Al-Qadisiyah Journal of Pure Science

Volume 26 | Number 3 Article 11

7-7-2021

Text Encryption Method Using multi Hyper-chaotic systems

Hayder A. Qasim
Ministary of Education,Baghdad, Iraq, marun_11981@yahoo.com

Recommended Citation
Qasim, Hayder A. (2021) "Text Encryption Method Using multi Hyper-chaotic systems," *Al-Qadisiyah Journal of Pure Science*: Vol. 26: No. 3, Article 11.
DOI: 10.29350/qjps.2021.26.3.1307
Available at: https://qjps.researchcommons.org/home/vol26/iss3/11

Al-Qadisiyah Journal of Pure Science

QJPS

Al-Qadisiyah Journal of Pure Science

ISSN(Printed): 1997-2490 ISSN(Online): 2411-3514

DOI : /10.29350/jops.

http://qu.edu.iq/journalsc/index.php/JOPS

Text Encryption Method Using multi Hyper-chaotic systems

Authors Names

Hayder A. Qasim

Article History

Received on: 17/ 3/2021
Revised on: 9/ 5/2021
Accepted on: 24/5/2021

Keywords:

Hyper-chaotic
Initial conditions
ASCII code
XOR operation

DOI:

https://doi.org/10.29350/ jops.2021.26. 3. 1307

ABSTRACT

With rapid evaluation of technologies, huge amount of critical information can exchange over unsecure network every day, secure and fast encryption schemes become more and more urgent need to provide the desirable confidentiality and thwart unauthorized access, lately and for many reasons, chaotic based encryption algorithms become more and more popular technique due to exceptionally superior characteristics such as simplicity, resistance attacks and high speed, in this paper the advantages of two nonlinear hyper-chaotic systems will utilized to strength the proposed encryption algorithm, the random sequences generated from systems will used to position scramble and value change of the plaintext, the main features of such method are efficiency, large key space, low computational overhead, and simple design as well as the experimental results demonstrate that the proposed method have more ability to thwart attacks.

Ministry of Education,Baghdad, Iraq, E-Mail: marun_11981 @yahoo.com

1. Introduction

Now days, people and companies exchange huge confidential information over internet and mobile network, the security of data become critical issue with increase the threat of attacks, cryptography is must important technique that allow to communication over unsecure network with preserving the message secrecy, and also support solutions to data integrity, authentication, non-repudiation etc.[7]

Cryptography can be categorize to Symmetric key cryptography and Asymmetric key cryptography, Symmetric key include that the sender and receiver will share the same secret key, during encryption operation, the sender use the key to encrypt the plain text, and through the decryption operation at the other end the receiver use the key to decrypt the cipher text and recover the plain text again, commonly examples algorithms like Data Encryption standard (DES) and Advance Encryption Standard (AES), with Asymmetric key cryptography, public key will utilized to encrypt the plain text, will the receiver who owns the private key can decrypt the cipher text and recover the plain text, Rivest-Shamir-Adleman (RSA) algorithm , an example of this type [12]

Many disadvantages associated the traditional encryption algorithms like high computational overhead, difficult to understand and inappropriate for real time application, some researchers propose chaotic based encryption algorithm, that characteristic with many desirable features such as high security, less computational overhead and easy to implement [10].

To strengthen the security, a new text encryption algorithm introduced based on two hyper-chaotic systems, the experimental results show more efficiency, fast, desirable security and less computational overhead.

