Journal of Engineering and Applied Sciences 13 (15): 6275-6280, 2018
ISSN: 1816-949X

Color Image Cryptography Based on Fraction Order Chaotic Systems

Weaam Talaat Ali, Warqaa Shaher Al Azawee and Zobeda Hatif Naji Al-Azzawi
Department of Computer Engineering, College of Engineering, University of Diyala, Baqubah, Iraq

Abstract: The increasing of demands for securely transfer of images through the internet and wireless systems gave the importance to cryptography systems. In this paper, image encryption technique come with chaos. Lorenz and Chua chaotic systems with fractional order that produces enlarged in key space are used to encrypt image. A high robustness and security for encryption process are guaranteed by using these chaotic systems with all properties which are owned such randomness, nonlinearity and the large key space. From the results, the low Peak Signal to Noise Ratio (PSNR) (around 8 dB) when any small change in any of the system parameters and perfect PSNR for the decrypted image. That shows the encrypted key has a large sensitivity to small change in any parameters of Lorenz or Chua chaotic systems. Consequently, a high complicated image encryption is suggested using the proposed system that is shown here.

Key words: Chaos, key space, fractional order, cryptosystem, Lorenz system, Chua system

INTRODUCTION

In recent years, the image encryption has been rapidly developed. To guarantee the security of transfer images and protect information from falling into violation hands, the encryption image concept has attracted people as inventive solutions for safe image commutation Zhaoa *et al.,* 2016; Jakub *et al.,* 2018).

Encryption involves converting a message data into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers (Nagaria *et al.,* 2012). Chaos-based encryption techniques have been preferred compared to other methods that are proposed in the literature before because they provide a good combination of speed and high security. In general, chaotic systems have some properties such as randomness, sensitivity to initial condition and ergodicity. These properties are essential in building cryptosystems and make them a good candidate for cryptography (Guesmi *et al.,* 2016).

Fractional order Lorenz and Chua chaotic systems are used in this paper to generate an encryption algorithm of color image that is provided increasing in the security level and robustness of the cryptosystem.

Chaotic cryptography: A response of nonlinear physical system can be evolved to chaotic behaviors at a specific parameters values of that system. The sensitivity to initial conditions, no periodicity topological transitivity, pseudorandom property and all other properties owned by Chaotic crypto systems. All these characteristics make it widely used in practical applications. Most properties provide some requirements such as diffusion and mixing in the sense of cryptography (Sankaran and Krishna, 2011).

Lorenz and chua systems with fractional order: Mathematical described for fractional-order Lorenz system is (Nicholas, 2015).

$$\begin{aligned} D^{\alpha 1}x &= \sigma(y-x) \\ D^{\alpha 2}y &= -xz+\rho_L x-y \\ D^{\alpha 3}z &= xy-\beta_L z \end{aligned} \quad (1)$$

where (σ_L, ρ_L, β_L) are system parameters ($\alpha 1$, $\alpha 2$ and $\alpha 3$) determine the fractional orders of the equation and ($\alpha 1$, $\alpha 2$, $\alpha 3>0$) and for Chua system (Leon, 1992).

$$\begin{aligned} D^{\varepsilon 1}x &= \sigma_c(y-x)-\sigma_c F(x) \\ D^{\varepsilon 2}y &= x-y+z \\ D^{\varepsilon 3}z &= -(\rho_c y+\beta_c z) \\ F(x) &= m_1 x+(m_0-m_1)(|x+1|-|x-1|) \end{aligned} \quad (2)$$

Corresponding Author: Weaam Talaat Ali, Department of Computer Engineering, College of Engineering, University of Diyala, Baqubah, Iraq

(a)

i	1	2	3	4	5	6	7	8	9	10
y(I)	0.32	0.91	1.7	-0.39	-1.27	-1.36	-1.02	-1.53	-0.43	-0.88

(b)

