2D-Crypt: Image Encryption and Decryption in Chaotic Domain

Prajwalasimha S N, Chethan Kumar M P, Shiva S, Suryaprasad G N, Navaneeth C S

Abstract: In this article, performance analysis of image cryptosystem designed based on modified Pseudo Hadamard Transformation (MPHT) and Duffing chaotic substitution has been accomplished. Modified Pseudo Hadamard Transformation (MPHT) effectively reduces the redundancy and chaotic Substitution condenses correlation between the adjacent pixels in the cipher image. Standard test images from Computer Vision Group (CVG) are considered for experimental analysis. Immunity against brute force attack is observed for a set of standard test images based on various mathematical analysis. Also better results are obtained for statistical security analysis. About 33.4642% Unified Average Changing Intensity (UACI) and 99.6052% Number of Pixel Changing Rate (NPCR) are obtained for a set of twenty standard images, and they are very close to the ideal value.

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

I. INTRODUCTION

Confidentiality and security of sensitive communication are the major concerns of cryptography. The advancement of information technology and expanding availability to the web, affiliations end up helpless against the insider and outsider threats [1]. Data frameworks are always presented to different kinds of risks, and these risks can cause diverse sorts of harms, Encryption is a process of restructuring the data into some unknown form controlled by a known random key to ensure privacy by keeping the message hidden from anyone for whom it is not intended [2]. Image corroboration anticipates substantiating accuracy and integrity of digital information [3]. An authentication technique of image implicates perceiving the tampered regions in an image by external attacks, localize those sites of changes and its recovery [4].

Image authentication scheme consists of two stages, namely an image embedding stage and a verification stage. Encryption and decryption techniques usually require some secret message, referred to as a key to enable authentication. Decryption is the reverse process of encryption [5]. The encryption process may use different keys for encryption and decryption. The message recipient creates a private key and a public key [6].

Revised Manuscript Received on December 30, 2019.

* Correspondence Author
Prajwalasimha S N*, Department of Electronics & Communication Engineering, ATME Research Centre, Mysuru, India.
Email: prajwalasimha.sn1@gmail.com

Chethan Kumar M P, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Shiva S, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Suryaprasad G N, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

Navaneeth C S, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.

The fruition of digital devices has made an informal routine to capture the digital contents. The digital data brings with its own advantages in terms of processing, usage, transmission and sharing. The security inferences of these sites like unauthorized use and manipulation of digital content should be deliberated in digital communication. To secure the multimedia content various techniques like cryptography, steganography, and watermarking are used [7]. Each technique has its persistence. Altering the connotation of the document involves cryptographic techniques. Steganography works well in covering the manifestation of the significant data. Encryption schemes works for both security and authorization of multimedia content.

The public key is distributed among the message senders and they use the public key to encrypt the message. The unencrypted data is referred to as the plaintext and the encrypted data as cipher text. The security of encryption lies in the ability of an algorithm to generate cipher text that is not easily reverted to the original plaintext. One can use a two dimensional polygraphic substitution cipher such as Hill cipher which increases the level of security [8].

The traditional image encryption in non-transform domain basically involves the matrix based pixel location and pixel value transformations causing histogram reshaping. One can also use complex scan pattern based permutations for image encryption [9].

Due to the intrinsic properties of chaotic maps: sensitivity to initial conditions, degree of randomness and dynamic behavior, and these maps are more commonly used in encryption techniques. Based on the above characteristics of chaotic maps, a new image encryption scheme has been described by Hua &et. al. [10]. The technique is based on 2D Logistic Sine Coupling map (2D-LSCM). Secrete key elements are first subjected to initial permutation and then subjected to 2D-LSCM. In the substitution process these chaotic sequences generated by 2D-LSCM are used for pixel value variations. Very less entropy, correlation between the adjacent pixels in the cipher image, Number of Pixel Changing Rate (NPCR) and Unified Averaging pixel Changing Intensity (UACI) values are observed, indicating the algorithm is less resistive against differential attacks.

Lan&et. al. [11] proposed an image encryption scheme which utilizes integrated chaotic system. The integrated chaotic system is used to increase the randomness behavior of existing chaotic maps. 1D-Sine chaotic maps are cascaded with each other, subjected to nonlinear combination and then introduced to encryption system. The algorithm results with better resistivity against differential attacks by providing prime NPCR and very small difference in UACI compared to their respective ideal values.
Very less redundancy in the cipher image has been observed by very minimum correlation between the adjacent pixels in the cipher image and high entropy values.

