International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

On the Sanctuary of a Combined Confusion and Diffusion based scheme for Image Encryption

Prajwalasimha S N, Aishwarya V Kumar, Arpitha C R

Abstract*: Confusion and diffusion are the frequently used embryonics in multimedia (image) encryption systems. Multimedia data protection against cryptanalysis can be effectually fortified by these techniques. Due to inherent properties of images such as high inter-pixel redundancy and bulk data capacity, encryption is performed in two stages: Confusion and Diffusion. In this article, a combined Pseudo Hadamard transformation in the confusion stage and Gingerbreadman chaotic substitution in the diffusion stage are used in the encryption phase of the algorithm. The strong correlation between contiguous elements in the host image is effectually reduced using Pseudo Hadamard transformation and entropy in the cipher image is enhanced using Gingerbreadman chaotic substitution. Secrete key length used in the algorithm is 128 bits, these are the initial conditions for Gingerbreadman chaotic generator. The elements of S-box in the substitution stage are considered from this random sequence generator. Experimental exploration including information entropy, correlation analysis, sensitivity analysis, key space analysis and computational complexity have been performed on set of standard images. Results obtained are better compared to many existing systems.

Keywords*: Confusion; Encryption; Correlation; Entropy; Security; Diffusion; Multimedia.

I. INTRODUCTION

Distinctive and swift evolution in the field of technology fortified significant advancement in past decade. Intellectual Property venders are more concerned about legitimacy of private information in multimedia due to security violations by unauthorized users [1]. Confidentiality can be enhanced by encrypting the original information into cipher form. In order to ensure secure transmission of image data, multimedia encryption mystifies the host stream into cipher form and conceded between two parties over a public channel. Popular encryption standardized, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been broadly espoused worldwide, since decades. But, the delinquent of image encryption is yonder the solicitation of conventional and renowned encryption algorithms. This is mainly due to the application requirements and constrictions levied by the data structure of images, such as format compliance, perceptibility, complexity, real-time performance, compression efficiency and the security level [2][16-26]. To treatise these disquiets, substantial endeavors have been made to mature robust encryption systems for the image data. Image encryption standards are designed with three diversified methods of operations, due to its grid nature. The three different stages include: value transformation, position permutation and the combination form. Between different maneuvers, permutation (confusion) is a frequently espoused primeval in most of the image encryption algorithms. This is essentially due to the easy enactment and application in both frequency and spatial domains [3]. Traditional and conformist encryption algorithms, such as DES, RSA or AES cannot be applied for images, due to rate adaptation in heterogeneous networks for multimedia transmission and for multimedia content in image extraction [4]. In order develop an efficient encryption algorithm, chaos based encryption schemes are more popular, now a day [5-9]. Shereek et al. [10] described a method for information security by applying a combined RSA and Fermat's algorithm. Even though Fermat's algorithm increases the speed of the RSA, the hybrid technique uses more time to generate the substitution elements. Liu et al. [11] formed a public authority based on privacy-preserving authentication protocol (SAPA) to discourse privacy concern in information stowage. They portrayed an improved Montgomery block Lanczos scheme for encryption in data protection. Rivest et al. [12] revealed a public-key encryption process using a secrete key overtly exposed by the envisioned inheritor where the message was deciphered with a decryption key. Saxena et al. [13] exemplified the review of numerous parallel implementations of RSA algorithm linking diversity of hardware and software enhancements. Symmetric key algorithms use a single key to encrypt as well as to decrypt the data whereas public key algorithms use two distinct keys for encryption and decryption. Padmaja et al. [14] proposed the security of cloud computing using public key cryptography using RSA algorithm. The amount of protection needed to secure data was directly proportional to the value of the data and the performance of the cloud network varies according to the type of the algorithm such as symmetric, asymmetric or hashing algorithms. Genkin et al. [15] exemplified a cryptoanalysis key abstraction technique through the application of RSA. A combined Pseudo Hadamard transformation (PHT) and Gingerbreadman Chaotic (GBC) replacement based image encryption algorithm has been proposed in order to provide two stage security per each round.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Prajwalasimha S N*, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.
Email: prajwalasimha.sn1@gmail.com
Aishwarya V Kumar, Department of Electronics & Communication Engineering, ATME College of Engineering, Mysuru, India.
Arpitha C R, Department of Electronics & Communication Engineering, ATME College of Enginnering, Mysuru, India.

