Combination of Transformation and Substitution Based Image Encryption for Lossless Furtive Image Sharing

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

Abstract—This article intends a fast and efficient cryptosystem based on confusion and Henon chaotic diffusion. The algorithm encrypts an image in two stages. In the first stage, the original image is transformed using Pseudo Hadamard transformation (PHT) along with substitution image. The key length used in the algorithm is 128 bits. These secret key digits are used as initial conditions for modified Henon chaotic generator. A substitution box (S-box) is constructed using random sequences generated by chaotic generator. The cipher image from confusion stage is then subjected for diffusion using S-box. Based on the results obtained from differential and analytical tests, the proposed algorithm withstands such security attacks in comparison with existing systems.

Keywords—Encryption; Secret Key; Confusion; Diffusion; Hadamard transformation; Henon sequence generator

I. INTRODUCTION

Sanctuary of confidential data has recognized ample interest by cryptographers in the ancient few eras [1]. Cryptography and Steganography are the two focal classifications of the information sanctuary system. The core inkling of cryptographic practices is to transmute confidential data into an indecipherable form by using secret key [2]. In steganography, the secret data is secured from antagonists by entrenching it into original data [3].

Compared to text or binary data, images have supplementary features such as higher correlation between adjacent pixels and large data capacity that essential to be reserved into deliberation, when electing an appropriate encryption standards [4-14]. Conventional encryption algorithms such as Advanced Encryption Standards (AES), Rivest-Shamir Adleman (RSA), Data Encryption Standards (DES) and Blow-Fish algorithms are not opposite for image encryption due to such intrinsic properties [15-16]. Thus, conformist encryption algorithms such as AES, DES, 3DES and RSA are not pertinent for digital images because of theirinefficiencyagainst real time applications.

Chaotic theory is one of the extents used to propose image cryptographs owing several anticipated features such as ergodicity, primary state responsibility and volatility [17]. Chaotic performance assessment signposts that the new combined technique has enriched obscurity, higher responsibility, and a larger chaotic factor range as related to other newly available chaotic bitification approaches [18].

Transformation techniques are more habitually adopted for pixel limping in image cryptosystem. Guomin et al. [19] proposed an encryption algorithm using skew Tent map and Line map for confusion and diffusion processes. Algorithm results with better NPCR but slightly less UACI compared to their respective ideal values and better entropy is noticed after each extended rounds. Amrane et al. [20] proposed a new non-chaotic diffusion based algorithm. The algorithm involves block wise shuffling and permutations of original image and diffusion of each pixel is carried out using secret key elements. The resultant image is noticed with slightly less entropy and better performance against differential security attacks. In combined Elliptic curve and Hill cipher based cryptosystem, symmetric key system is converted into asymmetric one in order to increase the security level against differential attacks. The algorithm results with very less UACI and slightly low entropy values and takes more execution time due to combined two systems [21]. Belazi et al. [22] described a combined substitution and permutation based image encryption scheme. The algorithm involves diffusion, substitution and permutation phases. The diffusion is carried out using logistic chaotic map and substitution using S-box. The algorithm results with better entropy, NPCR and UACI compared to their ideal values but correlation between host and cipher images is not very minimum compared to other algorithms. Toughi et al. [23] proposed a hybrid technique using Elliptic curve and Advanced Encryption System. The algorithm results with better entropy, NPCR and UACI compared to other algorithms and ideal values. The algorithm uses 256 bits secret key space, which is very huge and intern reduces the execution speed of the algorithm.

In this paper, a new hybridized image cryptosystem is proposed, in which Pseudo Hadamard transformation is adopted for pixel scrambling and modified Henon chaotic random sequence generator is used for pixel diffusion. Based on the above considerations, an efficient encryption should resist differential and analytical attacks utilizing very less execution time.
II. METHODOLOGY

The proposed algorithm encrypts image in two stages: Confusion and Diffusion. In the confusion phase pixel spots are swapped and in diffusion phase pixel values are varied. Figure 1 illustrates the block diagram of the proposed scheme.