Li & et al. [12] proposed a combined 2D Arnold Cat chaotic map and Discrete Wavelet Transformation (DWT) based image encryption technique. The original image is first subjected to 2D Arnold Cat map for further reduction in redundancy. The algorithm results with less UACI values and high NPCR, indicating moderate resistivity against differential attacks. Very less correlation between the adjacent pixels values in the cipher image is also noticed, indicating optimal reduction in the redundancy. A combined chaotic map with Logistic, Sine and Tent maps based image encryption scheme has been described by Zhongyn&et. al. [13]. Pixel scrambling is performed in two stages. At first stage, a combined Logistic-Sine- Cosine chaotic map is used and in the next stage Sine-Tent-Cosine chaotic map is used to reduce inter-pixel redundancy in the host image. The algorithm results with optimal reduction in the redundancy in the cipher image by providing very less correlation between the adjacent pixels in the cipher image. The algorithm results with better NPCR but comparatively less UACI values, indicating moderate stability against differential security attacks.

The remainder paper is organized as follows: Section 2 describes methodology. Section 3 provides comparisons between experimental results obtained from proposed scheme with other existing algorithms. And finally, Section 4 concludes the approach.

II. PROPOSED METHOD

The encryption is carried out in two stages: Transformation and Substitution. The strong redundancy and correlation between adjacent pixels in an image is reduced by subjecting it to pixel position alteration with the help of modified Pseudo Hadamard transformation (MPHT) and pixel value variation using chaotic substitution technique. The original (Host) image is first subjected for transformation using MPHT. A substitution image is considered and it is also subjected for transformation (MPHT). The resultant transformed images of both original and substitution are subjected for logical pixel wise XOR operation to get cipher image from first stage. The obtained cipher image is then subjected for pixel value variation using substitution box (S-box). A predefined S-box is used for substitution in which elements are randomly arranged. Each pixel in the cipher image obtained from the first stage and elements of S-box are subjected for logical pixel wise XOR operation to get final cipher image after substitution. The algorithm is illustrated as follows:

A. Encryption Process

Step1: The original (host) and substitution images are first subjected for Modified Pseudo Hadamard transformation.

\[ I'(\alpha, \beta) = I((\rho + \psi) \mod 2^n, (\rho + 2\psi) \mod 2^n) \]  

(1)

\[ S'(\alpha, \beta) = S'(\rho' + \psi') \mod 2^n, (\rho' + 2\psi') \mod 2^n \]  

(2)

Where,

I is the original (host) image of size \(2^n \times 2^n\)

S is the substitution image of size \(2^n \times 2^n\)

I' is the transformed image (host) of size \(2^n \times 2^n\)

S' is the transformed image (substitution) of size \(2^n \times 2^n\)

Step2: Both transformed images of host and substitution are subjected for bitwise XOR operation

\[ C(\alpha, \beta) = I'(\alpha, \beta) \oplus S'(\alpha, \beta) \]  

(3)

Where,

C(\alpha, \beta) is the cipher image from first stage of size \(2^n \times 2^n\)

Step3: Transformed and substituted image from previous stage is subjected for bitwise XOR operation with the predefined elements of S-box 1.

\[ C''(\alpha, \beta) = C(\alpha, \beta) \oplus S box 1 \]  

(4)

Step4: The cipher image from first stage is subjected for substitution with S-box 2 created using random sequences generated by Duffing chaotic generator.

\[ x_n = (y_n) \mod 2^n \]  

(5)

\[ y'_n = (-bx_n + ay_n - y_n^3) \mod 2^n \]  

(6)

Where,

x_n = present key value \((1 \leq n \leq 8)\)

Step5: The cipher image from first stage is subjected for diffusion of size \(2^n \times 2^n\)

\[ C'(\alpha, \beta) = C''(\alpha, \beta) \oplus S box 2 \]  

(7)

Where,

C'(\alpha, \beta) is the cipher image after diffusion of size \(2^n \times 2^n\)

B. Decryption Process

Step1: The obtained cipher image is first XORed with the elements of S-box 2 used for encryption.

\[ x'_n = (y_n) \mod 2^n \]  

(8)

\[ y'_n = (-bx_n + ay_n - y_n^3) \mod 2^n \]  