II. METHODOLOGY

Encryption is performed in two phases: Confusion and Diffusion. In the confusion phase, pixel positions in the host and substitution images are interchanged/mapped according to 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 are subjected to logical XOR operation to get the cipher image. S-box is developed for diffusion processes using random sequence generated by Gingerbreadman chaotic key sequence generator. Final cipher image is attained by relieving elements of S-box with each element of cipher image acquired from initial stage.

A. *Ciphering Phase*

Step1: The original (host) and substitution images are first imperiled to PHT.

$$H'(\psi,\mu) = H((\alpha+\beta)\ mod\ 2^n, (\alpha+2\beta)\ mod\ 2^n) \quad (1)$$

$$S'(\psi,\mu) = S^t((\alpha'+\beta')\ mod\ 2^n, (\alpha'+2\beta')\ mod\ 2^n) \quad (2)$$

$$1 \le \alpha, \alpha', \beta, \beta' \le 2^n$$

Where,

H - Original (host) image (2^n X 2^n)

S - Substitution image (2^n X 2^n)

H' - Transformed image (2^n X 2^n)

S^t- Transformed image (substitution) (2^n X 2^n)

Step2: Both transformed images of host and substitute are imperiled to bitwise XOR operation

$$C(\psi,\mu) = H'(\psi,\mu) \oplus S'(\psi,\mu) \quad (3)$$

Where,

$C(\psi,\mu)$ - Encrypted image from stage-1

Step3: Encrypted image from previous stage is imperiled to bitwise XOR operation with the predefined elements of Sbox-1 for first stage substitution (Second stage of encryption).

$$C"(\psi,\mu) = C(\psi,\mu) \oplus Sbox\text{-}1 \quad (4)$$

Step4: Encrypted image from second stage is imperiled to substitution with Sbox-2 created using arbitrary sequences engendered by Gingerbreadman chaotic generator.

$$a'_n = (1 - b_n + |a_n|)\ mod\ 2^n \quad 1 \le n \le 8 \quad (5)$$

$$b'_n = (b_n)\ mod\ 2^n \quad (6)$$

Where

a_n= present key value

$$C'(\psi,\mu) = C"(\psi,\mu) \oplus Sbox\text{-}2 \quad (7)$$

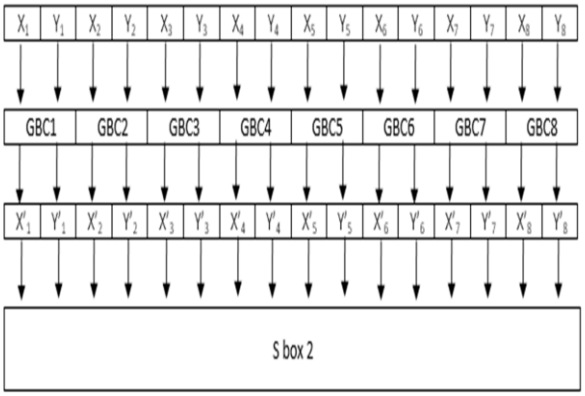


Fig. 1 Key sequence generation algorithm

B. De-ciphering Algorithm

Step1: Obtained cipher image is first bit wise XORed with the elements of Sbox-2, the same used for encryption.

$$a'_n = (1 - b_n + |a_n|)\ mod\ 2^n \quad 1 \le n \le 8 \quad (8)$$

$$b'_n = (b_n)\ mod\ 2^n \quad (9)$$

Where

a_n= present key value

$$C"(\psi,\mu) = C'(\psi,\mu) \oplus Sbox\ 2 \quad (10)$$

Step2: De-substituted image from previous stage is imperiled to bitwise XOR operation with elements of Sbox-1.

$$C(\psi,\mu) = C"(\psi,\mu) \oplus Sbox\ 1 \quad (11)$$

Step3: The substitution image same as that in the encryption stage is imperiled to PHT and then XORed with cipher image from previous stage.

$$S'(\psi,\mu) = S^t(\alpha'+\beta')\ mod\ 2^n, (\alpha'+2\beta')\ mod\ 2^n \quad (12)$$

$$H'(\psi,\mu) = C(\psi,\mu) \oplus S'(\psi,\mu) \quad (13)$$

Step4: The obtained image from substitution stage is exposed to inverse PHT to get original image.

$$H''(\alpha,\beta) = O'((2\psi - \mu)\ mod\ 2^n, (\mu - \psi)\ mod\ 2^n) \quad (14)$$

