A New IOT Image Encryption Algorithm based on Chaotic Map

Aqeel Mohsin Hamad
Computer Department, College of Computer and Mathematics, University of Thiqar, Thiqar, Iraq.
E-mail: aqeelhamad@utq.edu.iq

Naofal Mohamad Hassein
Computer Department, College of Computer and Mathematics, University of Thiqar, Thiqar, Iraq.
E-mail: nawofel_aziz@utq.edu

Received April 07, 2021; Accepted August 02, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I2/WEB18338

Abstract

IOT information is always subjected to attacks, because component of the IOT system always unsupervised for most of time, also due to simplicity of wireless communication media, so there is high chance for attack, lastly, IOT is constraint device in terms of energy and computation complexity. So, different research and study are proposed to provide cryptographic algorithm. In this paper, a new image encryption is proposed based on anew chaotic map used to generate the binary key. The proposed map is three dimensional map, which is more sensitive to initial condition, each dimension of the 3-D chaotic map is depended on the others dimension, which may increase the randomness of the behavior trajectory for the next values and this gives the algorithm the ability to resist any attacks. At first, 3-D chaotic map is proposed, which is very sensitive for initial condition, the three dimension is depended on each other, which make the system more randomness, then the produced sequences is converted on binary key by using mod operation. The original image is scrambled based on mod operation to exchange the row and interleaving them, the same operations are repeated for column of the image. Later, the image is divided into blocks of size (8*8) and scrambled by using negative diagonal scan, the final pixels are converted into binary sequences, which are XORed with the generated key to produce the encrypted image. The experiment is performed on different images with different properties and tested with different metrics such as entropy, correlation, key sensitivity, number of pixel change rate (NPCR) and histogram of the original and encrypted images. T results shows that the proposed encryption algorithm is more efficient and outperform other methods.

Keywords

IOT, Chaotic, Entropy, NPCR and UACI.

Introduction

The internet of thing (IOT) is a model that includes communicated devices, which are used to sense and communicate and transmit the collected information from remote device by using internet, these device can provide huge data, which very important, therefore, sharing such information must be securely transmitted through the internet especially in some application, which require more information confidentiality, so to adapt this technology, it is important to increase confidence for IOT application by terms of security and privacy (Xie F. and Chen Hu. (2016)). Unfortunately, IOT information is always is subjected to attacks, because firstly, the component of the IOT system are always unsupervised for most of time, also due to the simplicity of wireless communication media, so there is high chance for attack, lastly, the IOT is constraint device in terms of energy and computation complexity. (Ban H.et al. (2016), Khan S.et al. (2015), Wang J. et al. (2007), Muhammad U. et al. (2017)).

The literature review show that there are difficult shortcoming for IOT in terms of limited resource of IOT devices (Ebrahim M., Khan S, and Khalid B. (2014)). Present comparative study for different symmetric algorithms base on different metrics such as flexibility, scalability and architecture, and he address the limitation of communication security. In (D Engels D et al. (2011)) proposed encryption algorithm by using 128 key with 64 bit as initialization, the algorithm is software and implemented by hard ware. In (Muhammad U. et al. (2017)) proposed lightweight algorithm named as (SIT), in this algorithm, 64 bit key is used, also it is constructed from mixture of fastened with uniform substantial permutation. In (Khan Muhammad et al. (2018).) proposed secure surveillance monitoring for IOT based on logistic chaotic system, in this algorithm, the author is used two dimensional chaotic sequence based on sin wave function, which is used as key to encrypt the IOT image. In (Ganesan P. et al. (2003)) present comparative study by means of entropy consumption for different encryption algorithm such as RC4, RC5 and IDEA. (B. Schneier. (2007); Ganesan P. et al. (2003); Xuejial L. (1992)), also they compare between computation complexity for different algorithms. (Zhijuan Deng and Shaojan Zhong (2019)) proposed image encryption algorithm based on chaotic system, he used the basic features for the image as parameters for used chaotic map (which is designed by (Xiong et al.). (Bhagya Maybel J and A. Umamakeswari, (2018)) proposed systematic algorithm to transmit image to web server by using Raspberry pi, the algorithm is depended on scrambling pixels and using chaotic map, and it is implemented by hardware by using raspberry pi3. (Mohammed Karim et al. (2017)) in this paper, we have proposed anew cryptographic image algorithm based on anew chaotic map. We have proposed three dimensional chaotic system, the encryption key is generated based on the proposed map system, which produce chaotic sequence, this sequence will be used to generate the binary key after amplified and normalized it, then it is used to encrypt the image, which is also under go different stages of processing such as row interleaving by rearrange it according specific technique, the same method is used to interleave the column of the image, later, it is divided into (8*8) blocks, scrambled and scanned in negative diagonal method,then converted to binary sequence and XORed with the generated key to produce the ciphered image.

Chiotic Map

The chaotic sequence is anon linear dynamical sequence, the generation of this sequence is depended on initial conditions. There are different types of chaotic system such as logistic map, Lorenz map, Rossler map and Bernoulli map (Hua X et al (2013); Joan D., René G. and René G. (1993); Lingfeng Lu. et al. (2014)). Dynamical sequence means that, the system changes its condition at each iteration, chaotic map is nonlinear system that contains some interacting variables depending on simple rules, which is very sensitive to initial conditions of its variables and parameters (Abir A et al. (2008)), the most common type of chaotic map is logistic map, which is represented by equation (1), which is very well known in theory of dynamics nonlinear system and it is defined by equation(1):

$$X_{n+1} = f_m(X_n) = \mu\, X_n(1 - X_n) \qquad (1)$$

Where $X_n \epsilon$ [0,1] and n is integer number and μ =3.999.