2.Related work

This section introduced brief summary of present text encryption algorithm based chaotic map, the British mathematician Matthews was the first who utilized the chaotic map for encryption in 1989, low dimension logistic map generate chaotic sequence which can be used as one time pad to encrypt text message [5], more and more researchers based chaos for encryption, in[1] proposed chaos encryption method, three different non-linear low dimension chaos generator are employ, Pinchers Map, Logistic Map and Sine-Circle Map which are commonly referred in the literature used to realize application, the cipher needed for encryption is generated by chaos generators to increase the ambiguity at the same time and to enhance the security of communication additional nonlinear function is used ,the important advantage of text encryption with these three chaotic generators is that the encryption can be realized by using microprocessor or FPGA, the performance analysis of method considering the value of entropy and time, which demonstrate that the proposed algorithm is efficient and feasible to employ.in[2]introduced text encryption algorithm process data as blocks and consists of multilevel (coding of character, generates array of keys(weight), coding of text and chaotic NN), also the decryption process consists of multilevel (generates array of keys(weights), chaotic NN, decoding of text and decoding of character) the chaotic neural network is used as a part of the proposed system with modifying on it, the proposed key generation algorithm formed the keys that are used in chaotic sequence, with based random key generator and chaotic neural network, the coding and decoding of character algorithms will transform the value to another value, and the proposed generating key(weights) algorithm will be based on scramble the positions of data and transformed it, the result data from this algorithm will be used as weights in encryption and decryption process in addition to the weights that are generated by chaotic neural network, the proposed system characteristic's with efficiency and security and the long messages can be encryption and decryption with small memory and short time, in [8] proposed chaotic based encryption algorithm to encrypt text , the algorithm utilized the nature of non-linear chaotic map by using MS map as a key stream generator, the key stream generated by MS map will be operated with the plaintext by XOR(exclusive-OR) operation to produce the ciphertext, the same key stream will be operated with the ciphertext by XOR operation to produce the decrypted text, and to test the performance of proposed algorithm plaintexts with different length are used, the plaintext characters are based on ASCII code, the performance analysis ensure that the result ciphertext is very secure and difficult to be cracked by the brute-force attack and known-plaintext attack, and any small change in decryption key lead to completely different plaintext.

3.Hyper-chaotic systems

Recently, hyper-chaotic systems attract more attention in wide applications like nonlinear circuits, cryptography, secure communications, and synchronization[13], in cryptography utilized of hyper-chaotic systems lead to desirable cryptography characteristics such as high randomness, unpredictability, high capacity, more security and efficiency [9], proposed encryption method utilized the chaotic sequence generated from different hyper-chaotic systems to encrypt message text, Rossler hyper-chaotic system which can be described as[3] :

$$\begin{aligned} \dot{x}&=-y-z,\\ \dot{y}&=x+ay+w, \qquad (1)\\ \dot{z}&=b+xz,\\ \dot{w}&=-cz+dw, \end{aligned}$$

The hyper-chaotic behavior generated when the control parameters values chosen as: a= 0.25, b=3, c=0.5, d=0.05, and initial conditions taken as (-10,-6, 0,10).

In addition, the second hyper-chaotic system used expressed by the following mathematical equations [14]:

$$\begin{aligned} \dot{x}&=y-xz-yz+w,\\ \dot{y}&=axz+d, \qquad (2)\\ \dot{z}&=y^2-bz^2,\\ \dot{w}&=-cy, \end{aligned}$$

And display hyper-chaotic attractor when the values of real parameters a=5, b=0.28, c=0.05,d= -0.001 and the initial conditions selected as (0,0,0.8,0.02).

4. Proposed Encryption Algorithm

this section presented the encryption cryptosystem that take the, letters, digits, punctuation marks, and miscellaneous symbols as input, the plaintext converted into integers that represent their corresponding arithmetic ASCII code between 0 and 128, the hyper-chaotic systems iterate with the values of initial conditions and control parameters mentioned to generate the chaotic sequence which utilized as key to encrypt plaintext and produce the ciphertext, the detailed encryption procedure described as follows:

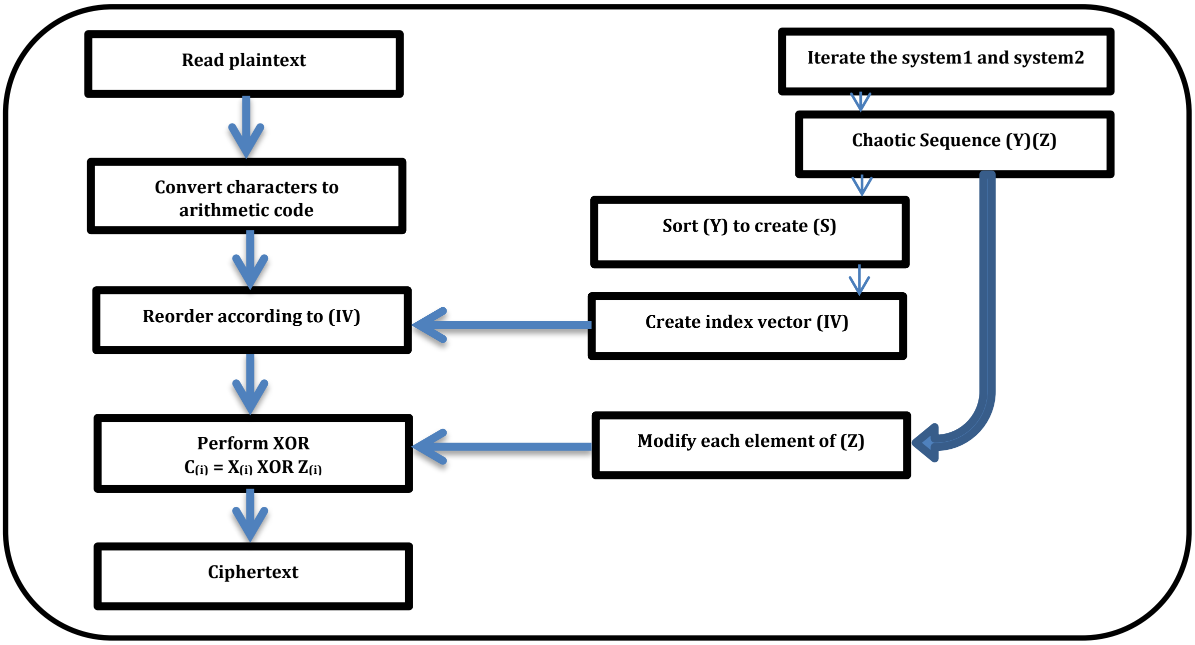

Read plaintext
Iterate the system1 and system2
Chaotic Sequence (Y)(Z)
Convert characters to arithmetic code
Sort (Y) to create (S)
Reorder according to (IV)
Create index vector (IV)
Perform XOR $C_{(i)} = X_{(i)}$ XOR $Z_{(i)}$
Modify each element of (Z)
Ciphertext

Figure (1): the proposed method

Algorithm (1): Proposed Encryption Algorithm

Input:

- Plaintext
- Initial condition and control parameter

Output :

- Ciphertext

Step1: Read the string of plaintext (X) of size N and convert to their corresponding arithmetic code.

Step2:Iterate the system (1) and system (2) with the values of control parameters and initial conditions, after many rounds we can get two chaotic sequences Y , Z of chaotic real numbers, convert each matrix to vector of size N.

Step3: Sort vector Y in ascending order manner to create vector S,for each element (i) in S

- **Find its position in vector Y**
- **Store its position in index vector IV**

Steps4: Reorder the elements of (X) in step1 according to index vector IV.

Steps5: Modify each element of chaotic sequence Z using the following formula:

$$x = \text{double}\ (\text{uint8}(\text{mod}\ (\ \text{ceil}(\ (x \times 10^{14}) \div 64))\ , 127\ ))) \qquad (3)$$

Wheredouble returns the double − precision , uint8 converts the element into unsigned 8 − bit integer, ceil(i)returns the nearest integer less than or equal to i and mod returns the remainder after division.

Steps6: Perform XOR between the elements of plain text Xand Z, employ the following formula :

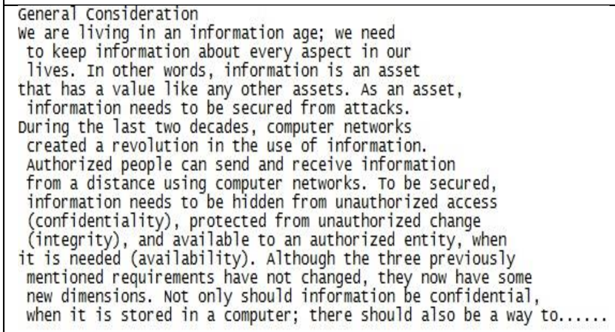
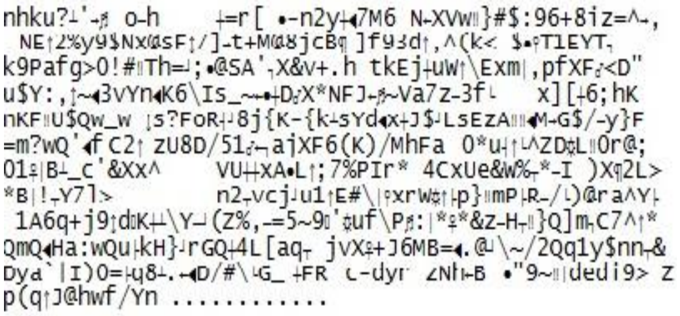
$$C(i) = \{X(i) \oplus Z(i)\} \qquad (4)$$

Steps7: store the result ciphertext C.

