Noise Assisted Image Encryption and Decryption using 2-D Chaotic System

Namrata Biswas

B S Abdur Rahman Crescent Institute of Science & Technology

I. Raja Mohamed (rajamohamed@crescent.education)

BS Abdul Rahman Institute of Science and Technology: B S Abdur Rahman Crescent Institute of Science & Technology https://orcid.org/0000-0003-0404-1291

Research Article

Keywords: chaos-based cryptosystem, Image Encryption/Decryption, Security Analysis.

Posted Date: December 17th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-807624/v1

Noise Assisted Image Encryption and Decryption using 2-D Chaotic System

Namrata Biswas

Department of ECE, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai-600048, India

namrata_ece_phd_18@crescent.eduction

I. Raja Mohamed

Department of Physics, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai-600048, India

rajamohamed@crescent.education

ABSTRACT: In this paper, a new two-dimensional (2-D) chaos-based colour image encryption and decryption scheme is proposed in which the noise signal is selected randomly to set the initial values for a chaotic system which also enhances the security of the system. The 256-bit hash value of noise is transformed into one-time initial values for the state variables of this proposed chaotic system. XOR operation is further carried out to diffuse the pixels. Finally, statistical and security analyses are performed for understanding the effectiveness of the proposed system. Experimental results confirm that the proposed chaos-based cryptosystem is efficient and suitable for information (image) transmission in a highly secured way.

Keywords: chaos-based cryptosystem, Image Encryption/Decryption, Security Analysis.

I. INTRODUCTION

In recent years, many researchers have shown interest in Chaos theory and its applications in wide spread areas, especially in the field of engineering and communication due to the unique features of chaotic sequence such as highly sensitive to the initial conditions, broad-band power spectrum, ergodicity in randomness. Even though there is consistency in the sustained development in the field of communication, increased security aspects have been the main concern for the users. To fulfil this requirement, chaos theory is capable of providing solutions with its inherent cryptographic properties. Cryptography is the technique of converting the plaintext in a non-readable form and vice-versa. Therefore, it is difficult for the attacker to decode the original information. The data can be of any form such as text, audio, video or image. Conventional encryption algorithm such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest, Shamir, Adleman) etc. cannot be used for the multimedia data transmission due to bulk data volume and high correlation among the pixels of an original plain image. Also, it is seen that it is more complicated and difficult to implement.

Many algorithms and schemes [1-3] have been proposed time to time for image encryption/decryption [4-5]. The discrete multi-dimension Chaotic System has increased application in image encryption [6-7] because of their complex structures and multiple parameters. According to Shannon's theory of secrecy systems [8-10], cryptography based on one-time key is theoretically unbreakable, but in practical implementation there exist some problems. For example, one time key requires the key stream generated using true random number generator (TRNG) never be reused, the key stream and the plain image must be of same length. Also, it is impractical to send the whole key stream generated by TRNG to the receiver. To solve this problem in this work, it is preferred to take several true random numbers from environmental noise as the pseudo-random generator (PRNG) to produce key stream dynamically which makes it is extremely difficult for the attacker to produce two identical noise signals in finite time.

Recently Chaos-based image encryption algorithm has been proposed with some chaotic maps, such as logistic map [6], tent map and Chebyshev map [10], Lorenz system [11]. But security aspects of the transmission are still need to be addressed.

In this paper, a new version of chaotic system is proposed and a chaos-based color image encryption and decryption technique is discussed which uses the one-time key from the environmental noise that enhances the security but also reduces the encryption rounds making the known-plaintext attack, ciphertext attack and differential attack ineffective. The hash value of the noise is applied to generate the initial conditions of the chaotic system. This chaotic system will generate sequence with good randomness to encrypt the Red (R), Green (G), Blue (B) components of the color image to fit for XOR operation.

Section II introduces the dynamical and numerical simulation of the new chaotic system. In Section III, the encryption and decryption algorithm are discussed. Section IV gives the MATLAB simulation results of the proposed cryptosystem. In Section V the security analysis of the system is analyzed. Finally, the results are discussed and concluded in the last section.

II. THE NEW CHAOTIC SYSTEM

A new chaotic system with additional parameters helps to set more random chaotic behaviors and larger key space which

increases the security in transmission line. The state equations of the new version of (Henon Map) are given below:

$$x_{n+1} = ax_n - x_n y_n$$

$$y_{n+1} = bx_n - cy_n \quad (1)$$

The parameter values are set as a=2.3, b=0.4 and c=0.8. Then Chaotic system is modelled using MATLAB Simulink in Fig. 1 to understand the dynamics of the system.

Theoretical calculation of the system is derived and results are given below:

The system has two equilibrium points E1 and E2:

E1$(+\frac{c^2}{b}, +\frac{ab}{c^2})$ and E2$(-\frac{c^2}{b}, -\frac{ab}{c^2})$)

To find the Eigen value of the given system:

$$\frac{d\vec{x}}{dt} = A\vec{x} \quad (2)$$

Where,

$$\vec{x} = \begin{bmatrix} x \\ y \end{bmatrix} \text{ and } A = \begin{bmatrix} a & -x \\ b & -c \end{bmatrix} \quad (3)$$

Try $\vec{x}(t) = e^{\lambda t}\vec{V}$

$$A\vec{V} = \lambda\vec{V} \quad (4)$$

$$\det(A-\lambda I) = \det\left(\begin{bmatrix} a-\lambda & -x \\ b & -c-\lambda \end{bmatrix}\right)$$

$$\det\left(\begin{bmatrix} 2.3-\lambda & -1 \\ 0.4 & -0.8-\lambda \end{bmatrix}\right) = \lambda^2 - 1.5\lambda - 1.44 \quad (5)$$

