International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

# Design and Implementation of Transformation and Non-Chaotic Substitution Based Image Cryptosystem

**Prajwalasimha S N, Basavaraj L**

***Abstract*: *In this article, a Modified Pseudo Hadamard Transformation (MPHT) and non-Chaotic substitution based image encryption scheme has been proposed. Due to intrinsic properties such as, strong redundancy and correlation between the adjacent pixels, images are more vulnerable to cyber-attacks. In the proposed technique, the redundancy and correlation have been effectively reduced by pixel position transformation using MPHT and pixel value variation using non chaotic substitution, providing two stage security in encryption for secrete images. An average 99.6089% of Number of Pixel Changing Rate (NPCR) and 33.4328% of Unified Average pixel Changing Intensity (UACI) are obtained for a set of standard test images compared to more popular existing techniques.***

***Keywords*: *Redundancy, Correlation, Transformation, Substitution, Encryption.***

## I. INTRODUCTION

Information security is one of the challenging issues nowadays, in the field of multimedia technology. As technology grows, cyber-attacks are more common on communication channels. Images being pictorial representation of information carries bulk data are more vulnerable to cyber-attacks, due to their intrinsic properties. These cyber-attacks cause data corruption or modifications into miss-interpretation of data in a cloud [1-3]. Images are characterized by grid nature and hence encryption is done in different stages. Security attacks are majorly classified as: Analytical, Differential and Brute force attacks [4][5]. Communication channels are more vulnerable to analytical attacks. These channels are continuously monitored by security service providers. Any interruptions in the channels can be quickly traced and information is sent to source and destination regarding the attack. Cryptanalysis is a differential attack in which the cryptographic algorithm is vulnerable [5]. This involves cracking of cryptographic algorithm and decrypting the cipher data. Last resort tactics are also known as brute force attacks [4][6-7]. The secrete key is subjected for all possible combinations and analyzed in the cryptographic algorithm. With the help of all these tactics, the unauthorized third party user tries to hack the information. If an efficient cryptographic algorithm withstands differential attacks, indirectly it resists analytical and brute force attacks [4-8]. Multimedia protection is done through various cryptographic algorithms since 1970s [9].

Image encryption is a process of converting original data into cipher form. Transformation and substitution based algorithms are more effective in the present scenario. Pixel permutation based algorithm has been proposed by Alireza et al. [9] for pixel value variations. S-boxes are used for permutation and pixel positions are unchanged. This provides single stage authentication and hence the correlation between adjacent pixels is not effectively reduced. The immunity against noise is unnoticed. Marwa, et al. [10] proposed an algorithm in which, CAT and Logistic chaotic transformations are used to shuffle pixels and S-function is used to vary the pixel intensity. Encryption is done in two stages. Camellia block ciphering is used in the first stage and chaotic maps are used in the next stage of the algorithm. Number of rounds in the camellia algorithm is reduced from eighteen to two in order to reduce the complexity of the algorithm. The algorithm uses 128 bits of secrete key and the algorithm is very sensitive to secrete key. Even though the algorithm encrypts the information in just two rounds, it takes slight more execution time. A hybrid chaotic mapping based encryption algorithm has been proposed by Hikmat, et al. [11]. The algorithm uses three stages of encryption per round. At the first stage Arnold Cat chaotic map is used to change the pixel positions. Pixel shuffling is done in the second stage using random sequences and in the last stage Hanon and Logistic chaotic maps are used to diffuse the key image. The diffused key image is used for substitution along with the resultant image from the second stage. Security analysis is done for standard images and results are compared with individual chaotic transformation based algorithms. The algorithm utilizes more time for execution due to three different chaotic maps and number of rounds per stage. The algorithm results with less Unified Average Changing Intensity (UACI) value for standard test images and noise immunity is unnoticed. Transposition and substitution based chaotic maps are used for encryption process by Arivazhagan, et al. [12]. Arnold cat map and standard chaotic maps are used in the transposition stage and Logistic and Duffing maps are used in the substitution stage.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
**Prajwalasimha S N***, Department of Electronics & Communication Engineering, ATME Research Centre, Mysuru, India.
**Basavaraj L**, Department of Electronics & Communication Engineering, ATME Research Centre, Mysuru, India.