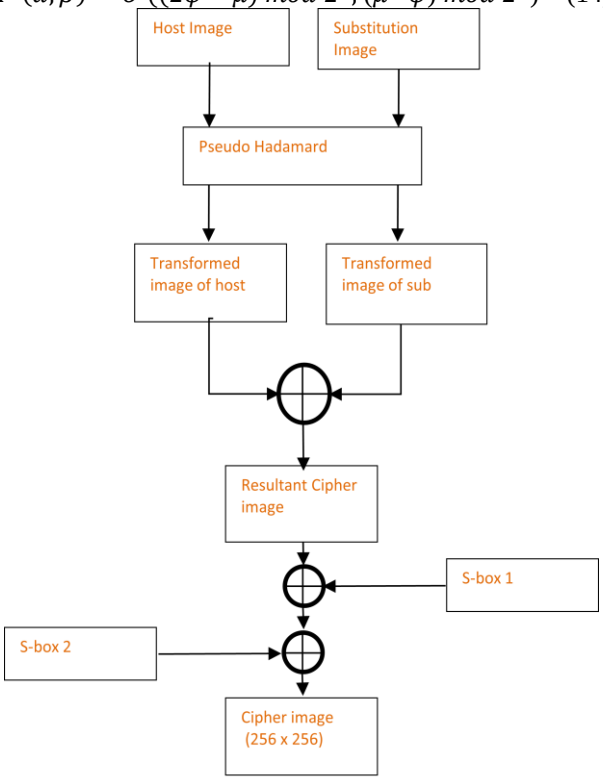


Fig. 2 Flow diagram of proposed encryption algorithm

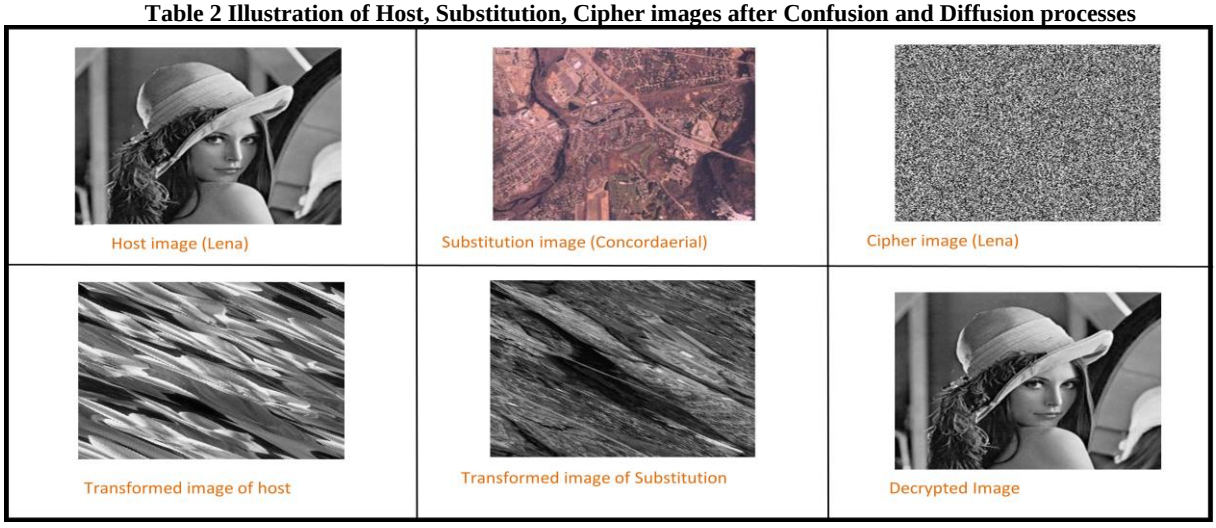
III. EXPERIMENTAL RESULTS

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. Experimental scrutiny and enactment are done using Matlab software. Database is considered from Computer Vision Group, Granada, Spain. Illustration of Host images, Substitution image, Cipher images after transformation and substitution in Table 2. The estimated values of UACI and NPCR are neighboring to the ideal values, signifying high competence in contradiction to differential security occurrences. After confusion phase, interpixel redundancy in the cipher image is effective reduced and high entropy is perceived after diffusion phase, very close to the ideal values [30].