Two roots:

$$\lambda_1 = -0.665,\ \lambda_2 = 2.165 \quad (6)$$

Eigen Vector:

$$A - \lambda_1 I = \begin{bmatrix} 2.3 & -1 \\ 0.4 & -0.8 \end{bmatrix} - (-0.665)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (7)$$

$$\begin{bmatrix} 2.965 & -1 \\ 0.4 & -0.135 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad (8)$$

$$2.965x_1 - x_2 = 0$$

$$x_1 = 1, x_2 = 2.965 \quad (9)$$

$$V1 = \begin{bmatrix} 1 \\ 2.965 \end{bmatrix} \quad (10)$$

For $\lambda_2 = 2.165$ (11)

$$\begin{bmatrix} 0.135 & -1 \\ 0.4 & -2.965 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad (12)$$

$$2.965x_1 - x_2 = 0$$

$$x_1 = 2.965, x_2 = 0.4 \quad (13)$$

$$V2 = \begin{bmatrix} 2.965 \\ 0.4 \end{bmatrix} \quad (14)$$

$$X(t) = C_1\left(\frac{1}{2.965}\right)e^{-0.665} + C_2\left(\frac{2.965}{0.4}\right)e^{2.165} \quad (15)$$

$$x_1 = C_1 e^{-0.665} + 2.965C_2 e^{2.165} \quad (16)$$

$$x_2 = 2.965C_1 e^{-0.665} + 0.4C_2 e^{2.165} \quad (17)$$

The real parts of the eigen value are positive, which states that the presence of chaos and the equilibrium points are unstable. Thus, the system orbits around the two equilibrium points.

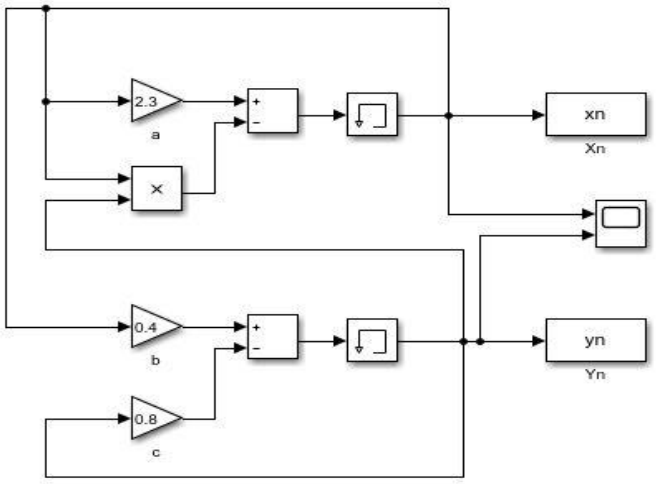

Figure 1. MATLAB Simulink model of a chaotic system with a=2.3, b=0.4 and c=0.8.

Bifurcation diagram for the new chaotic system is implemented by fixing the control parameter a and b and by only varying the value of c from 2 to 2.4 which can be seen in the Fig.2.

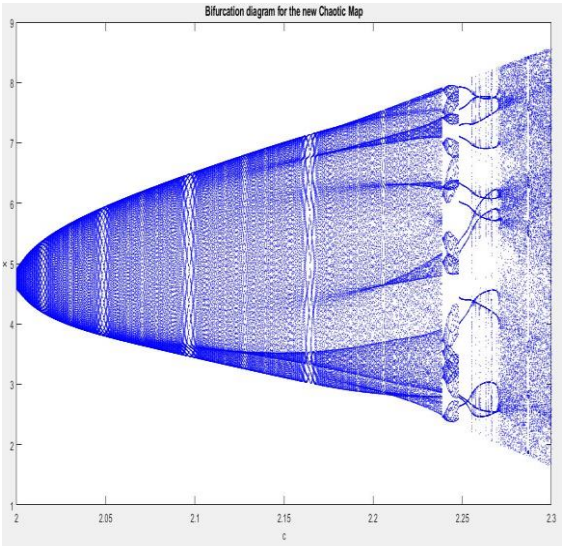

Figure 2. Bifurcation diagram of parameter c=0.8 for the system

Bifurcation diagram for the new chaotic system with the addition of noise is shown in Fig.3.

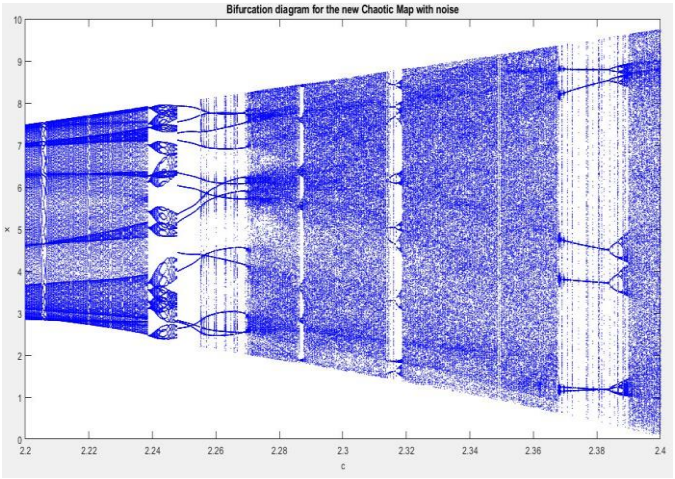

Figure 3. Bifurcation diagram of parameter c with addition of noise

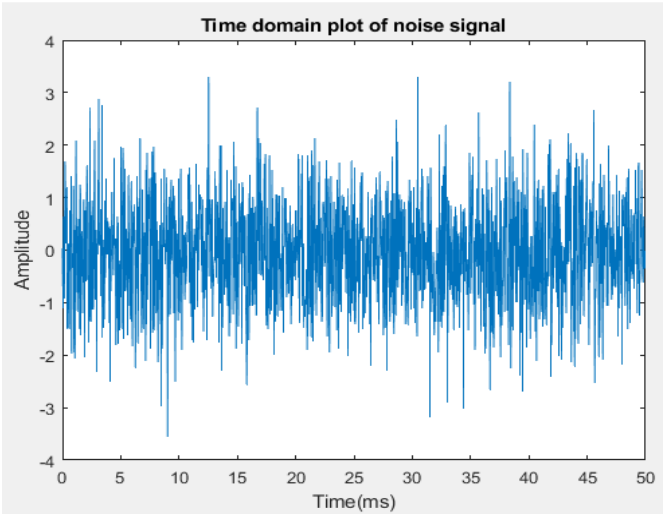

Figure 4. Time domain plot of noise signal

From the above graph we can say that at point 2.24 the bifurcation diagram is shifted with the addition of noise which will enhance the security and the maximum noise amplitude in time domain is given in Fig. 4.