A) Confusion Phase

Step1: The substitution image (256x256) is separated into four sub-images each having 128x128 and subjected for shuffling followed by Pseudo Hadamard transformation (PHT).

\[ S = \begin{bmatrix} s_1 & s_2 \\ s_3 & s_4 \end{bmatrix} \]  
\[ S' = \begin{bmatrix} s_2 & s_3 \\ s_4 & s_1 \end{bmatrix} \]  
\[ s' (\alpha', \beta') = s' \{(a + b) \mod 256, \} \] 
\[ (a + 2b) \mod 256 \]  

Where,

\( s \) is the substitution image

\( s' \) is the PH transformation image of the same

Step2: The original image of size 256x256 is also subjected for PHT.

\[ o' (\alpha', \beta') = o' \{(a + b) \mod 256, \} \] 
\[ (a + 2b) \mod 256 \]  

Where,

\( o \) is the original image

\( o' \) is the PH transformation image of original

B) Key Generation and Diffusion Algorithm

Step1: The 128 bits key is exposed for primary permutation.

Step2: The primary permuted key is separated into 8 groups each with 16 bits.

Step3: Each 16 bits sub-keys are then exposed to modified Henonchaotic key generator to get 256 random keys each with 8 bits and this is subjected to logical XOR process with cipher image after confusion stage.

\[ x_{n+1} = (1 - ax_n^2 + y_n) \mod 256, 0 \leq n \leq 256 \]  
\[ y_{n+1} = (x_n + 1) \mod 256, 0 \leq n \leq 256 \]  

Where \( x_n, y_n \) = present key values

\( x_{n+1}, y_{n+1} \) = new key values

Step3: Each bits of transformed substitution and original images are subjected for XOR operation to get cipher image after confusion stage.

\[ c_1 (\alpha, \beta) = o' (\alpha', \beta') \oplus s' (\alpha', \beta') \]  

Where,

\( c_1 \) is the cipher image after first stage
C) Decryption Phase

Step 1: The 128 bits key is exposed for primary permutation.

Step 2: The primary permuted key is separated into 8 groups each with 16 bits.

Step 3: Each 16 bits sub-keys are then exposed to modified Henon chaotic key generator to get 256 random keys each with 8 bits and this is subjected to logical XOR process with cipher image after confusion stage.

\[ x_{n+1} = (1 - ax_n^2 + y_n) \mod 256 \leq n \leq 256 \]  
\[ y_{n+1} = (x_n + 1) \mod 256 \leq n \leq 256 \]

Where, \( x_n, y_n \) = present key values  
\( x_{n+1}, y_{n+1} \) = new key values

Step 4: The substitution image (256x256) is separated into four sub-images each having 128x128 and subjected for shuffling followed by Pseudo Hadamard transformation (PHT).

\[
S = \begin{bmatrix} s_1 & s_2 \\ s_3 & s_4 \end{bmatrix} \quad (10)
\]

\[
S' = \begin{bmatrix} s_2 & s_3 \\ s_4 & s_1 \end{bmatrix} \quad (11)
\]

Step 5: Each bits of transformed substitution image and cipher image after substitution are subjected for XOR operation to get transformed original image.

\[
o'(\alpha, \beta) = c_1(\alpha', \beta') \oplus s'(\alpha', \beta') \quad (13)
\]

Where,  
\( o' \) is the transformed original image after first stage

Step 6: The obtained image is then subjected for Inverse PHT to get original image.

\[
o''(a, b) = o'((2\alpha' - \beta') \mod 256) \quad (14)
\]

Where,  
\( o'' \) is the retrieved image  
\( o^1 \) is the transformed original image

Step 7: The retrieved image is then subjected for filtering to remove noise.

\[
o''(a, b) = o''(2\alpha - \beta \mod 256) \quad (15)
\]

Where,  
\( o'' \) is the retrieved image

TABLE I Illustration of Host, Substitution, Cipher images after transformation, diffusion and substitution stages

| Host image (Pepper) | Substitution image (Concordseal) |
|---------------------|----------------------------------|
| Transformed image of host | Transformed image of Substitution |
| Diffused Cipher image of stage 1 | Cipher image of Etabl stage |
III. RESULTS AND ANALYSIS

Security tests are conducted on four standard images in Matlab using an Intel i3 processor @1.7 GHz, 4GB DDR RAM and Windows 8 OS. Results are tabulated (TABLE II, III &IV). It has been noticed that, an average 33.4919% of UACI and 99.6124% of NPCR values. And an average 7.9973 entropy and very less correlation between the original and cipher images for standard images. Computational time utilized by the algorithm is very less related to other schemes.