(9)

Where,

x_n = present key value \((1 \leq n \leq 8)\)

Step2: The substituted image from previous stage is subjected for bitwise XOR operation with elements of S-box 1.

\[ C(\alpha, \beta) = C'(\alpha, \beta) \oplus S box 1 \]  

(10)

Step3: The substitution image is subjected for MPHT and then XORed with cipher image from previous stage.

\[ S'(\alpha, \beta) = S'(\rho' + \psi') \mod 2^n, (\rho' + 2\psi') \mod 2^n \]  

(12)

\[ I'(\alpha, \beta) = C(\alpha, \beta) \oplus S'(\alpha, \beta) \]  

(13)
Step4: the obtained image from substitution stage is subjected for inverse MPHT to get original image.

\[ I(\rho, \psi) = I((2\alpha - \beta) \mod 2^n, (\beta - \alpha) \mod 2^n) \]  

(14)

### Table 1 Comparison of PSNR, MSE, WDR and Correlation between host and watermarked images

| Images    | Entropy = 8 [2] | Correlation | UACI ≥ 33.4635% [2] | NPCR ≥ 99.6093% [2] |
|-----------|-----------------|-------------|----------------------|----------------------|
| Lena      | 5.5407 (Blow Fish) [21] | 0.0021 [21] | 31.00 [20]           | 90.21 [20]           |
|           | 5.5438 (Two Fish) [21] |             |                      |                      |
|           | 5.5439 (AES 256) [20] |             |                      |                      |
|           | 5.5439 (RC 4) [20] |             |                      |                      |
|           | 7.5220 [20]      | 0.1500 [20] | 32.01 [20]           | 99.60 [20]           |
|           | 7.6427 [24]      |             |                      |                      |
|           | 7.9958 [20]      |             |                      |                      |
|           | 7.9970 [22]      | 0.0019      | 33.4201 [20]         | 99.5859 [20]         |
|           | 7.9971 [20]      |             |                      |                      |
|           | 7.9972 [20]      |             |                      |                      |
|           | 7.9973           |             |                      |                      |
| Baboon    | 7.9947 [20]      | -0.0084     | 30.87 [20]           | 99.59 [20]           |
|           | 7.9950 [20]      |             |                      |                      |
|           | 7.9972           |             |                      |                      |
| Peppers   | 7.9954 [20]      | 4.4768-04   | 30.71 [20]           | 99.61 [20]           |
|           | 7.9960 [20]      |             |                      |                      |
|           | 7.9977           |             |                      |                      |
| Plane     | 7.9973           | 0.0028      | 33.4234              | 99.6152              |
| Cameraman | 7.9973           | -0.0030     | 33.4369              | 99.6442              |
| Elaine    | 7.9973           | 9.1876e-04  | 33.5233              | 99.5849              |
| Carnev    | 7.9977           | -0.0021     | 33.4879              | 99.5889              |
| Donna     | 7.9974           | 0.0007      | 33.4218              | 99.6392              |
| Foto      | 7.9972           | 0.0032      | 33.5423              | 99.6072              |
| Galaxia   | 7.9973           | -0.0022     | 33.5439              | 99.5993              |
| Leopard   | 7.9973           | -0.0060     | 33.4389              | 99.6045              |
| Montage   | 7.9973           | 0.0088      | 33.4963              | 99.5788              |
| Pallon    | 7.9973           | -0.0046     | 33.3212              | 99.6145              |
| Vacas     | 7.9972           | -0.0060     | 33.5133              | 99.5869              |
| Fiore     | 7.9972           | -0.0034     | 33.2979              | 99.6023              |
| Mapasp    | 7.9977           | -0.0055     | 33.4164              | 99.5827              |
| Mare      | 7.9974           | -0.0032     | 33.4591              | 99.6088              |
| Mesa      | 7.9975           | 0.0032      | 33.6244              | 99.6228              |
| Papav     | 7.9974           | -0.0055     | 33.4286              | 99.6257              |
| Tulips    | 7.9975           | 0.0040      | 33.6219              | 99.6269              |

### III. EXPERIMENTAL RESULTS

The proposed algorithm is implemented using Matlab software. Security exploration is accomplished on the basis of Unified Average Changing Intensity (UACI), Number of Pixel Changing Rate (NPCR), Mean Correlation and Entropy between host and encrypted images as tabulated in Table 1.