Lyapunov exponent is a quantity that characterizes the points of divergence or convergence in phase space. When the control parameter a=2.3 and b=0.4 of the system are set, the largest Lyapunov exponent of c is [-0.5,0.5] is shown in Fig.5. One of the properties of chaos is sensitive to the initial values and control parameter, so in this cryptosystem, the control parameter c is varied dynamically in the interval c [-0.5,0.5] for randomness.

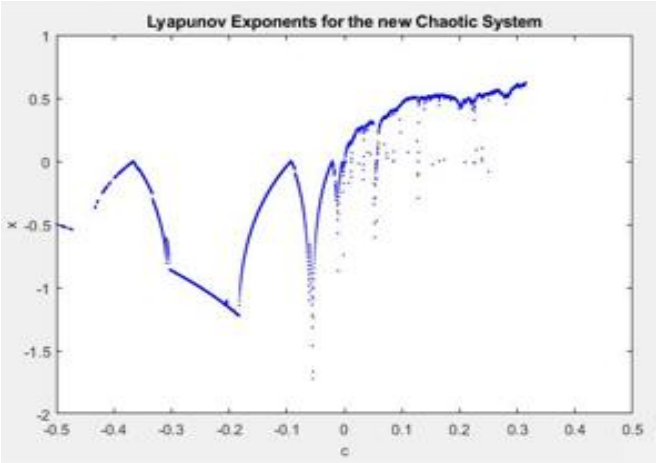

Figure 5. The Lyapunov exponent of the system

Using the MATLAB Simulink, the phase portrait of the model is achieved in Fig.6.

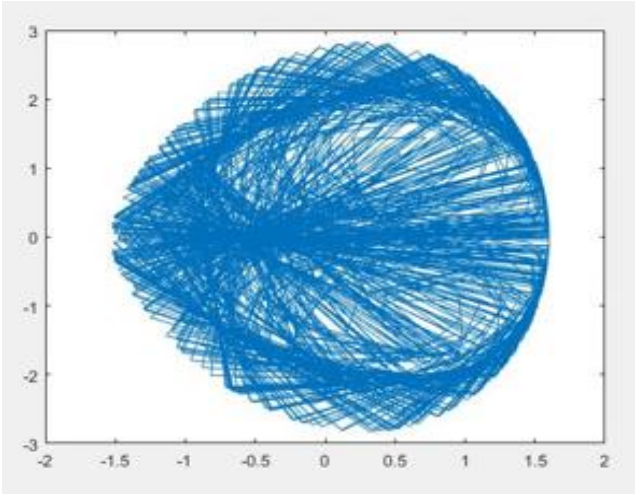

Figure 6. x-y phase portrait

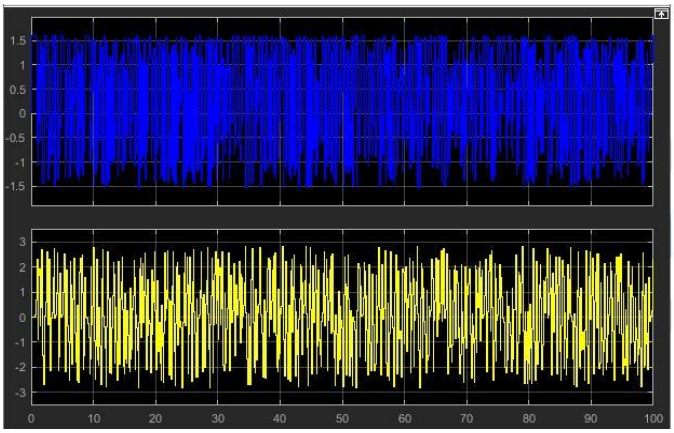

Figure 7. x and y time-series waveform

From the Fig.7 it is clear that the waveform is irregular and random which confirms the chaotic behavior in the model.

To enhance the randomness in the system three disturbance part is added in eq (1), where h is the step length.

$$x_{n+1} = x_n + hx_n(a - y_n) + hp_1 \quad (18)$$

$$y_{n+1} = y_n + h(bx_n - cy_n) + hp_2$$

Where

$$p_1 = \big((int)m_1 \ mod\ 256\big) * 10$$
$$p_2 = \big((int)m_2 \ mod\ 256\big) * 10 \quad (19)$$

In this cryptosystem, the pseudo random sequence is generated by (18) produced by the hash value of noise will encrypt the colour components, give initial values to the system and control parameter c.

III. IMAGE ENCRYPTION SCHEME

a. Generating the initial values and control

The proposed cryptosystem utilizes 256-bit external key H, which is the common hash value calculated by SHA- 256 of the noise which is randomly sampled for each encryption. The 256-bit hash value can be expressed as a hexadecimal number array H which is expressed as:

$$H = [h_1, h_2, \dots\dots\dots\dots\dots h_{64}] \quad (20)$$

The initial value for x, y, control parameter c, and pre- iteration n_0 can be obtained by:

x = N ([hex2dec (H (h_1: h_{21}))]mod L)

y= N ([hex2dec (H (h_{22}: h_{42}))] mod L) (21)

c = -0.5-((N ([|hex2dec (H (h_{43}: h_{56})) |]mod L)

n_0 = 500 + ((N ([|hex2dec (H (h_{57}: h_{64})) |]mod L) *10000) mod 1000)

Where N is the noise signal array.

b. Design of encryption algorithm

Input: Colour image P of size W_p X H_p with randomly sampled noise signal (N).

Output: Ciphered colour image C of the same size.

