 IJSIA

changes the value. In [2] a novel image encryption method based on total shuffling scheme is illustrated. In [3] combinations of two logistic maps are used for improving the security of encryption. Encryption in [4] uses multiple chaotic systems. But each of these methods has some security issues. The algorithm in [5] combines the diffusion and confusion operations and uses the spatial-temporal chaotic system for generating the key. But this is time consuming. As the key space increases the security of the algorithm also get improved. From [6] it is clear that this algorithm performs better as compared to the techniques in [5]. Although some of the chaos based image encoding techniques are resistant to these types of attacks to some extent; more secured solutions are needed for further improvement. Replay attack is one of the main security attacks. It can be stated as a network attack in which a legitimate data transfer is intentionally repeated or delayed. It can be done by the source or by any other advisory. The common remedies for these attacks are session tokens, one-time -password(OTP), addendum of MAC and timestamps. The reference [7] describes the replay attack. [8] and [9] proposes remedial methods. In [10], Denning stated a method for preventing replay attack by timestamps. These methods prevent replay attacks in normal data transfer. The proposed system is all about to prevent the replay attack on digital image transmission with the help of timestamps. In [11] only permutation is used for encoding the grey scale image. Although the proposed work betters the security of that algorithm by introducing a bit substitution technique in [12] for encrypting color images. The remaining of this paper is organized as follows. Section 2 describes the chaotic logistic map, section 3 describes DNA substitution method, section 4 describes the proposed method, section 5 gives the experimental results and analysis and section 6 gives the conclusion.

2. Chaotic Logistic Map

Chaos is an ubiquitous phenomenon existing in deterministic nonlinear systems which exhibit high sensitivity to initial conditions and have random behavior. It was discovered by Edward N.Lorenz in 1963.

To create a chaotic stream cipher, a random bit stream is to be generated using chaotic system. Pseudo Noise (PN) Sequences : A pseudo random bit generator [13] (PRBG) is a deterministic algorithm, which uses a truly random binary sequence of length k as input called seed and produces a binary sequence of length l>>k, which is called pseudorandom sequence. This pseudorandom sequence appears to be random. The output of a PRBG is not truly random; in fact the number of possible output sequences is at most a small fraction (/) of all possible binary sequences of length l. The basic idea is to take a small truly random sequence of length k and expand it to a sequence of much larger length l in such a way that an adversary cannot efficiently distinguish between output sequence of PRBG and truly random sequence of length.

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations. Mathematically, the logistic map is written as given in Equation 1.

$$x_{n+1} = \lambda x_n(1 - x_n) \quad (1)$$

where λ € (0,4) , n = 0,1…..

Response of logistic map for $\lambda = 2.8$ is given in Figure 1 and for $\lambda = 3.2$ is given in Figure 2.

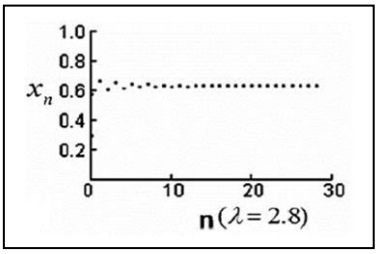

Figure 1. Response of Logistic Map for λ=2.8

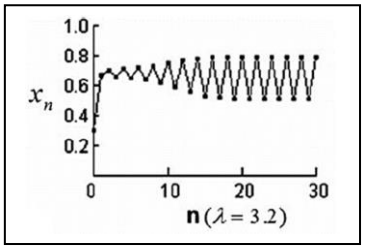

Figure 2. Response of Logistic Map for λ=3.2

A bifurcation diagram shows the values visited or approached asymptotically (fixed points, periodic orbits, or chaotic attractors) of a system as a function of a bifurcation parameter in the system. The bifurcation parameter λ is shown on the horizontal axis of the plot and the vertical axis shows the set of values of the logistic function visited asymptotically from almost all initial conditions. The bifurcation diagram shows the forking of the periods of stable orbits from 1 to 2 to 4 to 8 *etc*. Each of these bifurcation points is a period-doubling bifurcation. The ratio of the lengths of successive intervals between values of λ for which bifurcation occurs converges to the first Feigenbaum constant. The diagram also shows period doublings from 3 to 6 to 12 *etc*., from 5 to 10 to 20 *etc*., and so forth. Biufurcation diagram of logistic map is given in Figure 3.