3.Encryption result

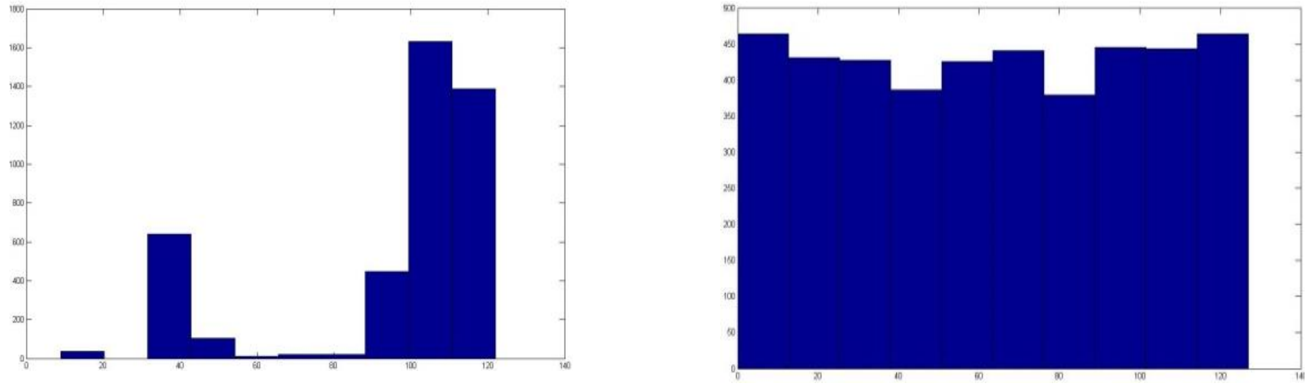
Security is crucial measure of the cipher, the ideal encryption system should be realize mainly three basic characteristics,(1) Simplicity moving the plaintext to incomprehensible ciphertext,(2) Canceled any statistical similarities between the plaintext and ciphertext, (3) High sensitivity, where any slight change in key or plaintext lead to completely different ciphertext [11], and to ensure robustness for cipher, many standard metrics done for different text file size and Table.1 show plaintext and corresponding ciphertext for file type .txt plaintext include 5120 characters.

Table(1): plaintext and corresponding ciphertext .

<table>
<tr><th>Plaintext</th><th>ciphertext</th></tr>
<tr><td>General Consideration
We are living in an information age; we need
to keep information about every aspect in our
lives. In other words, information is an asset
that has a value like any other assets. As an asset,
information needs to be secured from attacks.
During the last two decades, computer networks
created a revolution in the use of information.
Authorized people can send and receive information
from a distance using computer networks. To be secured,
information needs to be hidden from unauthorized access
(confidentiality), protected from unauthorized change
(integrity), and available to an authorized entity, when
it is needed (availability). Although the three previously
mentioned requirements have not changed, they now have some
new dimensions. Not only should information be confidential,
when it is stored in a computer; there should also be a way to......</td><td>nhku?┴'→♬ o-h ┼=r[•-n2y┼◄7M6 N←XVw‼}#$:96+8iz=^→,
NE↑Z%y9$Nx@sF↕/]-t+M@8jcB¶]f93d↑,^(k< $•♀T1EYT┐
k9Pafg>0!#‼Th=┘;•@SA'┐X&v+.h tkEj┼uW↑\Exm|,pfXF♂<D"
u$Y:,↕~◄3vYn◄K6\Is_~→•┼D♂X*NFJ→♬~Va7z-3f└ x][┼6;hK
nKF‼U$Qw_w ↓s?FoR┼┘8j{K-{k┴sYd◄x┼J$┘LsEzA‼‼◄M→G$/-y}F
=m?wQ'◄f C2↑ zU8D/51♂←┐ajXF6(K)/MhFa 0*u┤↑└^ZD☼L‼0r@;
01♀|B┴_c'&Xx^ VU╫XA•L↑;7%PIr* 4CxUe&w%┬*-I)X¶2L>
*B|!┬Y7l> n2┬vcj┘u1↑E#\|♀xrW☼↑├p}‼mP├R-/└)@ra^Y├
1A6q+j9↕d▯K╨\Y┘(Z%,-=5~9▯'☼uf\P♬:|*♀*&z-H┬‼}Q]m┐C7^↑*
QmQ◄Ha:wQu├kH}┘rGQ╫4L[aq┬ jvX♀+J6MB=◄.@┘\~/2Qq1y$nn┬&
Dya`|I)0=├q8┴.←◄D/#\└G_ ┼FR ∟-dyr ∠Nh├B •"9~‼|dedi9> Z
p(q↑J@hwf/Yn ....</td></tr>
</table>