8	6	5	7	10	9	4	1	2	3
-1.53	-1.36	-1.27	-1.02	-0.88	-0.43	-0.39	0.32	0.91	1.7

(c)

Input index	1	2	3	4	5	6	7	8	9	10
Output index	8	6	5	7	10	9	4	1	2	3

Fig. 1: Generation of permutation key: a) Original sequence; b) Ascending order sequence and c) New shuffled order

where (σ_C, ρ_c, β_c m_0, m_1) are system parameters (ε_1, ε_2 and ε_3) are fractional orders of the equation and ($\alpha1$, $\alpha2$, $\alpha3>0$). Using fractional backward difference methods (Sun *et al*., 2010) fractional Lorenz system can besolved as:

$$\begin{cases} x_m = h^{\alpha1} * \left[\sigma_L * (y_{m-1} - x_m)\right] - \sum_{k=1}^{m} w_k x(m-k_h) \\ y_m = h^{\alpha2} * \left[\begin{matrix} -z_{m-1} * x_{m-1} + \rho_L * x_{m-1} - \\ y_{m-1} \end{matrix}\right] - \sum_{k=1}^{m} w_k x(m-k_h) \\ z_m = h^{\alpha3} * [x_{m-1} * y_{m-1} - \beta_L * z_{m-1}] - \sum_{k=1}^{m} w_k z(m-k_h) \end{cases} \quad (3)$$

Also, it can be written for Chua system as:

$$\begin{cases} y_m = h^{\varepsilon1} * [x_{m-1} - y_{m-1} + z_{m-1}] - \sum_{k=1}^{m} w_k y(m-k_h) \\ y_m = h^{\varepsilon2} * [-x_{m-1} - y_{m-1} + z_{m-1} -] - \sum_{k=1}^{m} w_k y(m-k_h) \\ z_m = h^{\varepsilon3} * [-\rho c * y_{m-1} - \beta * z_{m-1}] - \sum_{k=1}^{m} w_k z(m-k_h) \end{cases} \quad (4)$$

where, m = 0, 1, 2, ..., N and h, is step size parameter. The coefficients w_k can be calculated in a recursive scheme (with w_0 = 1) by:

$$wk = \left(1 - \frac{\varphi+1}{k}\right) w_{k-1} \quad (5)$$

where, φ is order of chaotic sequence.

Key generation using fractional chaotic systems: Two groups of keys are used in this proposed system, one is used to pixel permutation and second to pixel value XORed with key.

All sequences (x_L, y_L, z_L, x_C, y_C and z)$_c$ that are computed by applied (Eq.3 and 4) for fractional-order Lorenz system and fractional-order Chua system respectively are used as permutation keys. A chaotic sequence with length equal to N is sorted in ascending order. So that, the indexes will change, resulting new indexes are taken as the shuffled order. Figure 1 shows an example with N = 10 for permutation key generated.

Now, to generate second kind of the encryption keys, for XORed process, magnification and modulo transformation is done to chaotic sequences by Eq. 6 (Ahmad and Farooq, 2010):

$$\begin{cases} M_L(n) = \mathrm{mod}\left(\mathrm{floor}\left(M_L(n) \times 10^{15}\right), 2^N\right) \text{for Lorenz} \\ M_c(n) = \mathrm{mod}\left(\mathrm{floor}\left(M_c(n) \times 10^{16}\right), 2^N\right) \text{for Chua} \end{cases} \quad (6)$$

Where:

M_L and M_c = (x, y, z) sequences for Lorenz and Chua

M_C respectively

N = Maximum number of bits required to quantize M

Now, the fractional-order of Lorenz and Chua sequences arecombined together by using XOR to get new keys as in Eq. 7:

$$\begin{aligned} K_1(n) &= \mathrm{BITXOR}\left(x_L(n), x_c(n)\right) \\ K_2(n) &= \mathrm{BITXOR}\left(y_L(n), y_c(n)\right) \\ K_3(n) &= \mathrm{BITXOR}\left(z_L(n), z_c(n)\right) \end{aligned} \quad (7)$$

By combine those chaotic sequences, encryption process complexity is enhanced the security level and the robustness of the cryptosystem are improved.