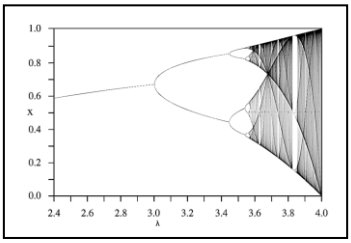

Figure 3. Bifurcation Diagram of Logistic Map

The pseudo random bit sequence is generated by comparing the outputs of two chaotic logistic maps. The chaotic logistic map produces the binary sequences by comparing the outputs of the piecewise linear chaotic maps in the way as given in Equation 2.

$$(2) \quad g(x_{n+1}, y_{n+1}) = 0 \text{ if } x_{n+1} < y_{n+1} \\ = 1 \text{ otherwise}$$

4. DNA Substitution Method

There are two rules in chaotic DNA substitution:-

- Binary Coding Rule
- Complementary Rule

The binary coding rule transforms letters transforms binary codes into A, T, G, C and vice-versa. In this method the following encoding is adopted A=00, C=01,

G=10, T=11. That means A is coded as "00", C as "01" *etc*. Each pixel value is then transformed into binary sequence using DNA substitution.

In complementary rule , each letter x is assigned to a complement denoted C(x). Here the C(x) represents the complement of x. This is how the complement operation takes place:-

(AT)(TC)(CG)(GA), the complement rule states that C(A)=T, C(T)=C,C(T)=G,C(G)=A. There are six allowable complementary transformation.

(AT)(TC)(CG)(GA)

(AT)(TG)(GC)(CA)

(AC)(CT)(TG)(GA)

(AC)(CG)(GT)(TA)

(AG)(GT)(TC)(CA)

(AG)(GC)(CT)(TA)

Initially we take a 12 bit key generated using chaotic logistic map sequence. We divide the 12 bits into 6 groups of 2 bits each. We perform XOR operation of Grp1 & Grp 2. We get a value of 2 bits. We perform XOR with this intermediate value with Grp3. Likewise, we progress by performing XOR operation with the intermediate values and the groups up to group 6. The final 2 bits value after performing XOR operation is then subjected to a mod 3 operation to get the iteration number.

4. Proposed Algorithms

4.1. Encryption Algorithm

The process start off by choosing an image and convert a pixel value into 8 bit binary format. Then this binary sequence is reversed. Now we make 4 pairs from these 8 bits, reverse each pairs. Now take four initial parameters for the logistic map as key. For each pair of bits generate a chaotic pseudorandom sequence of 12 bits length. Now divide the key (*i.e*. 12 bit sequence) into 3 groups each of length 4bit initially. Then generate a binary sequence of length 4 by performing XOR operation on 3 groups of key sequence. This operation is depicted in Figure 4. Now reverse these 4 bits and find the decimal value of it and calculate the mod 6 value to select a transformation sequence. Now divide the same 12 bit sequence key into 6 groups each of length 2. Then generate a binary sequence of length 2 by performing XOR operation on 6 groups key sequence. Now reverse these 2bits and find the decimal value of it and calculate the mod 3 value to select a iteration number. Choose the complementary value from the sequence and find the encoding value in decimal. In this way we get 4 values and convert these values in binary and reverse all these pairs. Now combine these pairs to get a 8 bit binary sequence.

Now for 4 pairs we get 48 bit key sequence. We divide it into 6 groups each of length 8. Then generate a binary sequence of length 8 by performing XOR operation on 6 groups key sequence. Now perform XOR operation with these 8 bits and 8 bits sequence generated in the previous step. This step provides an extra layer of security. Reverse the generated sequence and find the decimal value and assign it as an encoded image pixel.

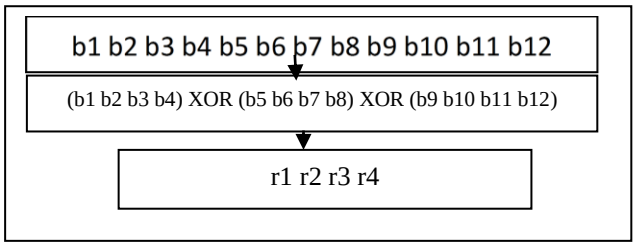

Figure 4. 4 Bit Key Generation from 12 Bit Sequence

The encryption algorithm is given below.