**TABLE. II Comparison of average correlation (NC) between standard and cipher images.**

| Images | NC after confusion | NC after diffusion |
|--------|--------------------|-------------------|
| Lena   | -0.0011            | 1.00E-07          |
| Baboon | -0.0026            | 0.0032            |
| Elaine | -8.23E-04          | -0.0011           |
| Peppers| 2.77E-05           | -0.0006           |

**TABLE. III Comparison of entropy between standard and encrypted images.**

| Images | Entropy ≈ 8 [14] |
|--------|------------------|
| Lena   | 5.5438 (Two Fish) [2] |
|        | 5.5439 (AES 256) [2] |
| Baboon | 7.9974           |
| Elaine | 7.9947 [2]       |
|        | 7.9950 [2]       |
| Peppers| 7.9969 [5]       |
|        | 7.9975           |
|        | 7.9954 [2]       |
|        | 7.9960 [2]       |
|        | 7.9974           |

**Inference 1:** The average entropy value of encrypted images is 7.9973. Its intimacy to the ideal value is about 99.96%. The average correlation coefficient between encrypted images in relation with host images is 3.75E-04. Very slightest correlation has been perceived between host and final encrypted image, indicating deprived similarity between them.

**TABLE. IV Security test performance of the proposed algorithm for standard images**

| Images  | UACI ≥ 33.464% [14] | NPCR ≥ 99.609% [14] |
|---------|---------------------|---------------------|
| Lena    | 28.3192 [2]         | 99.61 [2]           |
|         | 33.4201 [24]        | 99.5859 [24]       |
| Baboon  | 33.4975             | 99.6125             |
| Elaine  | 98.2354 [25]        | 98.2354 [25]       |
| Peppers | 29.3452 [2]         | 99.5412 [2]        |
|         | 33.5127 [16]        | 99.6002 [16]       |
|         | 33.4983             | 99.6194             |

**Inference 2:** The average value of Number of Pixel Changing Rate (NPCR) is 99.6124% for encrypted images and is very much neighbouring to the ideal value 99.6093% [14] with a very minimum variance of 0.0035%. The NPCR value drifts among 99.6071% to 99.6129%. The average value of Unified Average Changing Intensity (UACI) is 33.4919% for cipher images, neighbouring to ideal value 33.4635% [14] with the minimum variance of 0.0284%. The UACI value drifts among 33.4822% to 33.4919%. 

**Fig. 2** Comparison of average correlation (NC)

**Fig. 3** Comparison of entropy
IV. CONCLUSION

The proposed algorithm encrypts an image using pseudo Hadamard transformation and modified Henon chaotic substitution. The key length used is 128 bits. This makes $2^{128}$ more combinations for brute force attacker to extract the key set and these secret key digits are used as initial conditions to the chaotic generator in the substitution stage. The resultant image obtained after encryption process is subjected for various differential attack analysis. An average 33.4919% of UACI and 99.6124% of NPCR values are obtained, which are greater than the respective ideal values and better compared to other existing schemes. The algorithm results with an average 7.997 entropy values and it is about 99.96% close to the ideal value, indicating effective reduction of redundancy in the cipher image. Very less similarity in terms of correlation between original and cipher images is noticed. The algorithm utilizes very less execution time related to conventional method. Different chaotic generators can be used in the substitution stage to get better entropy in the cipher image.

REFERENCES

1. Pauline Puteaux and William Puech, “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images,” IEEE Transactions on Information Forensics and Security, Vol. 13, No. 7, 2018, pp. 1670-1681.

2. Prajwalasimha S N and Basavaraj L, “Performance Analysis of Transformation and Bogdonov Chaotic Substitution based Image Cryptosystem,” International Journal of Electrical and Computer Engineering, Vol. 10, No. 1, 2020, pp. 188-194.

3. Prajwalasimha 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, 2019, pp. 1297-1304.

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. Prajwalasimha 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. Prajwalasimha S.N., Sowmyashree A.N., Suraksha B., Shashikumar H.P. (2019) Logarithmic Transform based Digital Watermarking Scheme. 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

7. Prajwalasimha 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.

8. Prajwalasimha S N et al., “Digital Image Watermarking Based on Sine Transformation with Constant Co-Efficient,” Proceedings of the International Conference on Inventive Research in Computing Applications, pp. 21–24, 2018.