Depending on the value of μ, the system is doubled in period as μ is increased, and the bifuriction diagram can be used to show the period doubling, which is produced based on increasing the value of μ as shown in Figure 1.

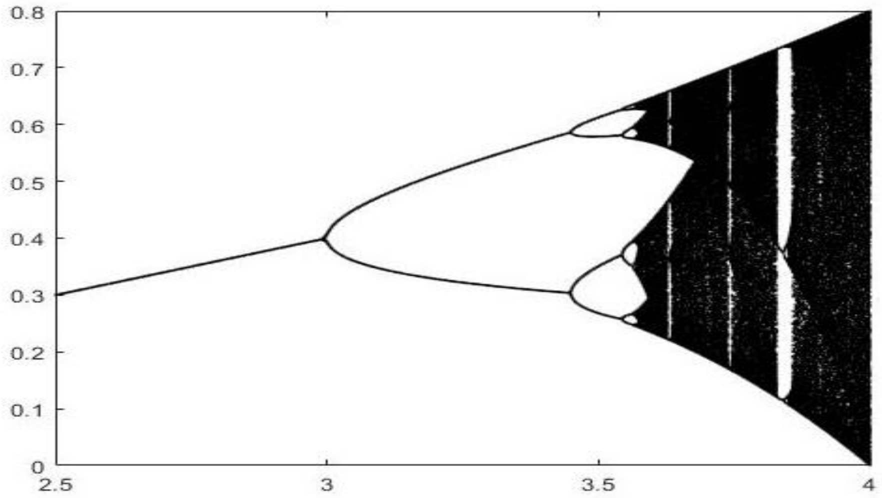


Figure 1 Bifurcation diagram for logistic map

Also, chaotic and system can be characterized by contrast depending on their sensitivity to their initial conditions if there is changes, as it is more sensitive to small changes in their initial condition as it is more chaotic system. Quality called LE is introduced by alexander lyapunov, this quality represent how fast the chaotic system is different depending on the initial condition by (ε) so, $f(X_0) =$ will be $f(X_0 + \varepsilon_0)$, and after (n+1) iterative states, then $f(X_0)$ will be changed to be written as $f(X_n + \varepsilon_n)$ and then, the variation from state (X_0) to state (X_n) will be written in equation (2):

$$\ln\left|\frac{\varepsilon_n}{\varepsilon_0}\right| = \ln\left|\frac{\varepsilon_n}{\varepsilon_{n-1}}\right|.\ln\left|\frac{\varepsilon_{n-1}}{\varepsilon_{n-2}}\right| \dots\dots..\sum_{i=1}^{n}\left|\frac{\varepsilon_1}{\varepsilon_0}\right| \quad (2)$$

Where:

$$\left|\frac{\varepsilon_i}{\varepsilon_{i-1}}\right| = \left|\frac{f(X_{i-1}+\varepsilon_{i-1}}{\varepsilon_{i-1}}\right| \xrightarrow[\varepsilon_{\iota-1}]{} \left|\bar{f}(X_{i-1})\right| \quad (3)$$

While lyapunov exponent map $X_{n+1} = f_m(X_n)$ is in equation (4).

$$\Lambda_L(x) = \lim_{n\longrightarrow\infty} \frac{1}{n}\sum_{i=1}^{n} ln\left|\bar{f}(X_{i-1})\right| \quad (4)$$

Figure 2 shows the lyapunov exponent for μ value between (3,4), as shown in Figure 2 (Mohammed Karim, et al. (2018); Adedeji K. and Ponnle A. (2017); Stephen L. (2004)).

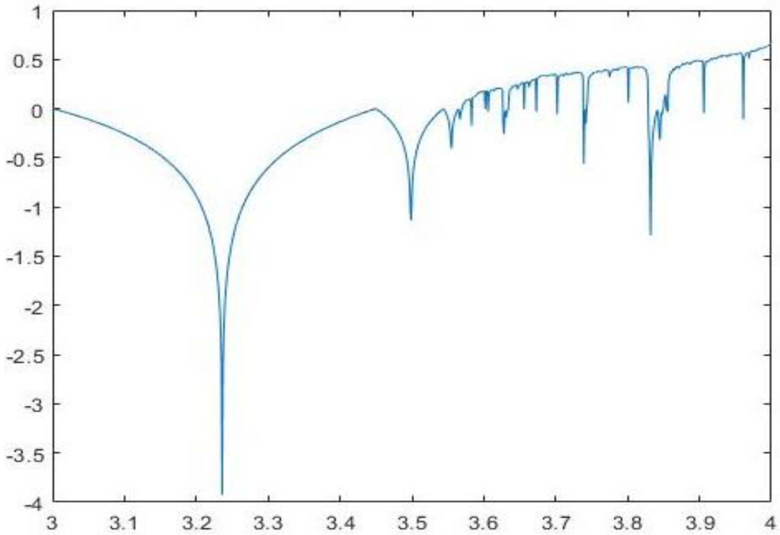


Figure 2 lyapunov exponent of logistic map

Proposed Methodology

In this paper, we have proposed a new IOT image encryption algorithm based on dynamic chaotic system, which is used to generate key that is used in image encryption.

Proposed Chiotic Map

We have proposed 3-dimensional chaotic map system based on the logistic map and it is described in equations (5, 6 and 7).

$$X_{n+1} = \mu\, X_n - cX_n{}^2 \quad (5)$$

$$Y_{n+1} = \mu X_n - Y_n{}^3 \quad (6)$$

$$Z_{n+1} = Y_n - k\, X_n{}^2 \quad (7)$$

As described in the equations above, the values of X_n, Y_n and Z_n are depends on each other, Z_n is depended on Y_n, which is also depended on $X_n$and Y_n, and this is the main strengths of the proposed chaotic map, because it increase the randomness of the generated sequence and increase the chaotic behavior, this make the sequence is very difficult to be discovered.