Step 1: Input an image.
Step 2: Choose a pixel and convert it into 8bit binary and reverse it.
Step 3: Make 4 pairs of pixels, reverse each pair and convert it into decimal.
Step 4: Now for every pair, find 12bits sequence using chaotic logistic map.
Step 5: Now divide the key into 3groups each of length 4.
Step 6: Then generate a binary sequence of length 4 by performing XOR operation on 3 groups key sequence.
Step 7: Now reverse these 4bits and find the decimal value of it and calculate the mod 6 value to select a Transformation sequence.
Step 8: Now divide the key into 6 groups each of length 2.
Step 9: Then generate a binary sequence of length 2 by performing XOR operation on 6 groups key sequence.
Step 10: Now reverse these 2 bits and find the decimal value of it and calculate the mod 3 value to select a Iteration number.
Step 11: Choose the complementary value from the sequence and find the encoding value in decimal
Step 12: In this way we get 4 values and convert these values in binary and reverse all these pairs
Step 13: combine these pairs to get a 8 bit binary sequence
Step 14: Now for 4pairs we get 48 bit key sequence. We divide it into 6groups each of length 8.
Step 15: Then generate a binary sequence of length 8 by performing XOR operation on 6 groups key sequence
Step 16: Now perform XOR operation with newly generated key and 8 bits sequence
Step 17: Reverse the generated sequence and find the decimal value and assign it as an encoded image pixel

4.2. Decryption Algorithm

The decryption process follows exactly the reverse method of the encryption process. At first, generate a 48 bit sequence for each pixel and divide it into 6 groups of 8 bits each. Generate 8 bits by performing XOR operation among these 6 goups. Now convert the encoded pixel value into 8 bit binary format and reverse it. Now perform XOR operation between pixel and previous 8 bits. Make 4 pairs of pixels, reverse each pair and convert it into decimal. Now for every pair, generate 12 bits sequence using chaotic logistic map. Now divide the key into 3 groups each of length 4. Then generate a binary sequence of length 4 by performing XOR operation on 3 groups key sequence. Now reverse these 4 bits and find the decimal value of it and calculate the mod 6 value to select a transformation sequence. Now divide the key into 6 groups each of length 2. Then generate a binary sequence of length 2 by performing XOR operation on 6 groups key

sequence. Now reverse these 2 bits and find the decimal value of it and calculate the mod 3 value and subtract it from 4 to select iteration number. Choose the complementary value from the sequence and find the encoding value in decimal. In this way we get 4 values and convert these values in binary and reverse all these pairs. Combine these pairs to get a 8 bit binary sequence, reverse it and convert it into decimal and assign this value as decrypted image pixel value.

The decryption algorithm is given below.

Step 1: Input the encrypted image.
Step 2: Generate a 48 bit sequence for each pixel and divide it into 6 groups of 8 bits each.
Step 3: Generate 8 bits by performing XOR operation among these 6 groups.
Step 4: Convert the encoded pixel value into 8 bit binary format and reverse it.
Step 5: Perform XOR operation between pixel and previous 8 bits.
Step 6: Make 4 pairs of pixels, reverse each pair and convert it into decimal.
Step 7: Now for every pair, generate 12 bits sequence using chaotic logistic map.
Step 8: Divide the key into 3 groups each of length 4.
Step 9: Generate a binary sequence of length 4 by performing XOR operation on 3 groups key sequence.
Step 10: Reverse these 4 bits and find the decimal value of it and calculate the mod 6 value to select a transformation sequence.
Step 11: Divide the key into 6 groups each of length 2
Step 12: Generate a binary sequence of length 2 by performing XOR operation on 6 groups key sequence
Step 13: Reverse these 2 bits and find the decimal value of it and calculate the mod 3 value and subtract it from 4 to select a iteration number
Step 14: Choose the complementary value from the sequence and find the encoding value in decimal
Step 15: In this way we get 4 values and convert these values in binary and reverse all these pairs
Step 16: Combine these pairs to get a 8 bit binary sequence,
Step 17: Reverse the generated sequence and find the decimal value and assign it as an decoded image pixel

5. Experimental Results and Analysis

The main goal of the image cryptographic algorithms is to produce a image that is difficult to understand. The quality of the image may degrade. The algorithm proposed in this paper degrades the image quality during the encryption technique but at the end of the decryption, the original image is restored. Automated quality measurement methods that are based on mathematical and computational algorithms are necessary because of the variability and inconsistency between human observers. The quality of the image is assessed by some parameters. In the following sections, details of the different parameters along with the results are given.