MATERIALS AND METHODS

System model and statistical factors

System model: Figure 2 shows the proposed system. Firstly, the color image is separated to three fundamental layers (red, green and blue) with M rows and N column. After that, five steps will be performed to create encrypted color image. The proposed encryption algorithm illustrates as:

Algorthm 1; The proposed encryption algorithm:

Input: An P image with M×N×3

Output: Encrypted EP image with same original size

Step 1: Each layer (P^r, P^g and P^b) is reshaped to one dimension vector (P^r_{od}, P^g_{od} and P^b_{od}) with (M*N) elements

Step 2: Each of generated vectors is permutated to rearrange order

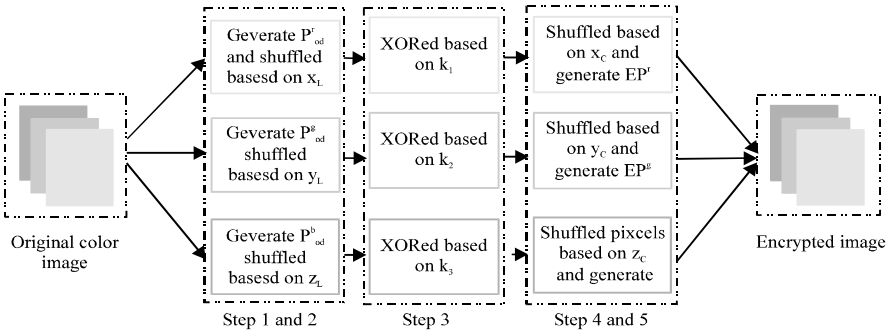

Fig. 2: Block diagram of proposed method of encryption image using two chaotic systems

depending on one of chaotic sequences that are generated by fractional order Lorenz system. red vector P^r_{od} is shuffled based on x_L sequence, green vector P^g_{od} is shuffled based on y_L sequence and blue vectorP^b_{od} is shuffled based on z_L sequence

Step 3: Each of resulting vectors from step2 is XORed with chaotic keys (k_1, k_2 and k_3 respectively) that are generated using Lorenz and Chua systems

Step 4: Every vector resulted from step3 is shuffled again but now depending on chaotic Chua sequences (x_C, y_C and z_C respectively)

Step 5: Each vector produced by step 4 is back with M row and N column to generate (EP^r, EP^g and EP^b). After that, they are merged together to generate encrypted image

All steps that are used in image encryption will be followed with reversely order to decrypt the image. The fractional orders, initial values and control parameters that are used to generate chaotic sequences must be same in encryption and decryption process.

Image statistical factors: Many statistical factors are used in this paper to test the proposed image encryption scheme. The encrypted image should be extremely various from its original image as a general requirement for all the image encryptions chemes. Such difference can be measured by Number of Pixel Change Rate (NPCR) (Mannai *et al*., 2015) as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \quad (8)$$

where, L is the totalnumber of pixels in the image and D(i, j) is defined by Eq. 9:

$$D(i,j) = \begin{cases} 0 \text{ if } M(i,j) = M'(i,j) \\ 1 \text{ if } M(i,j) \neq M'(i,j) \end{cases} \quad (9)$$

where, M(i, j) and M′(i, j) are the pixel values of the two images M and M′, respectively. Normalized Correlation NC is used here to computed the similarity between encrypted and decrypted image according to Eq. 10.

$$NC = \frac{\sum_{K=1}^{QN} M(K) M'(K)}{\sqrt{\sum_{K=1}^{QN} M(K)^2} \sqrt{\sum_{K=1}^{QN} M'(K)^2}} \quad (10)$$

where, M and M' are original and received images respectively, QN represents pixel position in each one of them (Kaur and Kumar, 2018). Also, Peak signal to Noise Ratio (PSNR) is presented as another comparison parameter as (Kaur and Kumar., 2018):

$$PSNR = 10 \log_{10} \frac{Max^2}{\frac{1}{M \times N \times 3} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{3} \left(D(i,j,k) - S(i,j,k) \right)^2} \quad (11)$$

where, N and M are height and width of image respectively, Max is the maximum possible pixel value of the image, S (i, j, k) is the original image. D (i, j, k) is the decrypted image.