The bifurcation diagram of the proposed chaotic map is shown in Figure 3, it is clear that, the value of ($\mu = 3$) gives 2 and $\mu = 3.4$ gives 4, while $\mu = 4$ make the number of the sequences are undefined. Also the relation between three dimension of the proposed dynamical system are shown in Figure 4, which are describe the behavior of the sequences with n=1000 between different dimension of the proposed system (X, Y and Z), which prove the chaotic property of the system, as shown in figure the proposed chaotic system achieved high randomness between the different dimension (Xn, Yn and Zn).

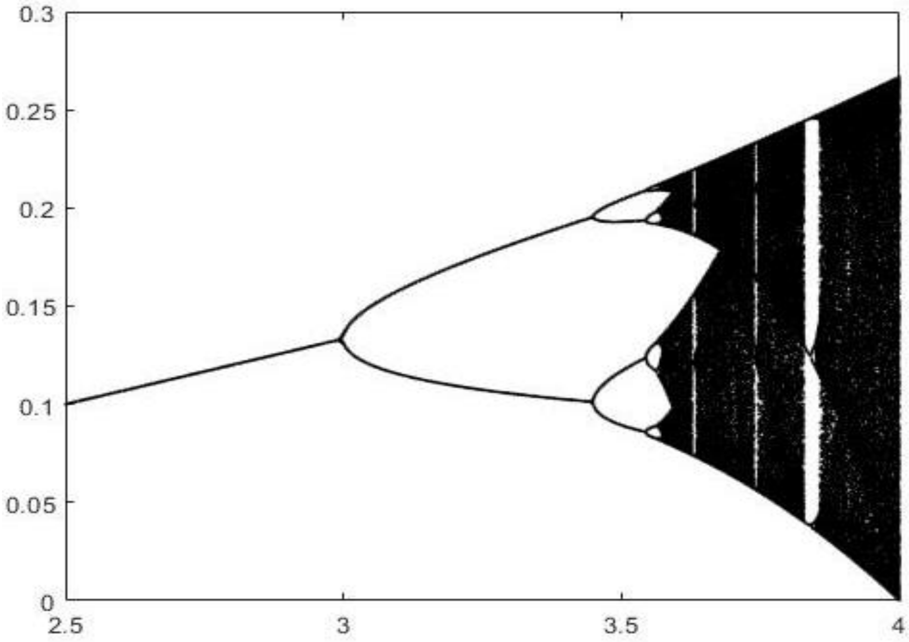


Figure 3 Bifurcation diagram of the proposed chaotic map

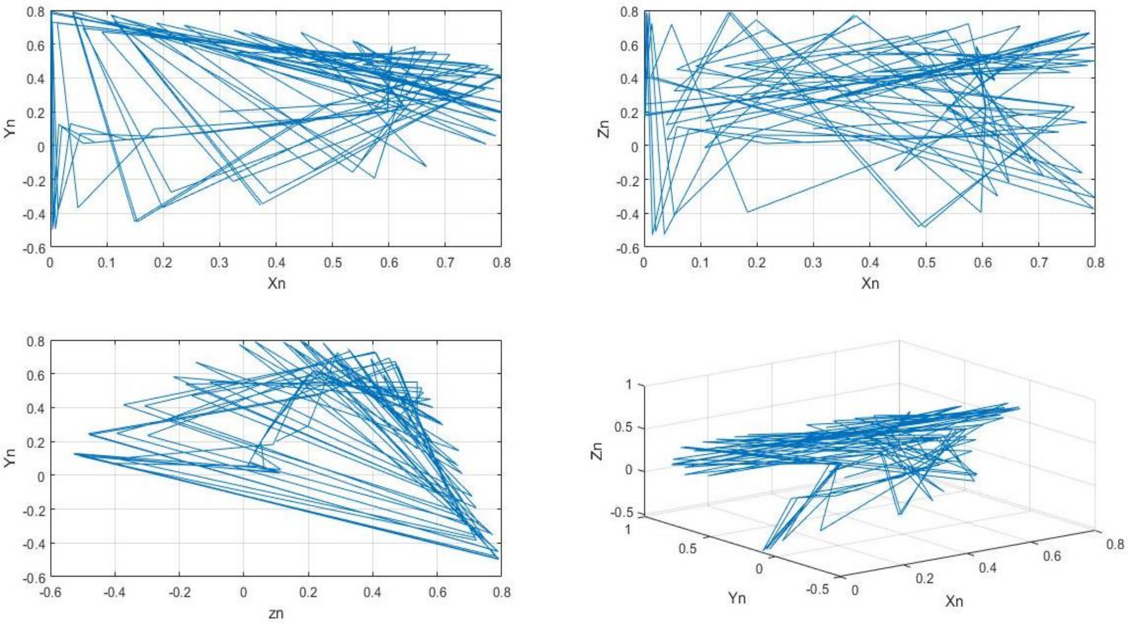


Figure 4 Relation between three dimensional proposed chaotic map

Proposed Encryption Algorithm

Figure 5 shows the block diagram of the proposed encryption algorithm, the proposed algorithm is constructed from three basic blocks, in the first block, the image is interleaved according to the row and column of pixels while second block represent scan the pixels of each block in the image, while the third block is used to diffuse the key with the original image, the encryption procedure can be summarized by the following steps:

Step 1 Apply row by row exchange by replace first, second, third and fourth by third, one, four and two respectively.
Step 2 Repeat the row interleaving step for column pixels in the same method.
Step 3 Divide the image into 8*8 blocks and interleave their pixel by using the following equation (8) for row and column.

$$\text{new location} = (k \ mod \ 8 + 1) \qquad (8)$$

Where K is row/column number.