5.1. Correlation Co-Efficient

Correlation coefficients have been tested in three different direction *i.e*. horizontal, vertical and diagonal. Correlation coefficients are calculated for the selected pairs using Equation 3 [14].

$$R_{xy} = COV(xy)/\sqrt{D(x)}\sqrt{D(y)} \quad (3)$$

Where,

$$COV(xy) = \frac{1}{T}\sum_{i=1}^{T}((x_i - E(x))(y_i - E(y))) \quad (4)$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i \, , E(y) = \frac{1}{T}\sum_{j=1}^{T} y_j \quad (5)$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x_i)\right)^2 \, , D(y) = \frac{1}{T}\sum_{i=1}^{T}\left(y_i - E(y_i)\right)^2 \quad (6)$$

where x, and y in the above equations are the gray-scale values of the two adjacent pixels in the image, and T is the total pair of pixels randomly selected from the image. Table 1 provides the comparison of proposed approach and some other benchmark approaches. Table 2 shows the results obtained from proposed approach on some standard images.

Table 1.Comparison of Correlation Coefficients in Original and Encrypted Images

Encryption Method	Test Image	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
Proposed	Lena	0.946	-0.0055	0.973	-0.0075	0.921	0.0026
	Lake	0.958	-0.0025	0.958	0.00977	0.929	0.0127
Tedmori and Najdawi [15]	Lena	0.919	0.0023	0.927	0.0042	0.962	0.0053
	Lake	0.987	0.0025	0.936	0.0015	0.927	0.0105
Ye [16]	Lena	0.904	0.0020	0.903	0.0042	0.953	0.0088
	Lake	0.976	-0.0730	0.904	-0.0038	0.912	0.0191
Sethi and Sharma [17]	Lena	0.913	0.0031	0.920	0.0049	0.925	0.0062
	Lake	0.942	-0.0016	0.922	0.0036	0.887	0.0144
Huang and Nien [18]	Lena	0.916	0.0058	0.929	0.0092	0.946	0.0058
	Lake	0.982	0.0074	0.898	0.0084	0.924	0.0146

Table 2.Correlation Coefficients in Original and Encrypted Images based on the Proposed Encryption Algorithm Results

Test Image	Horizontal			Vertical			Diagonal		
	Org	Enc	Dec	Org	Enc	Dec	Org	Enc	Dec
Lena	0.946	-0.006	0.946	0.973	-0.008	0.973	0.921	0.003	0.921
Lake	0.958	-0.002	0.958	0.958	0.009	0.958	0.929	0.013	0.929
Peeper	0.967	0.005	0.967	0.973	-0.005	0.973	0.943	0.012	0.943
House	0.985	0.00007	0.985	0.981	-0.004	0.981	0.968	0.021	0.968
Cameraman	0.956	0.010	0.956	0.974	-0.008	0.974	0.934	0.0004	0.934
Mandril	0.874	0.004	0.874	0.836	0.00004	0.836	0.795	0.001	0.795

5.2. PSNR

PSNR is an abbreviation for Peak Signal to Noise Ratio. PSNR is a well-known parameter and can be computed from Equation 7 [10]. The PSNR results in an undefined value under one condition only; *i.e.*, when the original image is compared to itself. In this

case the MSE value in the denominator part of the Equation 7 would result in a zero value, and hence, a division by zero situation occurs).

$$PSNR = 10 \log_{10}\left(\frac{L^2}{MSE}\right) \quad (7)$$

Where

$$MSE = \frac{1}{N}\sum_{i=0,j=0}^{N,N}\left(x_{ij} - y_{ij}\right)^2 \quad (8)$$

N is the number of pixels in the frame, and xij, yij are the ith and jth pixels inthe original and processed frames, respectively. L is the dynamic range of pixel values (L is 0 to 255 for gray-scale images).

Table 3 provides the comparison of proposed approach and some other benchmark approaches. Table 4 shows the results obtained from proposed approach on some standard images.