3.1 Histogram Analysis

The statistical relationship between the plaintext and ciphertext should be break to avoid extract meaningful information about the nature of plaintext, the ideal histogram for ciphertext should be uniform or flat distributed, the Figure 2(a) shows the ASCII code distribution for file type .txt plaintext include 5120 characters, and corresponding ciphertext in Figure2(b), it is clearly show no statistical similarities with plaintext and algorithm can thwart the know plaintext attack[6].



(a) (b)

Figure2 : (a)ASCII codes distribution for plaintext,(b) ASCII codes distribution for ciphertext.

3.2 Key Sensitivity Analysis

The another aspect of good cryptosystem is sensitivity to slight change for encryption and decryption key, the test include slight modify the initial condition (3) for system (2) from 0.8 to 0. 800001, and show the impact of such change to result ciphertext values for same plaintext, Figure3 clearly depicted that the result ciphertext2 (dotted line) is completely different from ciphertext1(green line) and the algorithm behavior extreme sensitive to key change[15].

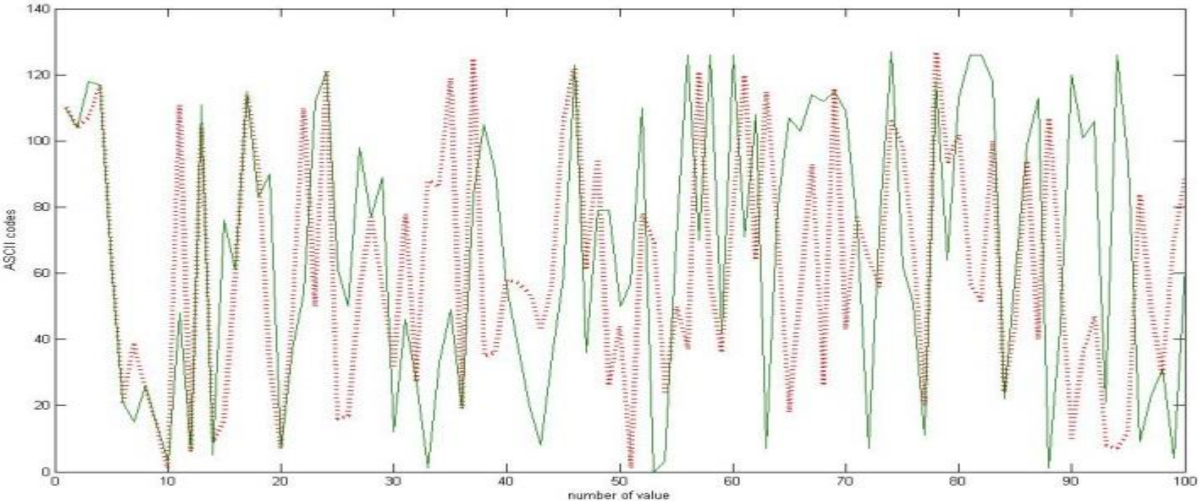


Figure3 : Sensitivity test explore the difference between ASCII values for ciphertext1and ciphertext2 with same plaintext and little change in encryption key.

3.3 Correlation Coefficient Analysis

Correlation is a measure of level of similarities between two ASCII values, the correlation value lies between -1 and +1, to demonstrate the encryption quality and avoid any statistical attacks the strong correlation should be cancelled and ideal value for ciphertext close to (0), Table2 listed the result where correlation is reduced and close to (0).[4]

Table(2): Correlation Coefficient for different files.

	plaintext			ciphertext		
File size(Byte)	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
8612	**0.1955**	**0.0058**	**0.0183**	**0.0903**	**0.0027**	**0.0019**
11656	**0.1437**	**0.0028**	**0.0069**	**0.0344**	**0.0089**	**0.0124**
30808	**0.0090**	**0.0020**	**0.00005**	**0.00004**	**0.0033**	**0.0025**

3.4 Time Analysis

This section present important factor to measure the efficiency of the proposed algorithm, the proposed method realized by Matlab 2013b on 2.16GHz Intel CPU with 4.00 GB RAM in Windows 7 ultimate, the Table 3 show the execution time for different file size and ensure that the method is appropriate for real time application.