Step 4 Scan the block elements in diagonal negative scan manner.
Step 5 Generate the image key by using the proposed chaotic map and convert the sequence into binary by using binary bit generation by applying the following equations:

$$X_n = X_n + \min(X_n) \qquad (9)$$

$$X_n = rounn(X_n, -2) \qquad (10)$$

$$\text{GKey} = mod(X_n * 100, 2) \qquad (11)$$

Where eq.9 is used to shift the sequence to be in [0 1] range, eq.10 is used to rounded the sequence, while eq.11 is used to generate the binary key (Gkey).

Step 6 The result of the block scan are XORed with the binary key, which is produced from step 5 to be transmitted.

While the basic steps of description, which are invers procedure of encryption method are listed below:

Step 1 Generate the chaotic sequence key by using the proposed chaotic map and apply binary generator on chaotic sequence to reconstruct the key.

Step 2 The scrambled blocks are retrieved by perform XOR the encrypted image with binary key.

Step 3 Inverse the negative scan elements for each 8*8 block of the image.

Step 4 De-interleaved the 8*8 block by using:

New row/col=(K mod 8)+1

Step 5 Apply column by column exchange by replace first, second, third and fourth by third, one, four and two respectively.

Step 6 Apply column by column exchange by replace first, second, third and fourth by third, one, four and two respectively.

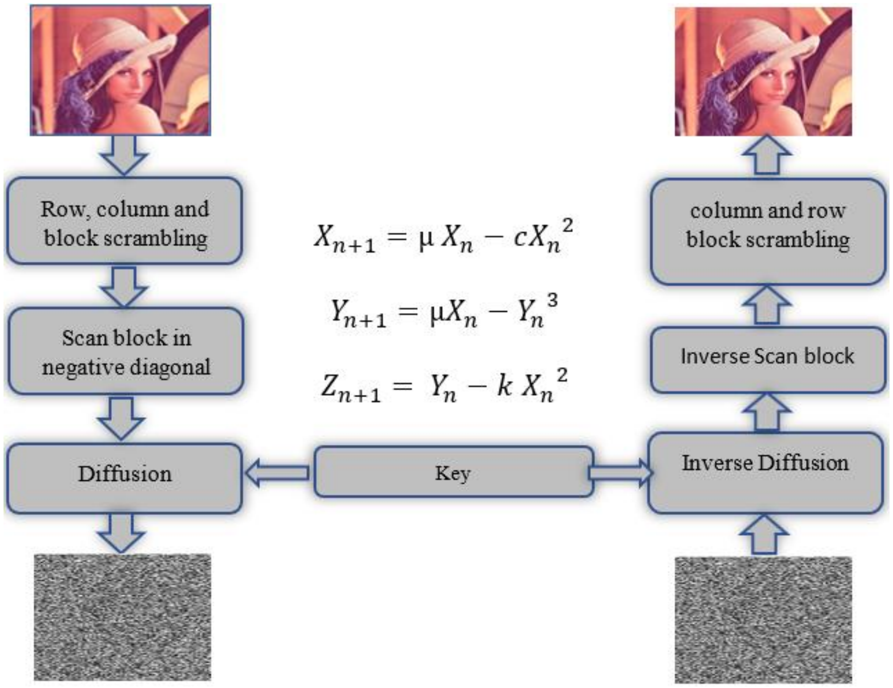

Row, column and block scrambling
Scan block in negative diagonal
Diffusion
Key
$X_{n+1} = \mu X_n - cX_n{}^2$
$Y_{n+1} = \mu X_n - Y_n{}^3$
$Z_{n+1} = Y_n - k X_n{}^2$
column and row block scrambling
Inverse Scan block
Inverse Diffusion

Figure 5 Block diagram of the proposed algorithm

Evaluation Metrics

To evaluate the performance of the proposed encryption algorithm, it is evaluated based on basic criteria such as image correlation, image histogram, image entropy, mean square error and peak signal to noise ratio, these metrics are described as following:

Correlation

This metric depict the depending between one value to another, we calculate the correlation coefficients by using equation (12):

$$\text{corr.} = \left(\frac{\text{cov(x,y)}}{\sqrt{D(x)}\sqrt{D(y)}}\right) \qquad (12)$$

Where $D(x)$ and $D(y)$ are variance for x and y respectively, while $\text{cov}(\text{x}, \text{y})$ is covariance and it is evaluated by equation (13):

$$\text{D(x)} = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (13)$$

Where $E(x) and\ E(y)$ are mean values of x and y respectively and they are computed by equation (14):

$$\text{E(x)} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (14)$$

Where x_i and N is the total number of elements. As the correlation is decreased as the encryption is better (Muhammad U. et al. (2017); Khan Muhammad et al. (2018)).

Image Entropy

Encryption algorithm can result in increasing the information in the encrypted image in order to make the original data difficult to introducer to distinguish between original and encrypted, also the added information, so higher the entropy, better algorithm efficiency, the entropy is measured by equation (15):

$$\text{H(I)} = -\sum_{i=1}^{2^8} P_i\ log2\ P_i \qquad (15)$$

Where P_i probability of I intensity level [Muhammad U. et al. (2017)].

Image Histogram

This metric is used to observe the encryption effect on image, image histogram is calculated for original and encrypted images, uniform histogram for encrypted image represent appreciable encryption. (Zhijuan Deng and Shaojan Zhong (2019)).

Key Sensitivity

One of the most important parameters of encryption algorithm is its sensitivity to the key. Algorithm sensitivity to key means that, it can retrieve the original image if there is difference to original key.