Table 1 Comparison of Entropy, Correlation, UACI and NPCR between standard and encrypted images

Images	Entropy = 8 [30]	Correlation	UACI ≥ 33.4635% [30]	NPCR ≥ 99.6093% [30]
Lena	5.5407 (Blow Fish) [28]	0.0021 [28]	31.00 [27]	90.21 [27]
	5.5438 (Two Fish) [28]			
	5.5439(AES 256) [27]			
	5.5439 (RC 4) [27]	0.1500 [27]	32.01 [27]	99.60 [27]
	7.5220 [27]			
	7.6427 [31]			
	7.9958 [27]	0.0256	33.4201 [27]	99.5859 [27]
	7.9970 [29]			
	7.9971 [27]			
	7.9972 [27]		33.46	99.57
	7.9972			
Baboon	7.9947 [27]	-0.0043	30.87 [27]	99.59 [27]
	7.9950 [27]			
	7.9970		33.28	99.59
Peppers	7.9954 [27]	5.1589e-04	30.71 [27]	99.61 [27]
	7.9960 [27]		33.46	99.59
	7.9973			
Plane	7.9971	0.0027	33.40	99.59
Cameraman	7.9972	-0.0037	33.42	99.62
Elaine	7.9973	8.1763e-04	33.49	99.58
Carnev	7.9975	-0.0024	33.49	99.58
Donna	7.9972	0.0028	33.42	99.61
Foto	7.9970	0.0064	33.58	99.60
Galaxia	7.9971	-0.0013	33.53	99.59
Leopard	7.9971	-0.0029	33.40	99.59
Montage	7.9972	0.0066	33.47	99.58
Pallon	7.9973	-0.0012	33.31	99.60
Vacas	7.9971	-0.0016	33.53	99.58
Fiore	7.9971	-0.0008	33.27	99.60
Mapasp	7.9974	-0.0018	33.41	99.58
Mare	7.9973	-0.0008	33.43	99.59
Mesa	7.9973	0.0027	33.63	99.61
Papav	7.9973	-0.0011	33.41	99.62
Tulips	7.9974	0.0034	33.62	99.61

Table 2 Illustration of Host, Substitution, Cipher images after Confusion and Diffusion processes



Inference 1: The average value of Number of Pixel Changing Rate (NPCR) is 99.594% for encrypted images and is very much neighbouring to the ideal value 99.6093% [30] with a very minimum variance of 0.015%. The NPCR value drifts among 99.57% to 99.62%. The average value of Unified Average Changing Intensity (UACI) is 33.4505% for cipher images, neighbouring to ideal value 33.4635% [30] with the minimum variance of 0.013%. The UACI value drifts among 33.27% to 33.63%

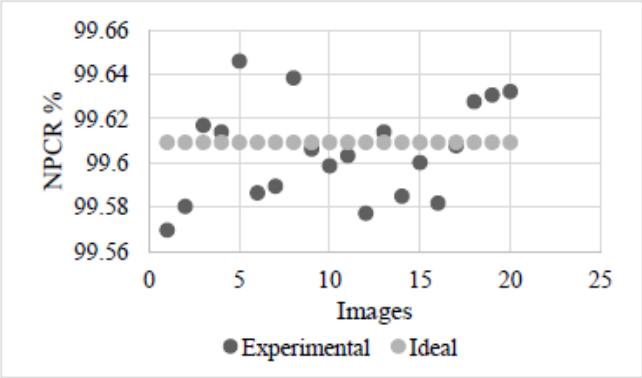


Fig. 3 Number of Pixel Changing Rate of cipher images

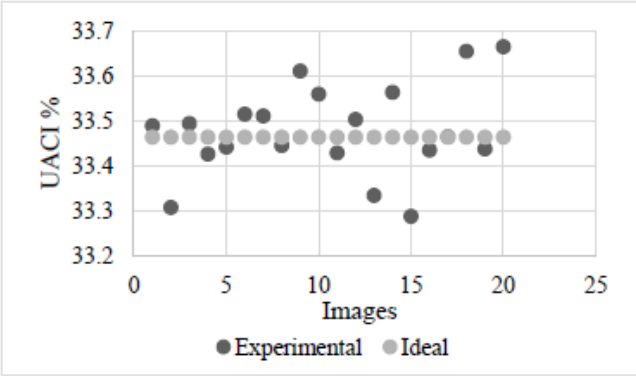


Fig. 4 Unified Average Changing Intensity of cipher images

***Inference 2*:** The average entropy value of encrypted images is 7.9972. Its intimacy to the ideal value is about 99.96%. The average correlation coefficient between encrypted images in relation with host images is 0.0014. Very slightest correlation has been perceived between host and final encrypted image, indicating deprived similarity between them.