RESULTS AND DISCUSSION

Simulation results: Table 1 illustrate the constraints values for the fraction-order. Lorenz and Chua systems that are used in this paper to generate secure chaotic sequences utilized to create encrypted keys. In this simulation, Lena and Peppers color images of size 256×256×3 pixels are used as an original image to test the proposed encryption algorithm.

Histogram analysis: The image histogram is a graphic that tells us how the pixels are distributed at each color intensity level of the image. In the histogram of ciphered images all pixel values from 0-255 are equally probable and the image looks like a random. The original, encrypted and decrypted images generated by using chaotic sequences and their histograms are shown in Fig. 3-6.

Table 1: Constraints values for the fraction-order Lorenz and Chua systems

	Fraction-order Lorenz systems			Fraction-order Chua system				
Parameter	σ_L	ρ_L	β_L	σ_C	ρ_C	β_C	m_0	m_1
Control parameters	10	28	8/3	10	14.78	0.0385	1.27	0.68
Initial conditions	x(0)	y(0)	z (0)	x(0)	y(0)		z (0)	
	0.11	-0.2	20	0.19	0.1		0.1	
Fraction order	α1	α2	α3	ε_1	ε2		ε3	
	0.965	0.985	1.115	0.975	1.001		1.011	
Step-size		h = 0.01					h = 0. 01	