Results are compared with Elliptic Curve encryption scheme, showing better values but the algorithm utilizes more time for execution due to implementation of different chaotic generates per stage. Two stage Logistic maps are used with two different initial conditions to generated two sets of random sequences and these are used as S-functions in each round. Haifaa, et al. [13] achieved minimum correlation between the original and cipher images by the double logistic mapping method, but the algorithm is inefficient for statistical security analysis. Wavelets are used for encryption process. One such algorithm has been developed by Ramtin, et al. [14].

A modified Pseudo Hadamard transformation (MPHT) is used to shuffle the pixel values and positions along with substitution technique. The degree of randomness is considered to differentiate conventional PHT [4] with a modified one from which better efficiency is achieved compared to more popular techniques and hence withstands differential cyber-attacks. The paper is organized as follows. Section 2 overviews Methods with different levels. Experimental results are tabulated in Section 3 along with different kind of tests in encrypted domain. Final section concludes the paper.

## II. PROPOSED METHOD

### A. Encryption Phase

The encryption is carried out in two stages: Transformation phase and Substitution (Saturation) phase.

In the transformation phase, pixel positions in the host and substitution images are interchanged or mapped according to modified Pseudo Hadamard transformation. Since image is a two dimensional matrix, each pixel can be represented by a two dimensional space. The resultant transformed images of both host and substitution images are subjected to logical XOR operation to get the cipher image.

**Step 1**: The host image is subjected for MPHT transformation.

$$i'(\alpha',\beta') = i\begin{Bmatrix}(a+3b)\ mod\ 2^n,\\(a+4b)\ mod\ 2^n\end{Bmatrix} \quad (1)$$

The initial values consider here with,

$$i'(\alpha',\beta') = i\begin{Bmatrix}(a+3b)\ mod\ 256,\\(a+4b)\ mod\ 256\end{Bmatrix} \quad (2)$$

Where,

$i$ is the host image

$i'$ is the MPHT transformation image of host

**Step 2**: The substitution image is subjected for MPHT transformation.

$$s'(\alpha',\beta') = s\begin{Bmatrix}(a+4b)\ mod\ 2^n,\\(a+5b)\ mod\ 2^n\end{Bmatrix} \quad (3)$$

The initial values consider here with,

$$s'(\alpha',\beta') = s\begin{Bmatrix}(a+4b)\ mod\ 256,\\(a+5b)\ mod\ 256\end{Bmatrix} \quad (4)$$

Where,

$s$ is the substitution image

$s'$ is the MPHT transformation image of the same

**Step 3**: The resultant transformed images of both host and substitution images are subjected for logical XOR operation pixel wise.

$$r(\alpha,\beta) = i'(\alpha',\beta') \oplus s'(\alpha',\beta') \quad (5)$$

Where,

$r$ is the cipher image of second stage

**Step 4**: The number of execution rounds (d) is placed in the four extreme corners of the cipher image along with the respective pixel values.

$$d = \sum_{n=1}^{N}\sum_{m=1}^{M} i(a,b) \quad (6)$$

Where,

M and N are number of rows and columns in image matrix respectively.

Substitution phase comprises of S-box of size $2^n$ x 1, which includes 256 bits secrete key. The values in the S-box are randomly selected. These values are constant for both encryption and decryption. The obtained cipher image from the transformation stage is subject for pixel wise logical XOR operation along with S-box in the row wise manner.

$$r'(\alpha,\beta) = r(\alpha,\beta) \oplus S-box \quad (7)$$

Where,

$r'$ is the cipher image of final stage

### B. Decryption Algorithm

The number of rounds for decryption stage (d) is taken from the pixel values in the four extreme corners of the cipher image.