Step1: the hash value of N is obtained to calculate the initial value for x, y, control parameter c and n_0 by solving equation (21).

Step2: solve eq(19) using Runge-Katta method with a step length of h = 0.008911. Then pre-iterate n_0 times for L = W_p X H_p to get a sequence of X and Y with the same length of L as shown in eq (22)

$$X = \{x_1, x_2, \dots\dots\dots\dots\dots x_L\}$$

$$Y = \{y_1, y_2, \dots\dots\dots\dots\dots y_L\} \quad (22)$$

And then generate the three sequence of X_R, X_G and X_B by eq (23).

$$X_R = \alpha\, x_i$$

$$X_G = \alpha\, x_i \quad (23)$$

$$X_B = \alpha\, x_i$$

Where α is signal gain and i = 1, 2……. L.

Step3: Apply these sequences to encrypt red, green and blue component of P by eq (24) to get Ciphered image C obtained by C_R,C_G and C_B.

$$C_R = P_R \oplus (X_R \bmod 256)$$

$$C_G = P_G \oplus (X_G \bmod 256) \quad (24)$$

$$C_B = P_B \oplus (X_B \bmod 256)$$

Where ⊕ is the XOR operation.

The flowchart for the encryption algorithm is shown in Fig. 8.

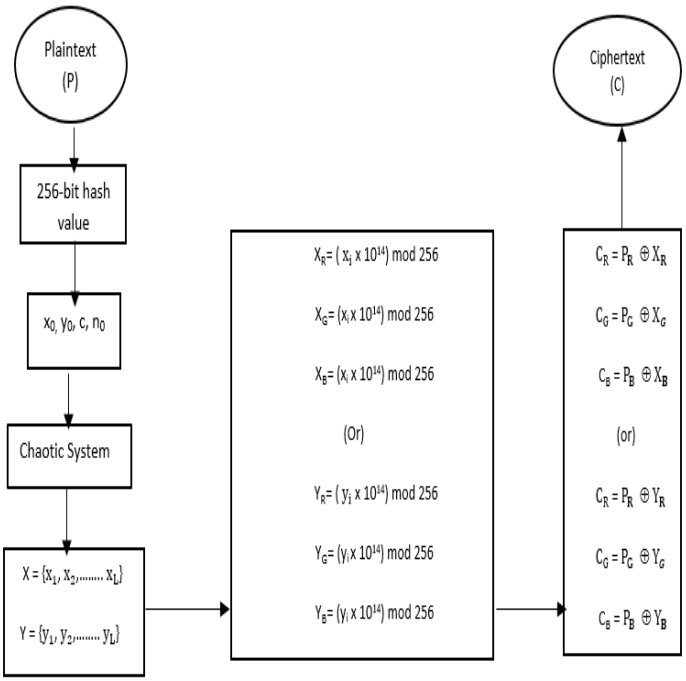

Figure 8. Flowchart of the encryption algorithm

c. Design of decryption algorithm

Input: Ciphered Colour image C, initial value x, y, control parameter c and the number n_0.

Output: Deciphered image P.

Step1: Same as Step 2 of the encryption algorithm above, to get three floating-point number sequences of XR, XG and XB.

Step 2: Apply XR, XG and XB to decrypt the red, green and blue components of image C by (25), to get PR, PG and PB, and then combine them into the deciphered image P

$$P_R = C_R \oplus (X_R \bmod 256)$$

$$P_G = C_G \oplus (X_G \bmod 256) \qquad (25)$$

$$P_B = C_B \oplus (X_B \bmod 256)$$

Where the symbol $\oplus$ denotes bitwise XOR operation.

The flowchart of the decryption algorithm is shown in Fig. 9.

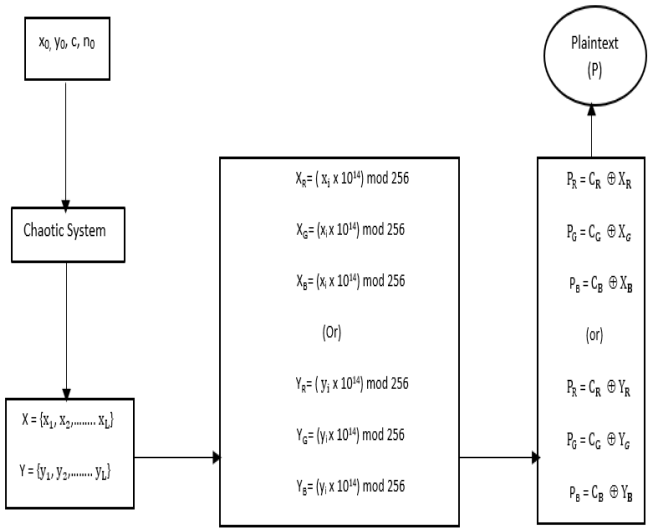

Figure 9. Flowchart of the decryption algorithm

IV. SIMULATION RESULTS

The colour plain image of Lena with size 512 X 512 is used for encryption using the discrete chaotic system. The initial condition and parameters used are x=12.0277, y=120.277, N=0.250577, n_0=1309.02 and c=2.1. The algorithm implemented in MATLAB. The Colour plain image is sown in Fig.10. The R, G, B component of the colour image is given in Fig. 10a, 10b and 10c and the encryption results of the R, G, B component of the plain colour image is shown in Fig. 11a, Fig. 11b and Fig. 11c below:

Figure 10. Colour Plain Image of Lena.