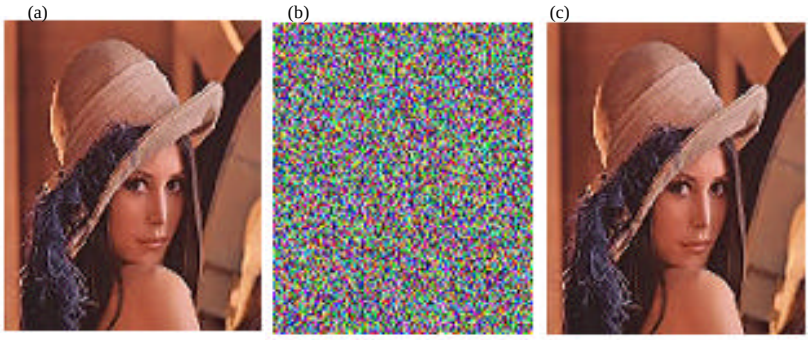

Fig. 3: Lena image: a) Original image; b) Encrypted image and c) Decrypted image

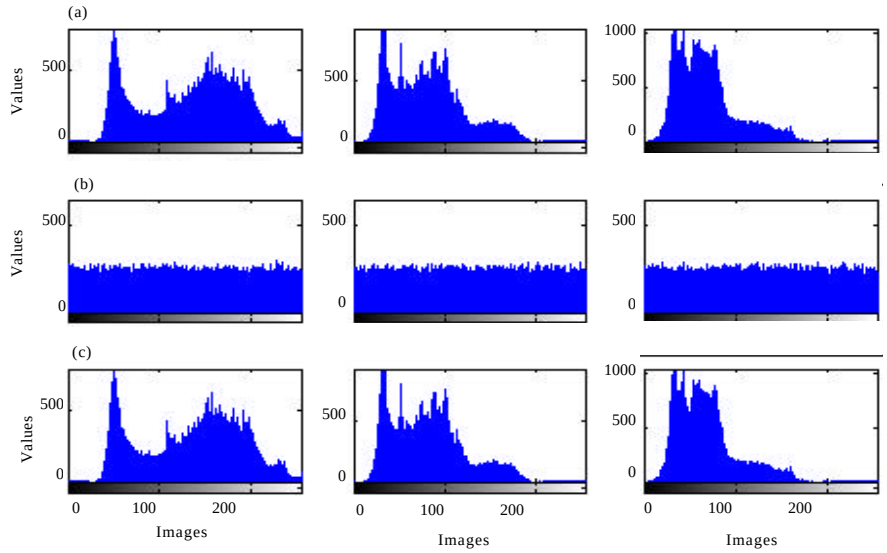

Fig. 4: Histogram of original, encrypted and decrypted lena image: a) Red channel histogram and b) Green channel histogram and Blue channel histogram

It is clear from these figures that the histogram for all layers of encrypted images are uniformand significantly different from the original images. And so, it does not afford any clue to employ an attack on the proposed image encryption algorithm.

Image statistical analysis: Table 2 shows statistical analysis between original, encrypted and decrypted Lena and Peppers images. The very high NPCR and a tiny NC values between the original and encrypted images indicate a significant change in the pixel's values for the original image that makes impossibility to any one discover the original content of the encrypted image without used the same key that is used in the encrypted process.

Sensitivity to chaotic parameters: To test the influence of variation any Lorenz and Chua systems parameters, two identical chaotic systems have same parameters except a tiny change in one of fractional orders or initial

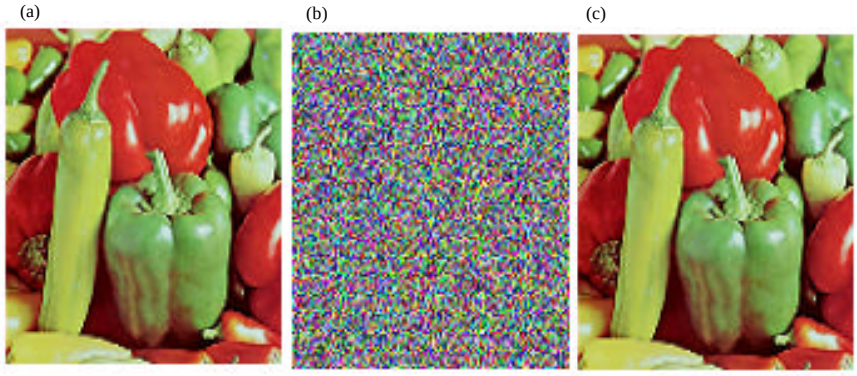

Fig. 5: Peppers image: a) Original image; b) Encrypted image and c) Decrypted image

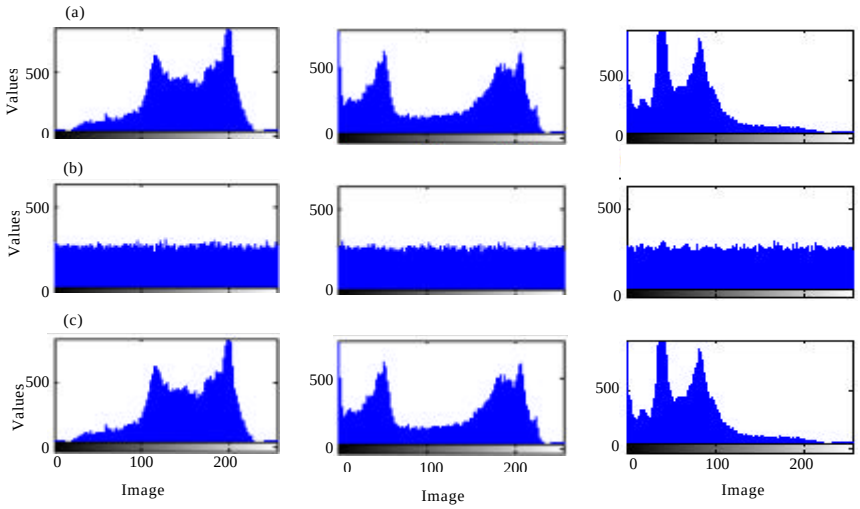

Fig. 6: Histogram of original, encrypted and decrypted peppers image: a) Red channel histogram and b) Green channel histogram and Blue channel histogram