NPCR and UACI

This is another type of encryption metric, which number of change pixel rate, sometimes, the attacker need to encrypt the image by using different pixel for the image, so the differences in the encrypted image should be very high for only one pixel change of the original image, in this test, two image is encrypted from the same image with only one pixel change as described in equation (16) and (17): (Zhijuan Deng and Shaojan Zhong (2019)).

$$\mathrm{NPCR}(\mathrm{C1},\mathrm{C2}) = \sum_{i,j} \frac{S(i,j)}{D} \times 100\ \% \qquad (16)$$

$$\mathrm{UACI}(\mathrm{C1},\mathrm{C2}) = \sum_{i,j} \frac{C1(i,j)-C2(i,j)}{255\times D} \times 100\ \% \qquad (17)$$

Where D is pixel number, and S is determined by equation (18)

$$\mathrm{S} = \begin{cases} 0\ if\ C1(i,j) = C2(i,j) \\ \quad 1\ otherwise \end{cases} \qquad (18)$$

Results and Discussion

The proposed algorithm is performed on different test images by using Mat lab 2019b on intel cori7, GHz processor and we compare our algorithm results with other works. Table 1 show the results of different images encrypted with our algorithm and algorithm of (Muhammad U. et al. (2017)), the comparison show that the proposed algorithm give better results, for example for Lena image, it achieved less correlation value (0.0010), this means that, there is high differences between original and encrypted image, while it is satisfied high value for original image (0.9753), this means that, there is no or less information are discarded from the original image though the encryption, the detail description is shown in Table 1.

Table 1 Correlation and entropy for the proposed algorithm

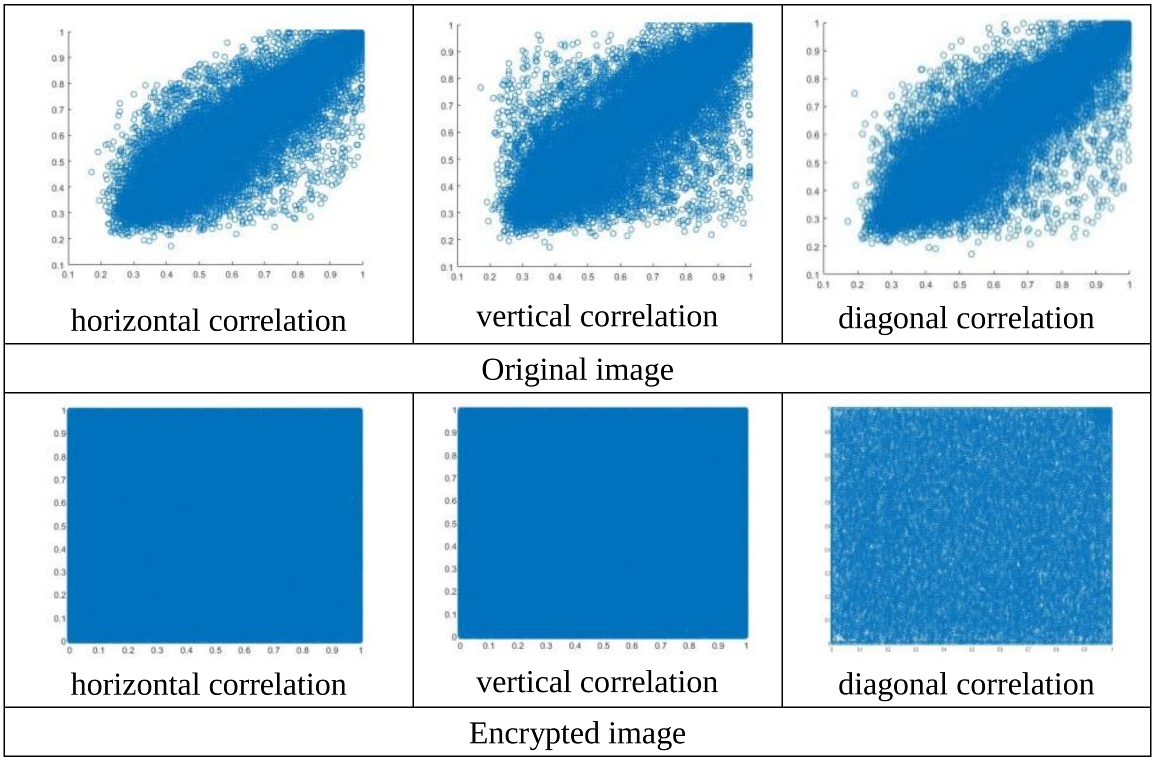
Image	Size	Correlation		Entropy	
		Original	Encrypted	Original	Encrypted
Lena	256 * 256	0.9753	0.001	7.4528	7.9974
Baboon	256 * 256	0.8968	0.001	7.2316	7.9973
Cameraman	256 * 256	0.9623	0.0011	7.0097	7.9975
Panda	256 * 256	0.9914	0.0023	7.4938	7.9973

The correlation comparison between original and encrypted image are shown in Figure 6, which is described high correlation in original image by concentrate the coefficients in very close manner in each to other, while the coefficients of the encrypted image are spreader out in all figure. The details of the comparison are shown in Table 2, it is clear that our algorithm achieved less correlation for encrypted image (for Lena image), which means, there are high differences between encrypted and original image, in other word there are good results for encryption results, also for all test images, the correlation with original image are always greater than (Muhammad U. et al. (2017)), which means that there is very small change between the decrypted and original image, because no eliminated information due to encryption method.