Table(3): show encryption time for different file size.

Original File size (bytes)		**Encryption time(sec)**	
Proposed method	**Ref (12)**	**Proposed method**	**Ref (12)**
4306	**3136**	**0.007278**	**1.015959**
5828	**3600**	**0.009640**	**1.201256**
8669	**4096**	**0.014433**	**1.506528**
10226	**4624**	**0.016912**	**1.568922**
15404	**5184**	**0.025150**	**1.770240**

4.Conclusion

In this paper, simple and fast text encryption method is introduced based on two hyper-chaotic systems, the first system utilized to position scramble of plaintext will the second system used to value change of the plaintext, the encryption process is very simple and overcome the drawbacks and disadvantages of traditional encryption method that include complexity of design, computational overhead and longtime for execution, and the results show that the cipher text have more ability to resist statistical attacks and the encryption process within real time.

References

[1] Akif Akgul, Sezgin Kacar, Burak Aricioglu, Ihsan Pehlivan, Text Encryption by Using One-Dimensional Chaos Generators and Nonlinear Equations, Conference Paper · November 2013.

[2] Ghada Salim Mohamed, Text Encryption Algorithm Based on Chaotic Neural Network and Random Key Generator, Ibn Al-Haitham journal for pure and application science, vol 29, No 3, 2016.

[3] Jafar Biazar, Tahereh Houlari and Roxana Asayesh,”Implementation of multi-step differential transformation method for hyperchaotic Rossler system”, International Journal of Applied Mathematical Research, Vol 6 No 1, 2017.

[4] Jean De Dieu NKapkop, Joseph Yves Effa, Jean Sire Armand Eyebe Fouda, Mohamadou Alidou, Laurent Bitjok and Monica Borda, A Fast Image Encryption Algorithm Based on Chaotic Maps and the Linear Diophantine Equation, Computer Science and Applications, Volume-1, Number-4, 2014.

[5] J. Vahidi, M. Gorji,” The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos”, Journal of mathematics and computer Science,Vol 9 , (2014),p 451 – 457.

[6] Kamlesh Gupta, Ranu Gupta, Rohit Agrawal and Saba Khan, An Ethical Approach of Block Based Image Encryption Using Chaotic Map, International Journal of Security and Its Applications, Vol-9, N-9, 2015.

[7] Murtala, Kabir and Adeniyi, Abidemi, Message Encryption and Decryption on Mobile Phones, Journal of Research and Development Studies Vol 5,No 1 June 2017.

[8] MYT Irsan and SC Antoro, Text Encryption Algorithm based on Chaotic Map, The 3rd International Conference On Science,2019.

[9] Nashwan A.Al-Romema,Abdulfatah S.Mashat, Ibrahim Albidewi,” New Chaos-Based Image Encryption Scheme for RGB Components of Color Image”, Computer Science and Engineering Volume-2,Number-5,2012.

[10] Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalini Stalin and Sanjay Kumar, Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing, Entropy 2015.

[11] Sheela S.J, Suresh K.V ,Secured Text Communication Using Chaotic Maps, International Conference on Algorithms, 2017.

[12] Sourabh Chandra, Bidisha Mandal, SK. Safikul Alam, and Siddhartha Bhattacharyya, Content based double encryption algorithm using symmetric key cryptography, International Conference on Recent Trends in Computing (ICRTC 2015).

[13] Sundarapandian Vaidyanathan,”Hyperchaos, adaptive control and synchronization of a novel 4-D hyperchaotic system with two quadratic nonlinerities”, Archives of Control Sciences, Volume-26,Number-4,2016.

[14] Viet-Thanh Pham, Christos Volos, Sajad Jafari and Xiong Wang, Generating a novel hyperchaotic system out of equilibrium, Vol. 8, No. 5-6, May - June 2014.

[15] Zhi-Liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation, Information Sciences, Volume-181, 2011.