Figure 10a. R component of Plain image

Figure 10b. G component of plain image

Figure 10c. B component of plain image

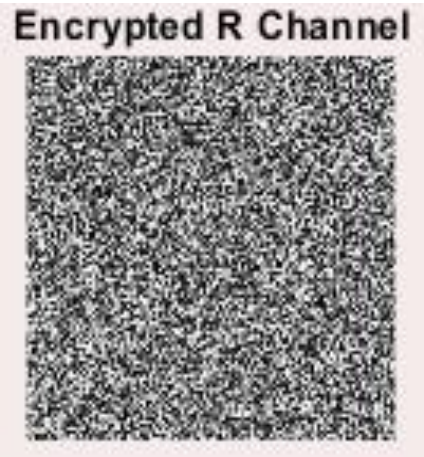

Figure 11a. Encrypted R component of plain image

Figure 11b. Encrypted G component of Plain image

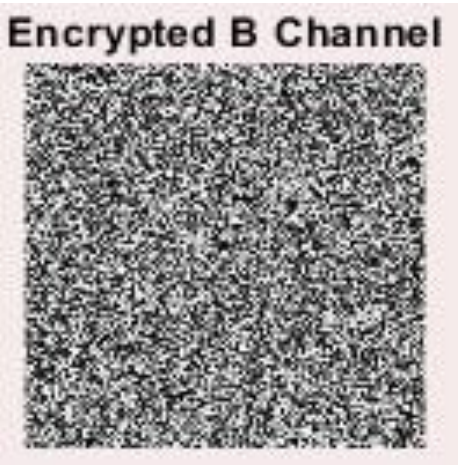

Figure 11c. Encrypted B component of Plain Image

Final cipher image of the plain image is shown in Fig. 12.

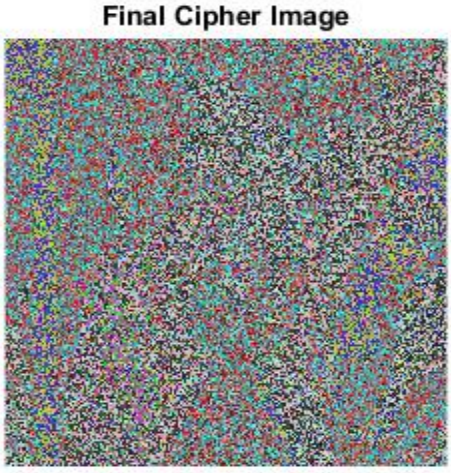

Figure 12. Final Cipher image of plain image

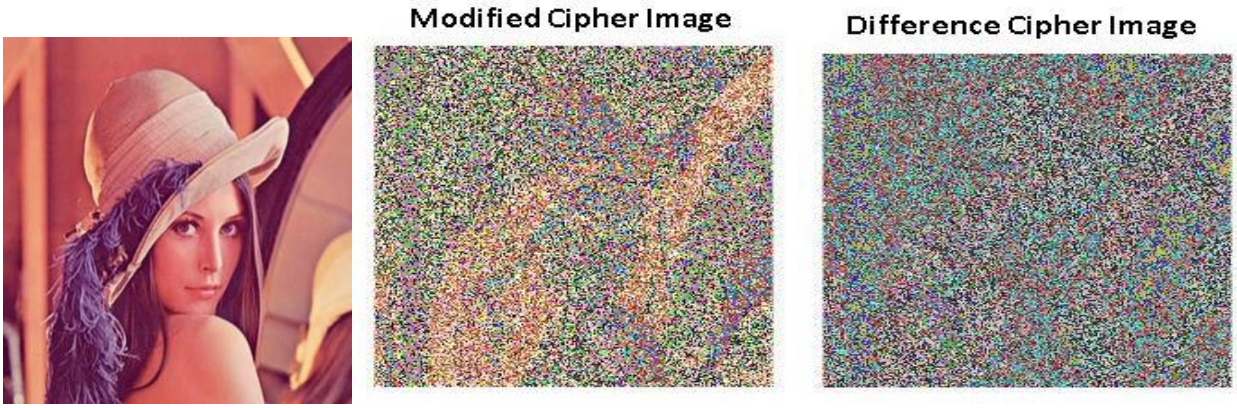

Figure 13a Lena with one-bit modified **Figure 13b** Encryption result of 11.a **Figure13c** Difference between Figs. 12 and 13b

V. SECURITY ANALYSIS

An efficient encryption process must be sensitive to the secret keys and should resist against all kinds of attacks, such as a plain-text attack, cipher-text attack, differential attack, brute force attack etc. The security analysis of the proposed encryption scheme is discussed based on Key Space analysis, Key Sensitivity analysis, Histogram analysis, Differential attack analysis, Correlation coefficient analysis, Information Entropy Analysis and Speed performance analysis.

a. Key Space Analysis

Key space size is the total number of different keys that can be used for encryption. The key must be large and very sensitive so that it can resist against Brute force attack. In this proposed cryptosystem the initial conditions and parameter for x, y, c and n_0 can be used as keys as well as the initial iteration. Generally, the initial condition is set to 10^{-14}[11] by which the key space size can reach up to 10^{56}. The n_0 key space can reach up to 10^3. Therefore, the total key space is 10^{56}x 10^3which is bigger than 2^{128} [12,13] which is large enough to resist against brute force attack.

b. Key Sensitivity Analysis

For an ideal encryption scheme the secret key must be very sensitive so that if there is any change in the bit, the secret key should produce a completely different encrypted image. Fig.10 above is the encrypted image of Lena with correct encryption key and original hash values.

H_original="a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3" with corresponding initial values as follows:

x_0= 83.51076,

y_0= 96.84381,

c =-0.003

n = 628.854.

H_modified="6b51d431df5d7f141cbececcf79edf3dd861c3b4069f0b11661a3eefacbba918" with corresponding initial values as follows:

x_0= 95.6168,

y_0= 103.087,

c =-0.4

n = 706.177.