**Step 1**: The obtained cipher image from encryption stage is logically XORed with the elements of S-box. The resultant image is the decrypted image from the second stage.

$$r(\alpha,\beta) = r'(\alpha,\beta) \oplus S-box \quad (8)$$

Where,

$r'$ is the cipher image of final stage

**Step 2**: The Substitution image is subjected for MPHT transformation for the same set of initial values as implemented in the encryption stage.

$$s'(\alpha',\beta') = s\begin{Bmatrix}(a+4b)\ mod\ 2^n,\\(a+5b)\ mod\ 2^n\end{Bmatrix} \quad (9)$$

The initial values consider here with,

$$s'(\alpha',\beta') = s\begin{Bmatrix}(a+4b)\ mod\ 256,\\(a+5b)\ mod\ 256\end{Bmatrix} \quad (10)$$

Where,

$s$ is the substitution image

$s'$ is the MPHT transformation image of the same

**Step 3**: The decrypted image from the first step is logically XORed with the transformed image from the second step to get the resultant image of the host in the transformed form.

$$i'(\alpha',\beta') = r(\alpha,\beta) \oplus s'(\alpha',\beta') \quad (11)$$

**Step 4**: The resultant image from the above step is subjected for inverse MPHT transformation to get the desired original image.

$$i(a,b) =$$

$$i' \begin{Bmatrix} (4\alpha - 3\beta)\ mod\ 2^n, \\ (\beta - \alpha)\ mod\ 2^n \end{Bmatrix} \quad (12)$$

The initial values consider here with,

$$i(a, b) = i' \begin{Bmatrix} (4\alpha - 3\beta)\ mod\ 256, \\ (\beta - \alpha)\ mod\ 256 \end{Bmatrix} \quad (13)$$