Table 2 Correlation and entropy for the proposed algorithm and results of (Muhammad U. et al. (2017))

Image	Size	Correlation		Entropy	
		Muhammad U. et al. (2017)	Proposed	Muhammad U. et al. (2017)	Proposed
Lena	256 * 256	0.0012	0.001	7.9973	7.9974
Baboon	256 * 256	0.0023	0.001	7.9972	7.9973
Cameraman	256 * 256	0.0011	0.0011	7.9973	7.9975
Panda	256 * 256	0.0022	0.0023	7.9971	7.9973

Also in term of entropy, it is clear that the proposed method achieved high entropy as shown in Table (2), which describe the added information and the high amount of the observed randomness in the encrypted image. The distribution between adjacent pixels (horizontal, vertical and diagonal) are shown in figure (6) for original and encrypted image, there are high distribution for encrypted image as compared with original image, which describes that there are high correlation between the coefficients of original image, while the encrypted image does not have any correlation giving strength to our algorithm.



horizontal correlation | vertical correlation | diagonal correlation

Original image

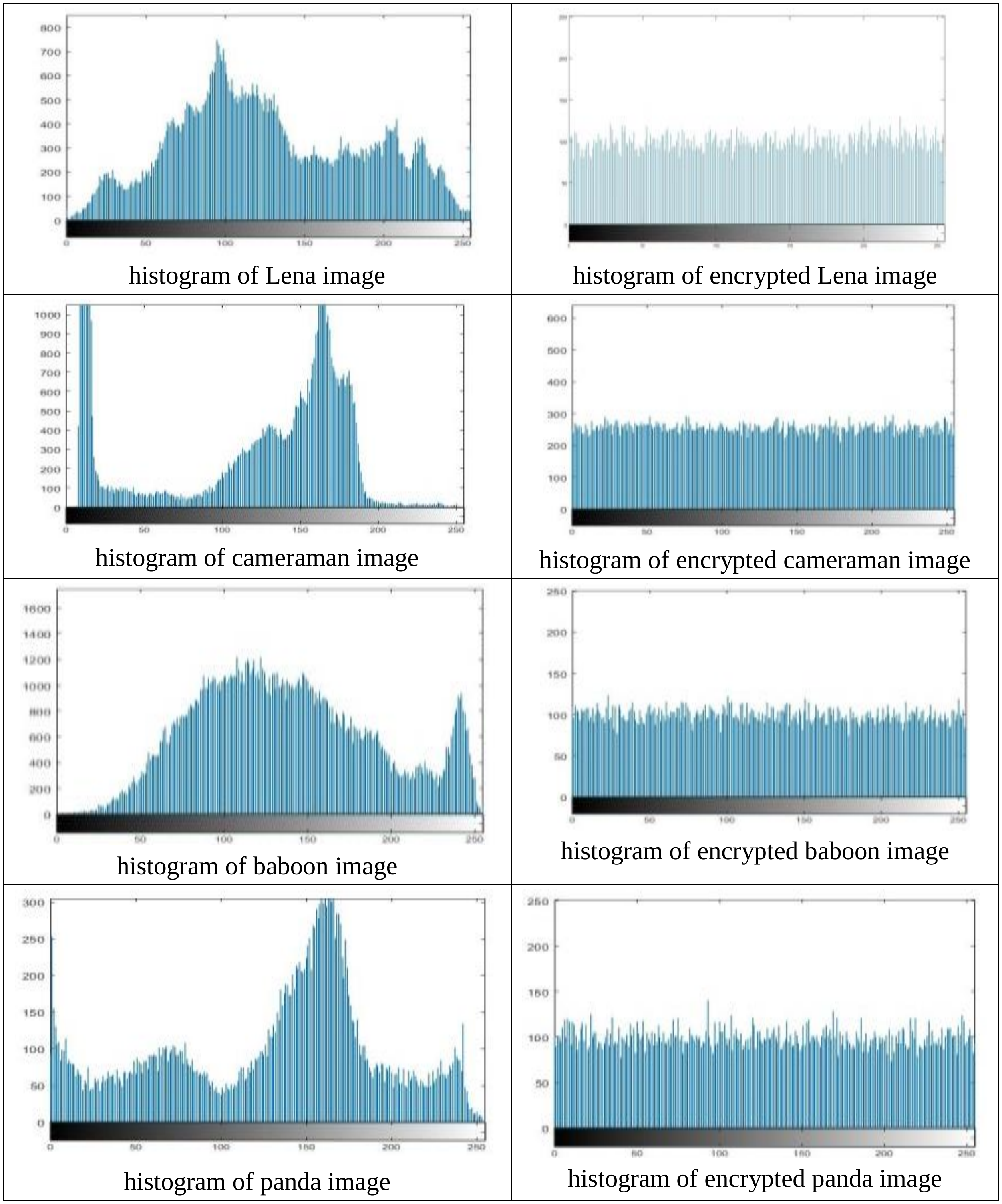
horizontal correlation | vertical correlation | diagonal correlation

Encrypted image

Figure 6 Distribution of adjacent pixels in original and encrypted image for horizontal, vertical and diagonal direction for Lena image

Also the results of histogram of test images are shown in Figure 7, the strength of our algorithm is shown from the uniform distribution of histogram of the encrypted image for all test images, while the original images as shown in the left part of Figure 7 have different distribution of pixels intensity. Table (3) show (NCPR) and (UACI) for proposed algorithm for different tests ciphered images, it is provided that, the algorithm have the ability to resist different attacks for ciphered image, we generate two ciphered images with change only one pixel from the original image, and from the results, we investigated that, the algorithm have the ability to avoid differential attacks depending on probabilistic encryption property. Our algorithm produce completely different two image, this means that it demonstrates completely secure different image for the next ciphered image, and the attacker cannot discover any information about the original image from the ciphered image. The comparison in terms of (NCPR) and (UACI) for proposed algorithm with other works is described in Table 4.