Table 2: Statistical analysis of original, encrypted and decrypted images

Statistical analysis results	Lena	Peppers
NPCR between original and encryption image		
(Red channel)	99.604	99.595
(Green channel)	99.598	99.614
(Blue channel)	99.669	99.639
Results between original and encryption image	8.4440	8.1230
(PSNR dB)	-0.0012	-0.0013
(NC)		
Results between original and decryption image	Infinity	Infinity
(PSNR dB)	1	1
(NC)		

conditions or control parameters (chosen to be 10^{-8}) are used, first to encryption process and second to decryption process.

Figure 7 and 8 show decrypted Lena image and its histogram as examples for effects any change in one parameters of decrypted system. Figure 7 illustrates decrypted Lena image with same parameters used in encryption except of $\alpha 1 = 0.96500001$ for Lorenz system and Fig. 8 illustrates decrypted Lena image with $x(0)_{Chua} = 0.19000001$ for Lorenz system.

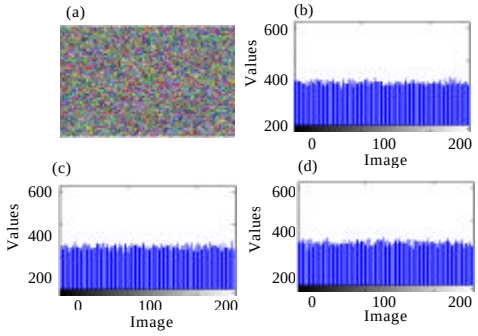

Fig. 7: Decrypted Lena image and its histogram with deference in fraction-order of Lorenz $\alpha+10^{-8}$: a) Decrypted image; b) Red channel histogram; c) Green channel histogram and d) Blue channel histogram

The similarity, between original and decrypted Lena image is summarized in Table 3. The key used to decrypt image is generated corresponding to a tiny amount of 10^{-8} variation in one parameter at a time of chaotic systems

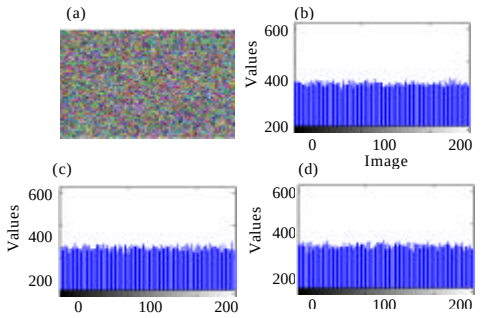

Fig. 8: Decrypted lena image and its histogram with deference in initial X(0)+10^{-8} of Chua: a) Decrypted image; b) Red channel histogram; c) Green channel histogram and d) Blue channel histogram

Table 3: The similarity between original and decrypted image

Parameter variated by 10^{-8}	PSNR (dB)	NC	Parameter changed by 10^{-8}	PSNR (dB)	NC
$\alpha 1$	8.432	-0.00129	$\gamma 1$	8.437	0.00324
$\alpha 2$	8.431	-0.00066	$\gamma 2$	8.429	-0.00136
$\alpha 3$	8.426	-0.00133	$\gamma 3$	8.450	0.00275
$x(0)_{Lorenz}$	8.451	0.00303	$x(0)_{Chua}$	8.442	-0.00149
$y(0)_{Lorenz}$	8.412	-0.00332	$y(0)_{Chua}$	8.443	-0.00050
$z(0)_{Lorenz}$	8.447	0.00246	$z(0)_{Chua}$	8.417	-0.00635
σ_L	8.445	0.00288	σ_C	8.444	0.00111
ρ_L	8.465	0.00261	ρ_C	8.439	0.00398
β_L	8.419	-0.00313	β_C	8.421	-0.00283

that are used in encryption process and keeping all other parameters unchanged. From Table 3 a small variation in one parameter of. Lorenz or Chua system shows the high sensitivity for encrypted and decrypted processes. These results show that high secure and quality are performed by proposed encryption algorithm.