Where,

$i$ is the host (original) image

$i'$ is the MPHT transformation image of host

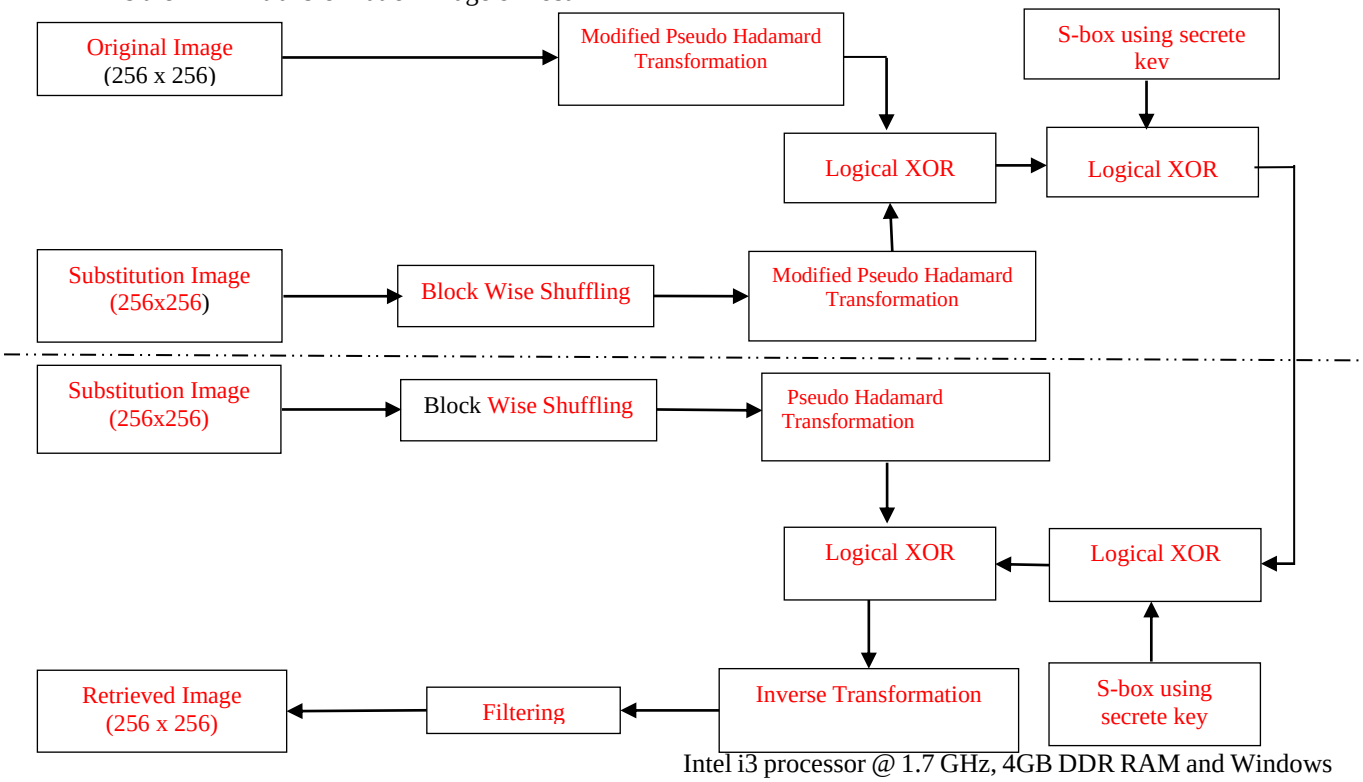


Fig.1 Block diagram of proposed system

**Fig. 2 Host Image**

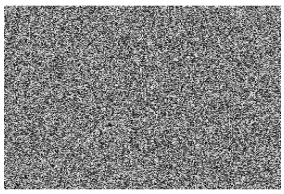

**Fig. 3 Cipher Image**

**Fig. 4 Decrypted Image**

## III. EXPERIMENTAL RESULTS

Security analysis is made on the basis of Number of Pixel Changing Rate (NPCR) and Unified Average Changing Intensity (UACI) and Execution time. Resultant cipher images are subjected for statistical and differential security tests. Matlab software is used for the implementation with Intel i3 processor @ 1.7 GHz, 4GB DDR RAM and Windows

ered to analysis differential hanging Rate (NPCR) test provides similarities between two cipher images. Unified Average Changing Intensity (UACI) test provides similarity index between two cipher images. Host image is encrypted with a secrete key. With the same secrete key, a pixel in the host image is randomly selected, its intensity is changed and subjected for encryption. Cipher images of two cases are compared with each other. Based on the performance from these two tests, the strength of the algorithm to resist differential attack will be decided.

$$UACI = \frac{1}{M\ X\ N}\left[\sum_{i,j=1}^{M,N} \frac{|C1(i,j) - C2(i,j)|}{Maximum\ Pixel\ Intensity}\right] X\ 100$$

$$NPCR = \left[\frac{\sum_{i,j} D(i,j)}{M\ X\ N}\right]\ X\ 100$$

Where,

C1 and C2 are two cipher images with the size M×N
If C1(i , j) ≠ C2(i , j), then D(i , j)=1;
Otherwise, D(i , j)=0.

From table 1 it has been noticed that, an average of 99.6089% NPCR and 33.4328% UACI values are achieved which are greater than 99.5876% and 28.2474% respective values from the conventional PHT algorithm [4] due to effective shuffling of pixel values by MPHT compared to conventional PHT. The algorithm takes an average of 0.18 second for encryption process and is less than 0.29 second mentioned in modified Camellia algorithm [7], 1.27 seconds as mentioned in the hybrid chaotic map [8] to encrypt 256X256 images. Time of execution will be more for large sized images.