To test our algorithm for key sensitivity, we decrypt the tests image with small change for initial condition x0=0.30000000001 instead of x0=0.3, The results are shown in figure (8), which describes the original, encrypted, decrypted image with correct key and decrypted image with wrong key, it is clear that, the original image will be remain non recognizable even when the change in the encryption parameters are very simple, and this explains the power of the proposed algorithm.



histogram of Lena image

histogram of encrypted Lena image

histogram of cameraman image

histogram of encrypted cameraman image

histogram of baboon image

histogram of encrypted baboon image

histogram of panda image

histogram of encrypted panda image

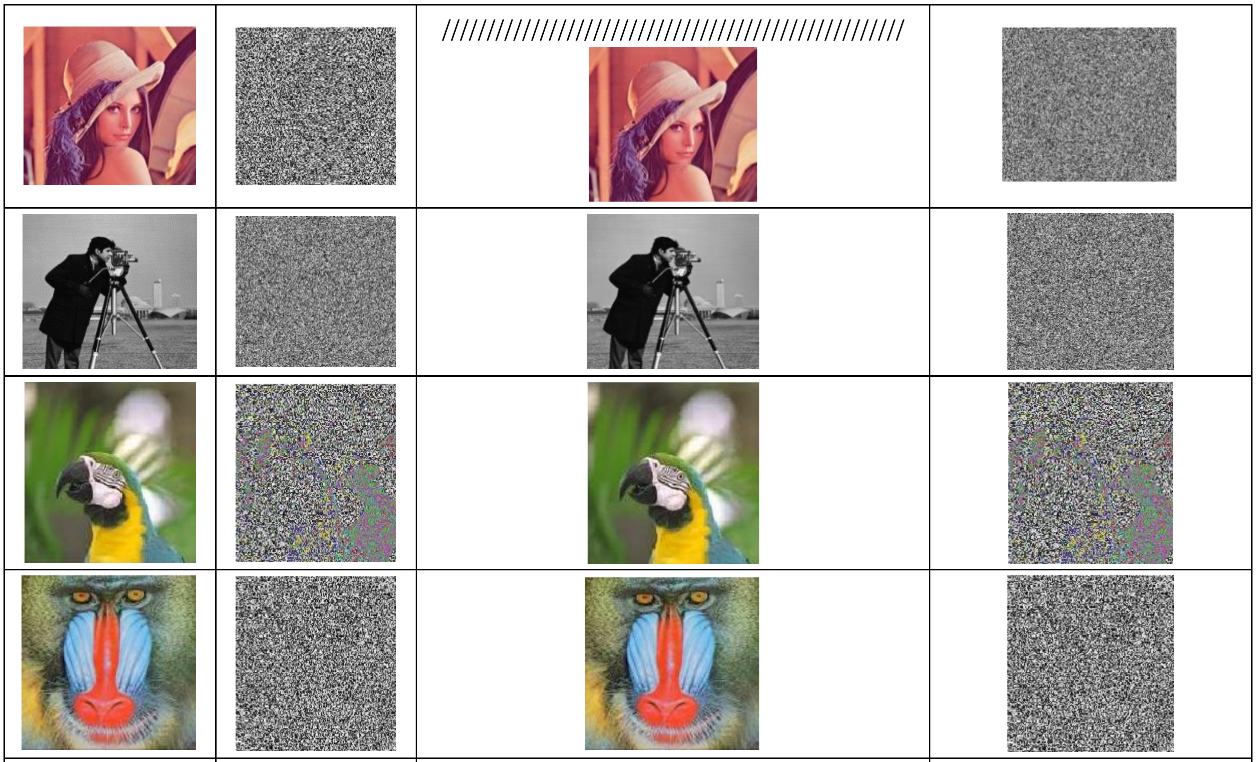
Figure 7 Histogram of original and ciphered image

Table 3 (NCPR) and (UACI) for different images

Image	**Size image**	**NPCR**	**UACI**
Lena	256 * 256	0.996093	0.3346
cameraman	256 * 256	0.99638	0.3346
Parrot	256 * 256	0.99550	0.3346
Baboon	256 * 256	0.9948	0.3347

Table 4 Comparison with other works

Metric	**Proposed**	**Khan M. et al. (2018)**	**Belazi A. et al. (2016)**	**Wei X. et al. (2012)**	**Zhou S. et al. (2016)**	**Zhou Y. et al. (2012)**
NPCR	99.6182	99.6125	99.2172	99.6177	99.60	99.6098
UACI	33.4457	33.4451	33.6694	33.4058	33.40	33.4384



a) Original image	b) encrypted image	c) decrypted image with x0=0.3	d) decrypted image with x0=0.30000000001

Figure 8 Original image, encrypted image, decrypted image with correct key and decrypted image with small change

Conclusions

IOT information is always subjected to attacks, because firstly, the component of the IOT system are always unsupervised for most of time, also due to the simplicity of wireless communication media, so there is high chance for attack, lastly, the IOT is constraint device in terms of energy and computation complexity. So different research and study are proposed to provide cryptographic algorithm. In this paper, anew image encryption is proposed based on anew proposed chaotic map, which is used to generate the binary key. The proposed map is three dimensional map, which is more sensitive to initial condition of its parameters, each dimension of the 3-D chaotic map are depended on the others dimension, which may increase the randomness of the behavior trajectory for the next values and this give the algorithm the ability to resist any attacks. At first we have proposed 3-D chaotic map, which is very sensitive for initial condition and the three dimension is depended on each other, which make the system more randomness, then the produced sequences is converted on binary key by using mod operation, then the original image is scrambled first by using specific form based on mod operation to exchange the row and interleaving them, the same operations are repeated for column of the image, later, the image is divided into blocks of size (8*8) and scrambled by using negative diagonal scan, the final pixels are converted into binary sequences, which are XORed with the generated key to produce the encrypted image.