Table 3. Comparison of PSNR values

Test Image	Proposed		Tedmori and Najdawi [15]		Samsom and Sastry [14]		Sethi and Sharma [17]		Huang and Nien [18]	
	O-D	O-E	O-D	O-E	O-D	O-E	O-D	O-E	O-D	O-E
Lena	Undefined	0.0049	Undefined	0.0017	40.22	0.113	69.70	0.036	45.78	0.154
Lake	Undefined	0.0043	Undefined	0.0043	33.49	0.098	43.65	0.072	51.83	0.127

Table 4. PSNR Values of Some Standard Images Obtained using Proposed Approach

Test Image	PSNR	
	O-D	O-E
Lena	Undefined	0.0049
Lake	Undefined	0.0043
Peeper	Undefined	0.0053
House	Undefined	0.0048
Cameraman	Undefined	0.0058
Mandril	Undefined	0.0063

5.3. Differential Attacks: NPCR and UACI

To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity(UACI). NPCR and UACI can be defined using Equation 9 and Equation 10 respectively [16].

$$NPCR = \frac{\sum_{i=j=1}^{m,n} D(i,j)}{w \times h} \times 100\% \quad (9)$$

$$UACI = \frac{1}{w \times h}\left[\sum_{i,j}^{m,n} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (10)$$

Where C1 and C2 are two encrypted images corresponding to two original images with subtle change *i.e.*, one pixel difference. w,h are the image width and height , D(i, j) is a bipolar array with the same size as image C1 ,D(i, j) is determined using on Equation 11 [19].

$$D(i,j) = \begin{cases} 1 \; if \; C_1(i,j) = C_2(i,j) \\ 0 \; Otherwise \end{cases} \quad (11)$$

Table 5 provides the comparison of proposed approach and some other benchmark approaches. Table 6 shows the results obtained from proposed approach.

Table 5. Comparison of NPCR and UACI Values

Test Image	Proposed		Tedmori and Najdawi [15]		Ye [16]		Sethi and Sharma [17]		Huang and Nien [18]	
	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%
Lena	99.932	39.520	99.941	38.981	99.105	36.241	95.124	20.113	99.214	27.481
Lake	99.85	40.303	99.953	40.874	98.642	37.121	34.124	98.642	98.349	27.628

Table 6. NPCR and UACI Values of Some Standard Images Obtained using Proposed Approach

Test Image	Proposed Approach	
	NPCR	UACI
Lena	99.932%	39.520%
Lake	99.85%	40.303%
Peeper	99.625%	37.221%
House	99.736%	45.652%
Cameraman	99.569%	39.641%
Mandril	99.317%	38.341%

5.4. Histogram

The histogram of the encrypted images is significantly different from the histogram of the original images (left-shifted) and hence it does not provide any useful information to perform any statistical analysis attack on the encrypted image.
Figure 5 shows an example of plotting the histogram of the original, encrypted, anddecrypted along with the correlation coefficients.

Figure 6 to Figure 7 shows some of the results of the proposed encoding/decoding algorithms are given. These results are obtained by applying proposed method on some standard test images.

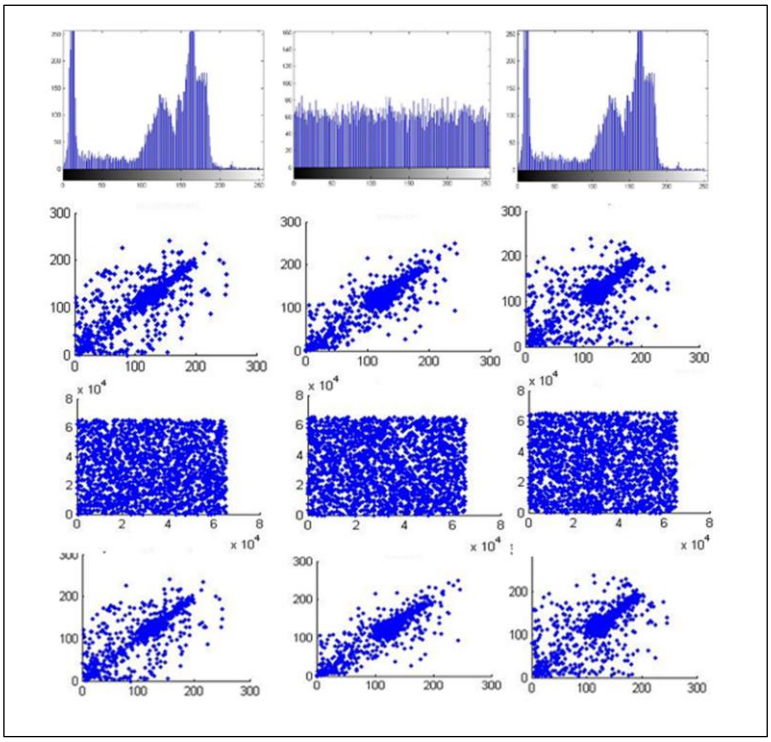

Figure 5. In the First Row Histogram Representation of the Cameraman standard Image (from left to right: Original, Encrypted and Decrypted), From Second Row-, Top to Bottom : Correlation Coefficients of Original, Encrypted and Decrypted, Left to Right: Correlation Coefficients in Horizontal, Vertical and Diagonal Directions