9. Prajwalasimha 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

10. Prajwalasimha S N et al., “Performance Analysis of Combined Discrete Fourier Transformation (DFT) and Successive Division based Image Watermarking Scheme,” International Journal of Recent Technology and Engineering, Vol. 8, Issue 3, 2019, pp. 34–39.

11. Prajwalasimha S N et al., “Digital Image Watermarking based on Sine Hyperbolic Transformation,” Proceedings of 3rd IEEE International Conference on Electrical,
Combination of Transformation and Substitution Based Image Encryption for Lossless Furtive Image Sharing

12. Prajwalasimha S N et al., “Design and Implementation of Image Watermarking Scheme based on Exponential Function,” International Journal of Innovative Technology and Exploring Engineering, Vol. 8, Issue 12, 2019, pp.5789-5792

13. Prajwalasimha S N et al., “Lossless Watermarking for Image Ratification: An Implementation based on 12th Root of Exponential Function,” International Journal of Innovative Technology and Exploring Engineering, Vol. 9, Issue 1, pp.4631-4636, 2019

14. 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

15. Prajwalasimha S N and Bhagyasheer S R, “Image Encryption using Discrete Radon Transformation and Non chaotic Substitution,” Proc. of IEEE International Conference on Electrical, Computer and Communication Technologies, pp. 842-846, 2017

16. Prajwalasimha S N and Usha Surendra, “Multimedia Data Encryption based on Discrete Dyadic Transformation,” Proc. of IEEE International conference on Signal processing and Communication, pp. 492-496, 2017

17. Prajwalasimha S N and Basavaraj L, “Design and Implementation of Transformation and non-Chaotic Substitution based Image Cryptosystem,” International Journal of Engineering and Advanced Technology, Vol. 8, Issue 6, pp.1079-1083, 2019

18. Prajwalasimha S N et al., “On the Sanctuary of a Combined Confusion and Diffusion based scheme for Image Encryption,” International Journal of Engineering and Advanced Technology, Vol. 9, Issue 1, pp.3258-3263, 2019

19. Guomin Zhou, Daxing Zhang, Yanjian Liu, Ying Yuan and Qiang Liu, “A novel image encryption algorithm based on chaos and Lane map,” Neurocomputing, Elsevier, Vol. 169, No. 2, 2015, pp.150-157.

20. AmraneHouas, ZouhirMokhtari, Kamal EddineMelkemi andAbdelmalikBoussaad,“A novel binary image encryption algorithm based on diffuse representation,”Engineering Science and Technology, Vol 19, No. 4, Dec 2016, pp. 1887-1894.

21. Ziad E.Dawahdeh, Shahrul N.Yaakob and RozmieRazif bin Otman “A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher,”Journal of King Saud University - Computer and Information Sciences, Vol 30, No. 3, 2018, pp. 349-355

22. Akram Belazi, Ahmed A. Abd El-Latif and Safya Belghith,”A novel image encryption scheme based on substitution-permutation network and chaos,”Signal Processing, Vol. 128, No. 1, 2016, pp. 155-170

23. Toughi Shahririya, Mohammad H. Fathi, Yoones A. Sekhavat,“An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System,”Signal Processing, Vol. 141, No. 1, 2017, pp. 217-227

24. 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, 2018, pp. 276-286

25. Y. Z. Leo, et al., “On the Security of a Class of Diffusion Mechanisms for Image Encryption,” IEEE Transactions on Cybernetics, Vol. 48, No. 4, 2018,pp. 1163-1175

26. S. E. Marwa, et al., “Image Encryption Using Camellia and Chaotic Maps,” Proc. IEEE International Symposium on Signal Processing and Information Technology, pp. 209-214, 2015.

27. A. N. Hikmat and A. Hansa, “Image Encryption Using Hybrid Chaotic Map,” Proc. IEEE International Conference on Current Research in Computer Science and Information Technology, pp. 121-125, 2017.

28. W. Xingsuan, et al, “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map,” IEEE Access Letters, Vol. 6, pp. 23733-23746, 2018.

29. C. Delong, et al, “Image Encryption Using Block Based Transformation with Fractional Fourier Transform,” Proc. IEEE International Conference on Communications and Networking, pp. 552-556, 2014.