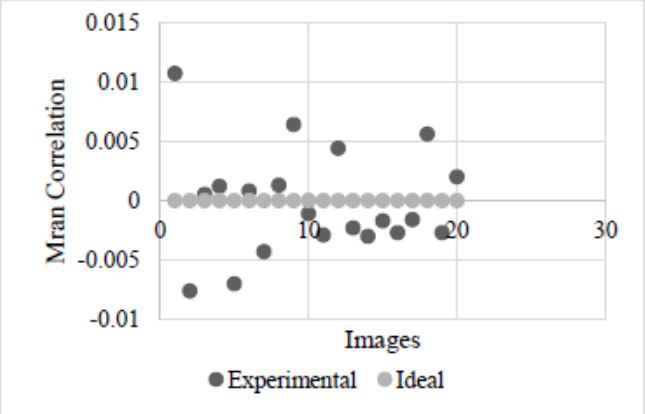


Fig. 5 Mean correlation between original and cipher images

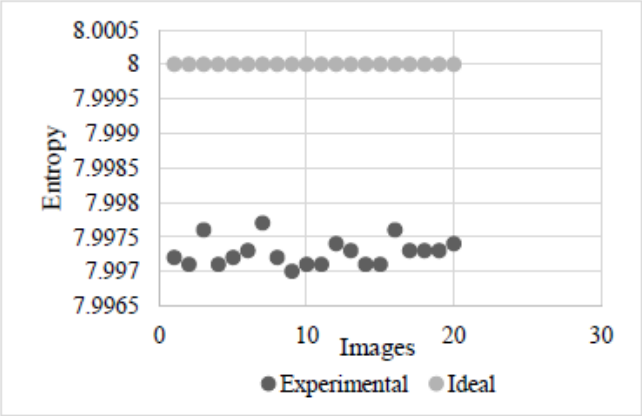
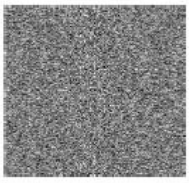
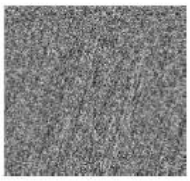
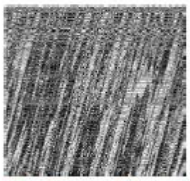
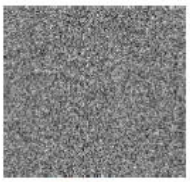
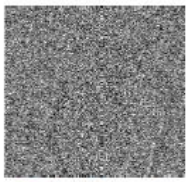
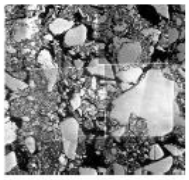
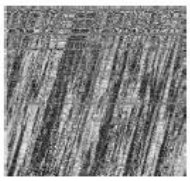
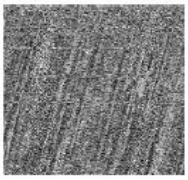
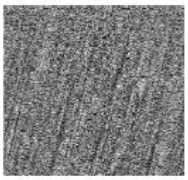
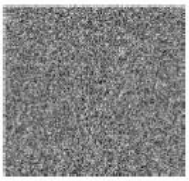
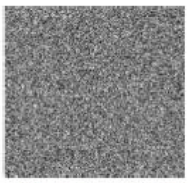
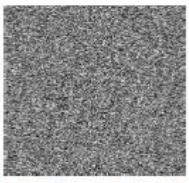
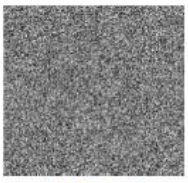
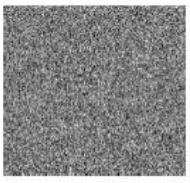
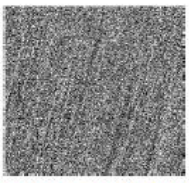
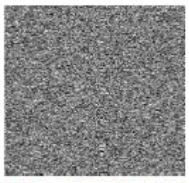


Fig. 6 Information entropy of cipher images

 Lena	 Baboon	 Pepper	 Airplane	 Cameraman
 Cipher Image (Lena)	 Cipher Image (Baboon)	 Cipher Image (Pepper)	 Cipher Image (Airplane)	 Cipher Image of (Cameraman)
 Elaine	 Carnev	 Donna	 Foto	 Soil
 Cipher Image (Elaine)	 Cipher Image (Carnev)	 Cipher Image (Donna)	 Cipher Image (Foto)	 Cipher Image (Soil)
 Barche	 Montage	 Pallon	 Vacas	 Tulips
 Cipher Image (Barche)	 Cipher Image (Montage)	 Cipher Image (Pallon)	 Cipher Image (Vacas)	 Cipher Image (Tulips)