The modified image of Lena is shown in Fig13.a. the corresponding encryption result is shown in Fig.13.b. the differences between the Figs.12 and 13.b. is shown in Fig.13.c. From the figures, we can say that their ciphered image are clearly different which states that small change in the key will generate a completely different decryption result and it will be difficult to obtain the correct plain image.

c. Histogram Analysis

An image histogram is the graphical depiction of the number of pixels distributed at each colour intensity level. It is one of the security analyses that explain about the statistical properties of a ciphered image. The Histogram of the original image and its encrypted form in Fig.14 and Fig.15 are given below:

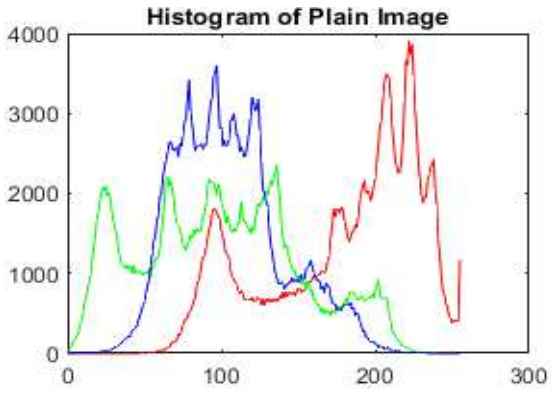

Figure 14. Histogram of the Original Image

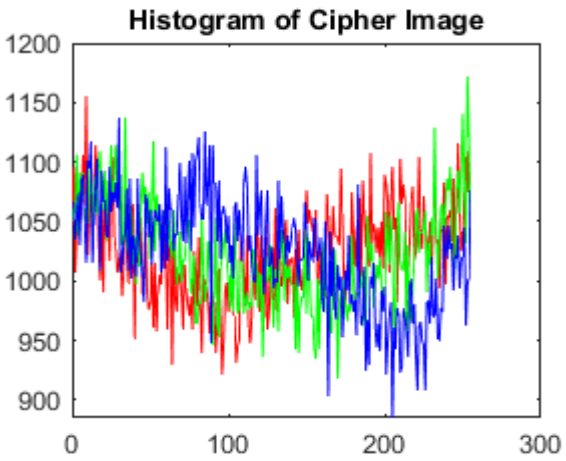

Figure 15. Histogram of the Cipher Image

The results shows that the pixel of the encrypted image is relatively uniform which makes the statistical attack difficult.

d. Differential Attack Analysis

The differential attack in which the attacker attempts to recover some information by comparing the cipher image with the corresponding plain image. To check the effect of change in one bit or one-pixel NPCR (net pixel change rate) and UACI (unified average changing intensity) measurements are used. They are defined as follows [14]:

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}}{WXH} X\ 100\%$$

$$UACI = \frac{1}{WXH}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{C_{i,j}-C'_{i,j}}{255} X100\% \quad (26)$$

$$D_{i,j} = \begin{cases} 0 & \text{if} C_{i,j} = C'_{i,j} \\ 1 & \text{if} C_{i,j} \neq C'_{i,j} \end{cases}$$

Where,

W and H are the width and height of the image.

$C_{i,j}$ and $C'_{i,j}$ are the cipher image before and after one pixel of the plain image is changed.

Table 1 lists their calculations of NPCR and UACI. The results are close to the theoretical value NPCR (99.609375%) and UACI (33.4635%) [15].

Table 1. Calculation of NPCR and UACI.

	NPCR%			UACI%		
Images	R	G	B	R	G	B
Original encrypted image of Lena (Fig.10)	**99.685**	**99.6961**	**99.7062**	**33.4799**	**33.5123**	**33.4787**
Modified encrypted image of Lena (11b.)	**99.6773**	**99.6722**	**99.6866**	**33.4642**	**33.5312**	**33.4845**
Lena in [12]	99.6755	99.6622	99.6619	33.4216	33.4211	33.4368
Lena in [16]	99.6100	99.6092	99.6099	33.4639	33.5042	33.4776

From the above Table 1. we can see that the results are satisfactory and better than the existing techniques in ref [12,16], so this scheme based on one-time key is secure against differential attack.

e. Correlation Coefficient Analysis

In the image, the pixels are highly correlated among each other. In order to inspect this, we compare the correlation of the adjacent

pixels in a horizontal, vertical and diagonal direction for the plain and ciphered image. The correlation between the adjacent pixels can be calculated by [16]:

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

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2 \qquad (27)$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})$$

Where N is the total number of pixels, $\bar{x},\bar{y}$ are the mean values of x_i and y_i. To analyse the correlation coefficient, we selected 1000 pairs of adjacent pixels from the horizontal, vertical and diagonal direction of the plain image and cipher image the of Lena (512 X 512) in Fig. 10 and Fig. 12. The correlation graph and the values of the plain and ciphered image are given in Fig. 16 and Fig. 17 below:

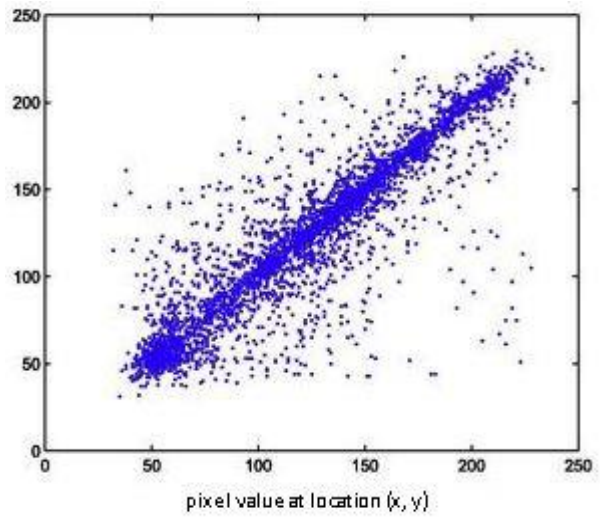

Figure 16. Correlation Coefficient of the Original Image

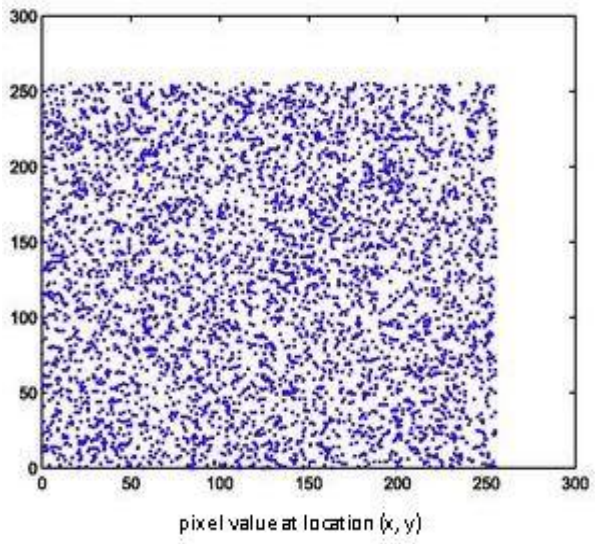

Figure 17. Correlation Coefficient of the Cipher Image.