**Inference 1:** The average value of count of pixel changing rate (NPCR) is 99.6052% for cipher images and is very much close to the ideal value 99.6093% with a hair line difference of 0.004% [2]. The NPCR value floats between 99.5729% to 99.646%. The average value of unified average changing intensity (UACI) is 33.4642%
Inference 2: The average entropy value of cipher images is 7.9973. It is almost 99.96% close to ideal value. The average correlation coefficient between cipher images with respect to their host images is -0.00128. Very minimum correlation has been observed between host and final cipher image after both transformation and substitution stages.

IV. CONCLUSION

In the proposed encryption scheme, modified Pseudo Hadamard transformation (MPHT) is used to condense inter pixel redundancy of original (host) image and Duffing chaotic substitution is used to escalate entropy in the cipher image. Due to MPHT, very slightest correlation between the adjacent pixels is perceived and due to Duffing chaotic map, high entropy in the cipher image is observed.
Deprived similarity between host and final cipher image is perceived with very slightest average correlation co-efficient. Average values of 33.4642% unified average changing intensity (UACI) and 99.6052% number of pixel changing rate (NPCR) are obtained for a set of twenty standard images, and they are very close to the ideal values. Secrete key of 128 bits length is used to increase the level of difficulty for brute force attacks. Further, more number of chaotic generators can be used in the substitution stage to surge the level of security.

REFERENCES

1. Chuman, et. al. “Encryption-then-compression systems using grayscale-based image encryption for JPEG images”, IEEE Transactions on Information Forensics and Security, Vol 14, No. 6, pp. 1515–1525, 2019
2. Wang, X. et al. “An image encryption algorithm based on Josephus traversing and mixed chaotic map”, IEEE Access Lett. Vol. 6, pp. 23733–23746, 2018
3. Prajwalasinha S N et. al., “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, pp. 1297-1304, 2019
4. Anupama Shetter et. al., “Image de-noising algorithm based on filtering and histogram equalization,” Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018, pp. 325-338
5. Prajwalasinha S N et. al., “Performance analysis of DCT and successive division based digital image watermarking scheme,” Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 2, pp. 750-757, 2019
6. Prajwalasinha S N and Pavithra A C, “Digital Image Watermarking based on Successive Division,” Proceedings of IEEE International Conference on Communication and Electronics Systems, pp. 31-35, 2018
7. Prajwalasinha S.N., Sonashree S., Ashoka C.J., Ashwini P. (2019) Digital Image Watermarking Using Sine Transform Technique. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, Vol 30. Springer, Cham
8. Prajwalasinha S N et. al., “CHT-domain Watermarking Technique for still Images: Robust and Imperceptibility Analysis under Noise,” International Journal of Engineering and Advanced Technology, Vol. 9, Issue 2, 2019
9. Prajwalasinha S N et. al., “Modified Gingerbreadman Chaotic Substitution and Transformation based Image Encryption,” Computational Vision and Bio-Inspired Computing, Advances in Intelligent Systems and Computing, Springer, Vol. 1108, 2020
10. Zhongyun Hua, et al., “2D Logistic-Sine Coupling Map for Image Encryption,” Signal Processing, Elsevier, Vol. 149, pp. 148-161, 2018
11. RushilAn, et al., “Integrated Chaotic Systems for Image Encryption,” Signal Processing, Elsevier, Vol. 147, pp. 133-145, 2018
12. Chun-Lai Lia, et al., “Multiple-Image Encryption by using Robust Chaotic Map in Wavelet Transform Domain,” International Journal for Light and Electron Optics, Elsevier, Vol. 171, pp. 276-286, 2018
13. Zhongyun Hua, et al., “Cosine-Transform-based Chaotic System for Image Encryption,” Information Science, Elsevier, Vol. 480, pp. 403-419, 2018

AUTHORSPROFILE

Prajwalasinha S N, Researcher from ATME Research Centre, India. His research interest includes Cryptography, Steganography, Digital Image Watermarking and Image Processing. He has published many research papers in International Journals, Conferences & Book Chapters indexed by Scopus and Web of Science. He is serving as Reviewer for many International Journals and Conferences. He has been conferred with the best research contribution award from IEEE ICECCT 2017.

Chethan Kumar M P, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.

Shiva S, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.

Suryaprasad G N, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.

Navaneeth C S, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.