Key space and security: The large number of parametersthat are used to generate encryption key gives large key space dimension and it is important to resist attack. Fraction-order, ($\alpha 1$, $\alpha 2$, $\alpha 3$, $\gamma 1$, $\gamma 2$, $\gamma 3$,) control parameters (σ_L, ρ_L, β_l, σ_c, ρ_c, β_c, m_0, m_1) and initial values of the chaotic systems have highly effected on the secret key that is used to encrypt and decrypt images.

CONCLUSION

In this paper, chaotic systems with high dimensional like fractional-order Lorenz and Chua are applied to generate six chaotic sequences have more complex and unpredictable properties. Pixels shuffling and XORed are performed by these high secure chaotic sequences generate complicated image encryption system. From results a high security is guaranteed by high NPCR results and low NC between original and encryption image. Also, a large key sensitivity is produced by used this system whereas a very small changing the secret parametercauses a large changein the decrypted image as shown by low PSNR and NC values when compared the similarity between decrypted image using incorrect parameter with original image. With the using of fractional order chaotic systems as the keys make the key space enlargeand warranty to high security.

REFERENCES

Ahmad, M. and O. Farooq, 2010. A multi-level blocks scrambling based chaotic image cipher. Proceedings of the 3rd International Conference on Contemporary Computing, August 9-11, 2010, Noida, India, pp: 171-182.

Guesmi, R., M.A.B. Farah, A. Kachouri and M. Samet, 2016. Hash Key-based image encryption using crossover operator and chaos. Multimedia Tools Appl., 75: 4753-4769.

Kaur, M. and V. Kumar, 2018. Colour image encryption technique using differential evolution in Non-subsampled contourlet transform domain. IET. Image Process., 12: 1273-1283.

Leon, O.C., 1992. The genesis of chua's circuit. CiteSeerX. Sci. Documents, 46: 250-257.

Mannai, O., R. Bechikh, H. Hermassi, R. Rhouma and S. Belghith, 2015. A new image encryption scheme based on a simple First-order Time-delay system with appropriate nonlinearity. Nonlinear Dyn., 82: 107-117.

Nagaria, B., A. Parikh, S. Mandliya and N. Shrivastav, 2012. Steganographic approach for data hiding using LSB techniques. Intl. J. Adv. Comput. Res., 2: 441-445.

Nicholas, R.R., 2015. Introduction to Lorenz's system of equations. J. Math, Vol. 2015,

Oravec, J., J. Turan and L. Ovsenik, 2018. Image encryption technique with key diffused by coupled map lattice. Proceedings of the 2018 28th International Conference on Radioelektronika (RADIOELEKTRONIKA), April 19-20, 2018, IEEE, Prague, Czech Republic, ISBN:978-1-5386-2485-2, pp: 1-6.

Sankaran, K.S. and B.V.S. Krishna, 2011. A new chaotic algorithm for image encryption and decryption of digital color images. Int. J. Inform. Educ. Technol., 1: 137-141.

Sun, K., X. Wang and J.C. Sprott, 2010. Bifurcations and chaos in Fractional-order simplified Lorenz system. Intl. J. Bifurcation Chaos, 20: 1209-1219.

Zhao, T., Q. Ran, L. Yuan, Y. Chi and J. Ma, 2016. Optical image encryption using password key based on phase retrieval algorithm. J. Mod. Opt., 63: 771-776.