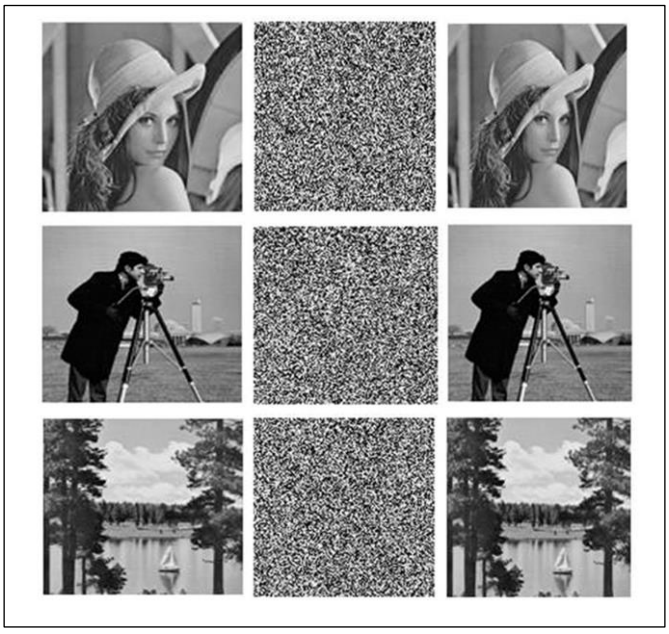

Figure 1. From Top to Bottom, Standard Images "Lena", "Cameraman" and "Lake" , from Right to Left, the Figure Present the Original, Encrypted and Decrypted Algorithms Results

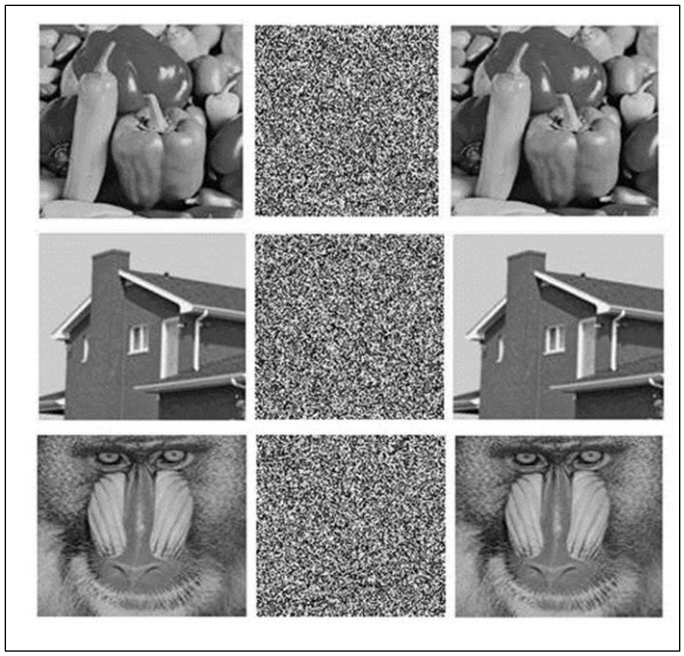

Figure 2. From Top to Bottom, Standard Images "Peeper", "House" and "Mandril" , from Right to Left,the Figure Present the Original, Encrypted and Decrypted Algorithms Results.

6. Conclusion

The proposed work is highly resilient and robust among most other cryptographic algorithms. In this approach the key is generated using a chaotic logistic map then we have applied the DNA Substitution algorithm. We perform various mathematical evaluations using various benchmark parameters namely correlation coefficients, PSNR, UACI *etc*. and our proposed approach has proven to be quite strong against cryptographic attacks. The method is lossless, so we get exactly the original image after the decryption process. This makes our approach resilient, robust and cogent enough in comparison to the other approaches available. Results are compared against standard algorithms which shows the effectiveness of the proposed work.