**Table- I: Comparison Of Entropy For Encrypted Images With The Existing Algorithms**

| Sl. No. | Images | Number of Pixel Changing Rate (NPCR) ≥ 99.609% [20] | Unified Average pixel Changing Intensity (UACI) ≥ 33.46% [20] | Execution time for encryption (Seconds) | Execution time for Decryption (Seconds) |
|---|---|---|---|---|---|
| 1 | Lena | 90.21 [15] | 31 [15] | 0.26 | 0.2 |
| | | 99.6 [17] | 32.01 [17] | | |
| | | 99.5859 [16] | 33.4201 [16] | | |
| | | 99.588 | 33.4338 | | |
| 2 | Baboon | 99.59 [17] | 30.87 [17] | 0.26 | 0.11 |
| | | 99.6 [18] | 33.43 [18] | | |
| | | 97.2387 [2] | 22.2154 [2] | | |
| | | 99.6262 | 33.2423 | | |
| 3 | Peppers | 99.61 [17] | 30.71 [17] | 0.06 | 0.06 |
| | | 99.6155 | 33.5577 | | |
| 4 | Airplane | 99.6109 | 33.6062 | 0.24 | 0.22 |
| 5 | Cameraman | 99.6460 [19] | 33.4416 [19] | 0.24 | 0.15 |
| | | 99.6414 | 33.6512 | | |
| 6 | Elaine | 98.2354 [2] | 28.1145 [2] | 0.06 | 0.04 |
| | | 99.5956 | 33.3656 | | |
| 7 | Clock | 99.6078 | 33.4257 | 0.11 | 0.11 |
| 8 | Donna | 99.6124 | 33.3818 | 0.11 | 0.09 |
| 9 | Foto | 99.646 | 33.4208 | 0.16 | 0.17 |
| 10 | Soil | 99.6201 | 33.3595 | 0.31 | 0.2 |
| 11 | Barche | 99.5377 | 33.5129 | 0.23 | 0.15 |
| 12 | Montage | 99.5758 | 33.3781 | 0.21 | 0.23 |
| 13 | Pallon | 99.6094 | 33.2864 | 0.2 | 0.22 |
| 14 | Vacas | 99.646 | 33.4354 | 0.1 | 0.11 |
| 15 | Tulips | 99.6017 | 33.4345 | 0.23 | 0.18 |

## IV. CONCLUSION

On the basis of Modified Pseudo Hadamard Transformation (MPHT) and non-Chaotic substitution, a new image encryption algorithm is proposed. The algorithm encrypts an image in two stages per each round. Pixel positions are effectively varied using MPHT and pixel values are effectively modified using non-Chaotic substitution (S-box).

The size of the S-box is 2Kb, with 128 bits of secrete key elements in between. About 2^128 combinations take huge time to execute brute force attack. Along with the S-box, a separate substitution image is considered in the transformation stage. The substitution image used is unique for a set of encryption. Even though the brute force attacker finds the S-box elements, it is very difficult to decrypt the information due to the presence of substitution image. The elements of substitution image are randomly shuffled in each round of encryption using MPHT. Based on these considerations, it is very difficult for unauthorized third party user to cryptanalyze the algorithm. The cipher image after encryption is subjected to various security analysis. In Number of Pixel Changing Rate (NPCR) test, an average of 99.6089% is obtained for fifteen standard images and about 99.9995% close to the ideal value is achieved. In Unified Average pixel Changing Intensity (UACI) test, an average of 33.4328% is obtained for fifteen standard images and about 99.9082% close to the ideal value is achieved.