From the above figures we can say that the two adjacent pixels are highly correlated for the original image and is concentrated in a certain region which can be seen in Fig.16 whereas there is a very negligible correlation between the two adjacent pixels in the cipher image as the pixels are scattered in Fig.17.

Table 2 gives the calculations of the correlation coefficients of two adjacent pixels in Fig. 10 and Fig. 12. The results indicate that the correlation of the adjacent pixels in plain image is very significant, while that of ciphered image is very small, so the encryption is satisfactory.

Table 2. Correlation coefficients of the two adjacent pixels in original and cipher image

Correlation	Horizontal	Vertical	Diagonal
Plain image Fig.10	0.9735	0.9992	0.9587
Encrypted image Fig.12	0.04175	**0.00039**	**-0.00052**
Lena in [16]	−0.0084	0.0004	-0.0015

f. Information Entropy Analysis

Information entropy is the measure of randomness that defines the texture in an image. It is calculated by [17]:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) log_2 \frac{1}{p(m_i)} \quad (28)$$

Where, p (m_i) is the probability of message m_i. The ideal value of the entropy of an encrypted image is 8. The Table 3 below shows the information entropy values of three colour components; the results are all close to the ideal value of 8 and better than in ref [15,16] which makes the algorithm resist against entropy attack.

Table 3. Information Entropy value for the cipher image

Ciphered Image	R	G	B
Fig.12	**7.9989**	**7.9976**	7.9956
Lena in [15]	7.9973	7.9971	7.9968
Lena in [16]	7.9893	7.9896	7.9903

g. Speed Performance Analysis

Speed of an algorithm is an important factor for an ideal encryption scheme. In this we have measured encryption speed of colour image of different sizes. The speed analysis is done in MATLAB 2018a on a desktop having specification as Windows 10 AMD A9 7th generation, 4GB RAM with 64-bit operating system. The encryption/decryption time taken by the proposed cryptosystem for different sized image is shown in Table 4. below:

Table 4. Time analysis for various image sizes

Image Size (in pixels)	Image size (in Kb)	Time (in Sec)
64x64	10.2	0.016
128x128	16.8	0.021
256x256	38.0	0.141
512x512	61.5	0.762
1024x1024	136.0	1.104
2048x2048	104.0	3.163

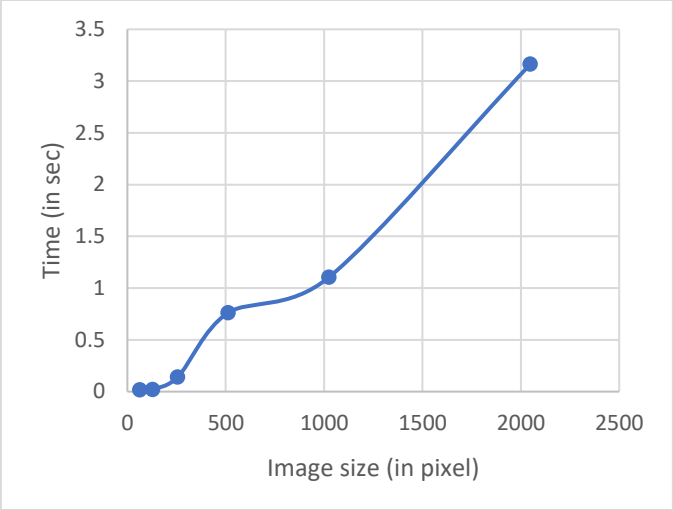

Figure 18. Plot of image size and time taken for encryption

From the above graph we can say that the relationship between size and time is nearly linear, which means size of the image is proportional to time taken for encryption/decryption.

h. Noise Attack Analysis

A good encryption scheme should be resistant against noise jamming. Here we add salt & Pepper noise and white Gaussian noise, respectively, to the ciphered image Lena of Fig. 12. The deciphered image below in Fig. 19 a,b shows that as we increase salt & Pepper noise density from 0.01 to 0.1, more noise points appear in the deciphered Lena, but the deciphered Lena can still be distinguishable. Similarly, we add the white Gaussian noise, when the mean value is set to zero, more noise points appear in the deciphered Lena with the increase of variance, from 0.001 to 0.01 and the deciphered Lena is still distinguishable. The overall effect of resisting against noise is better than that in Ref. [18].