References

[1] Z-l Zhu, W. Zhang, K-w Wong and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Elsevier Information Sciences, vol. 181, **(2010)**, pp. 1171–1186.
[2] G. Zhang and Q. Liu, "A novel image encryptionmethod based on total shuffling scheme", Optics Communications, vol. 284, no. 12, **(2011)**, pp. 2775–2780.
[3] Y. Mao and G. Chen, "Chaos-Based Image Encryption", in Hand- book of geometric computing, Springer, **(2005)**.
[4] H. Alsafasfeh, and, A.A.Arfoa, "Image encryption based on the general approach for multiple chaotic system", Journal of Signal and Information Processing vol. 2, **(2011)**, pp. 238- 244.
[5] Y. Wanga, K-W Wong, XiaofengLiaoc and Guanrong Chen, "A new chaos- based fast image encryption algorithm", in Applied Soft Computing, Elsevier, **(2011)**.
[6] L Abraham and N. Daniel, "Secure image encryption algorithms: A review", IJSTR, **(2013)**.
[7] L. Gong and P. Syverson, "Fail-stop protocols: An approach to designing secure protocols", In 5th
[8] International Working Conference on De- pendable Computing for Critical Applicaitons, September, **(1995)** pp. 44–55.
[9] S. Malladi, J. Alves-Foss and R. B. Heckendorn, "On Preventing Replay Attacks on Security Protocols".
[10] T. Aura "Strategies against replay attacks", In Proceedings of the 10th IEEE Computer Society Foundations Workshop, June **(1997)** pp 59 – 68, IEEE Computer Society Press.
[11] D. Denning and G. Sacco, "Timestamps in key distribution protocols". Communications of the ACM, **(1981)** vol. 24, no. 8, pp. 553–536.

[12] L. Abraham, N. Daniel, "Enhancing the Security of Image Encryption Algorithms by Adding Timestamp", IJARET, Vol. 1, Issue VIII, **(2013)**.
[13] A. Awad and A. Miri, "A New Image Encryption Algorithm Based on a Chaotic DNA Substitution Method", in , Communications (ICC) on IEEE, **(2012)**, pp. 1011-1015.
[14] N.K. Pareek, V Patidar and K. K. Sud, "A Random Bit Generator Using Chaotic Maps", vol. 10, no. 1, **(2010)**, pp.32-38.
[15] Z. Liu, J. Dai, X. Sun and S. Liu, "Triple image encryption scheme in fractional Fourier transform domains", Elsevier Optics Commun., vol. 282, no. 4, **(2009),** pp. 518-522.
[16] C. Samson and V. Sastry, "A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform", Int.l J. of Advanced Comput. Sci. App, Vol. 3, No. 9, **(2012),** pp. 178-183.
[17] S. Tedmori and N. Al-Najdawi, "Image Cryptographic Algorithm Based on the Haar Wavelet Transform", Elsevier Information Sciences, vol. 269, **(2014)**, pp. 21-34.
[18] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism", Elsevier Optics Commun., vol. 284, **(2011),** pp. 5290-5298.
[19] N. Sethi and D. Sharma, "Novel Method of Image Encryption Using Logistic Mapping", Int. J. Comput. Sci. Eng.,vol. 1, no. 2, **(2012),** pp. 115-119.
[20] C.K. Huang and and H. Nien, "Multi chaotic systems based pixel shuffle for image encryption", Elsevier OpticsCommun., vol. 282, no. 11, **(2009),** pp. 2123-2127.
[21] F. Sun, z. Lu and S. Liu, "A new cryptosystem based on spatial chaotic system", Elsevier Optics Commun., vol. 283, no. 10, **(2010),** pp. 2066–2073.

Authors

Shouvik Chakraborty, He is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. He received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. His research interests include soft and evolutionary computing, bioinformatics, digital image processing and cloud computing.

Arindrajit Seal, He is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. He received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. His research interests include digital image processing and bioinformatics.

Mousomi Roy, She is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. She received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. Her research interests include digital image processing and bioinformatics and cloud computing.

Dr. Kalyani Mali, She is currently working as Professor and Head in the Computer Science & Engineering Department at University of Kalyani, West Bengal, India. She obtained M.Tech. in Computer Science from Calcutta University and received Ph.D in Engineering from Jadavpur University. Her area of interest in research is Pattern Recognition, Image Processing, Data Mining and Soft Computing.