The experiment is performed on different images with different properties and tested with different metrics such as entropy, correlation, key sensitivity, number of pixel change rate (NPCR) and histogram of the original and encrypted images, the result shows that the proposed algorithm is very sensitive to initial condition, since it gives very good result and it is encrypted the image for less change value (0.000000001) as initial condition, also it achieved (NPCR=0.996 for Lena image) with correlation (0.001) which is less than in (Muhammad U. et al. (2017)) (0.0011), also it is achieved better the entropy value (7.9974) verses (7.45) for (Muhammad U. et al.(2017)) method, so the proposed algorithm is efficient for secure transmission of IOT image.

References

Xie, F., & Chen, H. (2016). An efficient and robust data integrity verification algorithm based on context sensitive. *International Journal of Security and Its Applications, 10*(4), 33-40.

Ban, H. J., Choi, J., & Kang, N. (2016). Fine-grained support of security services for resource constrained internet of things. *International Journal of Distributed Sensor Networks, 12*(5).

Khan, S., Ebrahim, M., & Khan, K.A. (2015). Performance evaluation of secure force symmetric key algorithm. *Conference: International Multi-Topic Conference (IMTIC),* 11-13.

Wang, J., Yang, G., Sun, Y., & Chen, S. (2007). Sybil attack detection based on RSSI for wireless sensor network. *In 2007 International Conference on Wireless Communications, Networking and Mobile Computing,* 2684-2687.

Usman, M., Ahmed, I., Aslam, M.I., Khan, S., & Shah, U.A. (2017). SIT: A Lightweight encryption algorithm for secure internet of things. *International Journal of Advanced Computer Science and Applications (IJACSA), 8*(1).

Ebrahim M., Khan, S., & Khalid, B. (2014). Symmetric algorithm survey: A comparative analysis. *International Journal of Computer Applications*, *61*(20), 12-19.

Engels, D., Saarinen, M.J.O., Schweitzer, P., & Smith, E.M. (2011). The Hummingbird-2 lightweight authenticated encryption algorithm. *In International Workshop on Radio Frequency Identification: Security and Privacy Issues*, 19-31.

Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H., & Baik, S.W. (2018). Secure surveillance framework for IoT systems using probabilistic image encryption. *IEEE Transactions on Industrial Informatics, 14*(8), 3679-3689.

Ganesan, P., Venugopalan, R., Peddabachagari, P., Dean, A., Mueller, F., & Sichitiu, M. (2003). Analyzing and modeling encryption overhead for sensor network nodes. *In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, 151-159.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C",* 2nd edition, John Wiley & Sons.

Xuejial, L. (1992). On the Design and Security of Block ciphers. *Ph.D. Dissertation, H. B¨uhlmann.*

Deng, Z., & Zhong, S. (2019). A digital image encryption algorithm based on chaotic mapping. *Journal of Algorithms & Computational Technology, 13,* 1-11.

Maybel, J.B., & Umamakeswari, A. (2018). Hard ware implementation of secure image transmition in raspberry. *International Journal of Mechanical Engineering and Technology, 9*(2), 670–678.

Krim, M., Ali Pacha, A., & Hadj Said, N. (2017). New Binary Code Combined with New Chaotic Map and Gold Code to Ameliorate the Quality of the Transmission. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 5*(1), 166-180.

Hua, X., Wang, S., & Meng, X. (2013). Logistic Map Study on One Modified Chaotic System Based. *Research Journal of Applied Sciences, Engineering and Technology, 5*(3), 898-904.

Daemen, J., Govaerts, R., & Vandewalle, J. (1993). A new approach to block cipher design. *In International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg,* 18-32.

Liu, L., Miao, S., Hu, H., & Deng, Y. (2016). Pseudorandom bit generator based on non-stationary logistic maps. *IET Information Security, 10*(2), 87-94.

Abir A., Safwan A., WANG Q. and Bassem B. (2008). Comparative Study of 1-D Chaotic Generators for Digital Data Encryption. *International Journal of Computer Science, 45*(4).

Krim, M., Ali-Pacha, A., & Said, N.H. (2018). The Quality of the New Generator Sequence Improvent to Spread the Color System's Image Transmission. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 16*(1), 402-414.

Adedeji, K.B., & Ponnle, A.A. (2016). Improved image encryption for real-time application over wireless communication networks using hybrid cryptography technique. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 4*(4), 307-318.

Stephen, L. (2004). *Dynamical Systems with Applications using MATLAB.* New York: Springer Science, 48-54.

Belazi, A., Abd El-Latif, A.A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155-170.

Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290-299.

Zhou, S., Wei, Z., Wang, B., Zheng, X., Zhou, C., & Zhang, Q. (2016). Encryption method based on a new secret key algorithm for color images. *AEU-International Journal of Electronics and Communications*, *70*(1), 1-7.

Zhou, Y., Hua, Z., Pun, C.M., & Chen, C.P. (2014). Cascade chaotic system with applications. *IEEE transactions on cybernetics*, *45*(9), 2001-2012.

Fedushko, S. (2014). Development of a software for computer-linguistic verification of socio-demographic profile of web-community member. *Webology*, *11*(2), 1-14.

Biographies of Author

Assist. Prof. Dr. Aqeel M.Hamad. He obtained his BSc. Tech in computer and control engineering from uninversity of technologya, iraq 2003 and M.Sc. from Basrah University/Iraq in 2010 and he is Ph.D. from Al-Nahrin University/Iraq. He is having 10 years of teaching and research experience worked as a head for computer center in ThiQar university for three years. He is presently working as Assistant Professor Dr. in Thiqar university/college of computer and mathematics.