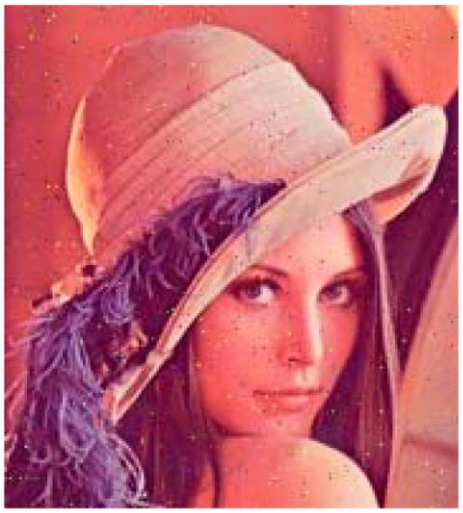

Figure 19a. The deciphered image with salt and pepper noise, d=0.01

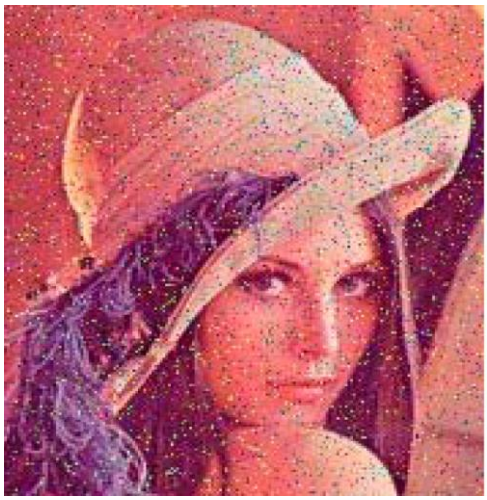

Figure 19b. The deciphered image with salt and pepper noise, d=0.1

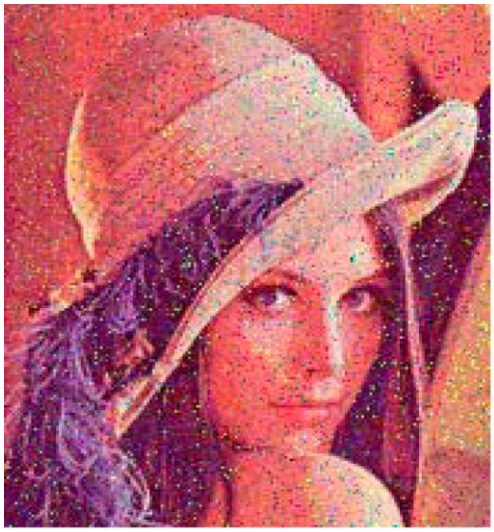

Figure 19c. The deciphered image with white gaussian noise, m = 0, v = 0.001

Figure 19d. The deciphered image with white gaussian noise, m = 0, v = 0.01

VI. CONCLUSION

In this paper, a new chaos-based cryptosystem is proposed which generates one-time-key using the hash value of the noise followed by XOR operation. The advantage of using a one-time password is that even if the attacker retrieves the plaintext and ciphertext pairs, it is very difficult to decrypt the next cipher as the same key cannot be re-used for the next encryption process. The cryptosystem is ineffective plaintext, ciphertext, differential and brute force attack. A detailed analysis of the proposed cryptosystem is carried out using MATLAB and the experimental results such as correlation coefficient, information entropy, noise attack analysis suggest that the proposed cryptosystem is efficient and can be used for real-time applications.

Declaration

***Funding –** No funding was received for conducting this study.

***Conflicts of interest/Competing interests-** The authors declare that there is no conflict of interest.

***Availability of data material –** The authors confirm that the data supporting the findings of this study are available within the article and in its supplementary materials. The data that support the findings of this study are available on request from the corresponding author **I. Raja Mohamed.**

***Code availability- MATLAB** software used for the analysis and is available in supplementary file.

***Author's contributions -** All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by **Namrata Biswas** under the supervision of **I. Raja Mohamed**. The first draft of the manuscript was written by **Namrata Biswas** and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

[1] Zhang, Q., Guo, L., Wei, X.P.: Image encryption using DNA addition combining with chaotic map as. Math. Comput.Model. 52, 2028–2035 (2010)

[2] Mao, Y.B., Chen, G.R., Lian, S.G.: A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurc. Chaos 14, 3613–3624 (2004)

[3] G.A.Sathishkumar, K. Bhoopathybagan, N. Sriraam, Image encryption based on diffusion and multiple chaotic maps, International Journal of Network Security & ItsApplications,3(2)(2011)181–194.

[4] A.ElLatif, L.Li,N.Wang, X.Niu,Image encryption scheme of pixel bit based on combination of chaotic systems, in: 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp.369–373.

[5] A.Kanso, M.Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simul.17(7) (2012) 2943–2959.

[6] S. Behnia, A.Akhshani, H.Mahmodi, A.Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos Solitons Fractals 35(2)(2008)408–419.

[7] Shannon, C.E.: 'Communication theory of secrecy systems', Bell Syst. Tech.J., 1949, 28, (4), pp. 656–715

[8] François, M., Grosges, T., Barchiesi, D., et al.: 'Pseudo-random number generator based on mixing of three chaotic maps', Commun. Nonlinear Sci.Numer. Simul., 2014, 19, (4), pp. 887–895

[9] ECRYPT I I. Yearly Report on Algorithms and Key sizes (2012). D. SPA. 20 Rev. 1.0[R]. ICT-2007-216676 ECRYPT II, 2012

[10] G. Chen, Y. Mao, and C. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals.21(2004) 749–761.

[11] Xiao, D., Zhang, Y.S.: 'Self-adaptive permutation and combined global diffusion for chaotic color image encryption', AEU – Int. J. Electron. Commun., 2014, 68, (4), pp. 361–368

[12] Zhang, Y.Q., Wang, X.Y.: 'A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice', Inf. Sci., 2014, 273, pp. 329–351

[13] Dong, C.: 'Color image encryption using one-time keys and coupled chaotic systems', Signal Process., Image Commun., 2014, 29, (5), pp. 628–640

[14] Yang, Y.G., Xu, P., Yang, R., et al.: 'Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudorandom number generation and image encryption', Sci. Rep., 2016, 6, article number: 1978

[15] Chen, J., Zhu, Z., Fu, C., et al.: 'A fast chaos based image encryption scheme with a dynamic state variables selection mechanism', Commun. Nonlinear Sci. Numer. Simul., 2015, 20, (3), pp. 846–860

[16] Wu, X., Kan, H., Kurths, J.: 'A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps', Appl. Soft Comput., 2015, 37, pp. 24–39

[17] Norouzi, B., Mirzakuchaki, S.: 'A fast color image encryption algorithm based on hyper-chaotic systems', Nonlinear Dyn., 2014, 78, (2), pp. 995–1015

[18] Dong, C.: 'Color image encryption using one-time keys and coupled chaotic systems', *Signal Process., Image Commun.*, 2014, **29**, (5), pp. 628–640

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- final.m
- final1.m
- sourcecodes.docx