## REFERENCES


1. Junhui H, Shuhao H, Shaohua T, Jiwu H. JPEG Image Encryption with Improved Format Compatibility and File Size Preservation. IEEE Transactions on Multimedia. Vol. 20, No. 10, 2018, pp. 2645-2658.
2. Leo Y Z, Yuansheng L, Fabio P, Kwok W, Riccardo R, Gianluca S. On the Security of a Class of Diffusion Mechanisms for Image Encryption. IEEE Transactions on Cybernetics. Vol. 48, No. 4, 2018, pp. 1163-1175.
3. Silva V M, Flores R C, Renteria C, Benosoc B L, Perez M A. Substitution box generation using Chaos: An image encryption application. Applied Mathematics and Computation. Vol. 332, 2018, pp. 123-135.
4. Prajwalasimha S.N. (2019) Pseudo-Hadamard Transformation-Based Image Encryption Scheme. In: Krishna A., Srikantaiah K., Naveena C. (eds) Integrated Intelligent Computing, Communication and Security. Studies in Computational Intelligence, vol 771. Springer, Singapore
5. Prajwalasimha S N, Kavya S R and Tanaaz Zeba Ahmed, "Design and analysis of pseudo hadamard transformation and non-chaotic substitution based image encryption scheme," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 3, 2019, pp. 1297-1304.
6. Prajwalasimha S N and S. R. Bhagyashree, " Image Encryption using Discrete Radon Transformation and Non chaotic Substitution," Proc. 2nd IEEE International Conference on Electrical, Computer and Communication Technologies, pp. 842-846, 2017.
7. Prajwalasimha S N and Usha Surendra," Multimedia Data Encryption based on Discrete Dyadic Transformation," Proc. IEEE International conference on Signal processing and Communication, pp. 492-496, 2017.
8. Lingfeng L, Shidi H, Jun L, Wang Z, Xinyi H, Suoxia M. Image block Encryption method based on chaotic maps. IET Journal on Signal Processing. Vol. 12, No. 1, 2017, pp. 22-30.
9. Alireza J, Xin W, Vallipuram M. On the Security of Permutation-Only Image Encryption Schemes. IEEE Transactions on Information Forensics and Security. Vol. 11, No. 2, 2018, pp. 235-246.
10. Marwa S E, Moataz, Abdel W, Sayed M S. Image Encryption Using Camellia and Chaotic Maps. In proceedings of IEEE International Symposium on Signal Processing and Information Technology, 2015, pp.209-214.
11. Hikmat A N, Hamsa A. Image Encryption Using Hybrid Chaotic Map. In proceedings of IEEE International Conference on Current Research in Computer Science and Information Technology 2017, pp. 121-125.
12. Arivazhagan S, Sylvia W, Kalyani S V, Abinaya A D. Mixed Chaotic maps based Encryption for High Crypto Secrecy. In proceedings of IEEE International Conference on Signal Processing, Communications and Networking, 2017, pp. 1-6.
13. Haifaa W S, Ashraf Y M. Image Encryption Using Double Chaotic Logistic Map. In proceedings of IEEE International Conference on Promising Electronic Technologies, 2017, pp. 66-70.
14. Ramtin M S and Sattar M. A Novel Image Encryption Algorithm Based on Discrete Wavelet Transform Using Two dimensional Logistic Map. In proceedings of. Iranian Conference on Electrical Engineering, 2016, pp.1785-1790.
15. Nitumoni H, Sagarika B, Monjul S. A Wavelet Based Partial Image Encryption using Chaotic Logistic Map. In proceedings of IEEE International Conference on Advanced Communication Control and Computing Technologies, 2014, pp. 1-5.
16. Zaheer A B , Muhammad I A, Irfan A .Energy efficient image encryption algorithm. In proceedings of IEEE International Conference on Innovations in Electrical Engineering and Computational Technologies, 2017, pp. 1-6.
17. Nabil B S , Kais B, Mohsen M. Nested chaotic image encryption scheme using two-diffusion process and the Secure Hash Algorithm SHA-1. In proceedings of IEEE International Conference on Control Engineering & Information Technology, 2016, pp. 1-5.
18. Zhengchao N, Xuejing K, Lei W. A Novel Image Encryption Algorithm Based on Bit-level Improved Arnold Transform and Hyper Chaotic Map. In proceedings of IEEE International Conference on signal and Image processing, 2016, pp. 3229-3234.
19. Prajwalasimha S.N., et al., "Image Encryption based on Transformation and Modified Gingerbreadman Chaotic Substitution," Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2019 (ISMAC-CVB), Lecture Notes in Computational Vision and Biomechanics, Springer, Cham
20. W. Xingyuan, et al, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," IEEE Access Letters, Vol. 6, pp. 23733-23746, 2018.


## AUTHORS PROFILE

**Prajwalasimha S N** received Bachelor of Engineering (B.E) Degree in Electronics & Communication from Visvesvaraya Technological University, India in 2012, Master of Technology (M.Tech) Degree in Digital Electronics & Communication Systems from Visvesvaraya Technological University, India in 2014 and pursuing Doctoral Degree (Ph.D) in the field of Cryptography under Visvesvaraya Technological University, India. He has published many research papers in International Journals, Conferences & Book Chapters and serving as Reviewer for International Journals and Conferences. He has been conferred with best research paper award from IEEE ICECCT 2017. His research interest includes Cryptography, Steganography, Digital Image Watermarking and Image Processing

**Dr. L Basavaraj** received Bachelor of Engineering (B.E) Degree in Electrical & Electronics Engineering from University of Mysore, India, Master of Technology (M.Tech) Degree in Digital Electronics from Darwad University, India and Doctoral Degree (Ph.D) in the field of Image & Signal Processing under University of Mysore, India. He has published more than 40 research papers in International Journals, Conferences & Book Chapters and currenty guiding 7 Ph.D scholars. Being senior member of IEEE, his research interest includes Image & Signal Processing