IV. CONCLUSION

A new image encryption/decryption scheme based on diffusion by Gingerbreadman Chaotic (GBC) substitution and confusion by Pseudo Hadamard transformation (PHT) is magnificently proposed. The strong correlation between contiguous elements in the host image is effectually reduced using Pseudo Hadamard transformation with an average correlation of 0.0014 between original and cipher images. Average entropy of 7.9972 in the cipher image is observed using Gingerbreadman chaotic substitution. The algorithm is intended with 128 bits of secrete key.

This is used as initial condition for chaotic generator in the substitution phase of the algorithm. Due to 2^128 combinations of secrete key, brute force attack is tardy with respect to execution speed of the processor. Standard test images are considered for experimental analysis. In the security tests, average values of 33.4505% UACI and 99.594% NPCR are obtained for a set of twenty standard images and they are very close to the ideal values. Further, UACI and NPCR can be increased by introducing constants along with variants in chaotic generator to obtain more randomness in the chaotic sequence.

REFERENCES

1. Tatsuya Chuman, Warit Sirichotedumrong and Hitoshi Kiya, "Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images," IEEE Transactions on Information Forensics And Security, Vol. 14, No. 6, 2019, pp. 1515-1525
2. Alireza Jolfaei, Xin-Wen Wu and Vallipuram Muthukkumarasamy, "On the Security of Permutation-Only Image Encryption Schemes," IEEE Transactions on Information Forensics and Security, Vol. 11, No. 2, 2016, pp. 235-246
3. Yinian Mao and Min Wu, "A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption," IEEE Transactions on Image Processing, Vol. 15, No. 7, 2006, pp. 2061-2075
4. 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
5. Zhongyun Hua, Fan Jin, Binxuan Xu, Hejiao Huang and Gianluca Setti, "2D Logistic-Sine Coupling Map for Image Encryption," Signal Processing, Elsevier, Vol. 149, 2018, pp. 148-161.
6. Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu and Xiaonan Luo, "Integrated Chaotic Systems for Image Encryption," Signal Processing, Elsevier, Vol. 147, 2018, pp. 133-145.
7. Chun-Lai Lia, Hong-Min Lia, Fu-Dong Lib, Du-Qu Weid, Xuan-Bing Yange and Jing Zhangf, "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
8. Zhongyun Hua, Yicong Zhou and Hejiao Huang, "Cosine-transform-based chaotic system for image encryption," Information Science, Elsevier, Vol. 480, 2019, pp. 403-419
9. Ahmad J and Hwang S O, "A secure image encryption scheme based on chaotic maps and affine transformation" Multimedia Tools and Applications, Elsevier, Vol. 75, No. 21, 2015, pp. 13951-13976
10. B. M, Shereek, Z. Muda, S. Yasin. 2014. Improve Cloud Computing Using RSA Encryption with Fermat's Little Theorem, IOSR Journal of Engineering. 4(2): 1-8.
11. H. Liu, H. Ning, Q. Xiong and L. T. Yang. 2015. Shared authority-based privacy preserving authentication protocol in cloud computing, IEEE Transactions on Parallel and Distributed Systems 26 (1):241–251.
12. R. L. Rivest, A. Shamir and L. Adleman. 1983. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 26:96–99.
13. S. Saxena and B. Kapoor, "State of the art parallel approaches for RSA public key-based cryptosystem", arXiv preprint arXiv: 1503.03593.
14. E. Vecharynski, Y. Saad and M. Sosonkina.2014. Graph partitioning using matrix values for preconditioning symmetric positive definite systems, SIAM Journal on Scientific Computing 36 (1): A63–A87
15. D. Genkin, A. Shamira and E. Tromer, 2014. RSA Key Extraction via Low Bandwidth Acoustic Cryptanalysis", in: International Cryptology Conference (CRYPTO'14), Springer: pp. 444–461
16. 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
17. 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
18. 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, 2019, pp.1079-1083.
19. 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
20. 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
21. 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
22. 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
23. 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
24. 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
25. Prajwalasimha S N, et al., "Digital Image Watermarking based on Sine Hyperbolic Transformation," Proceedings of 3rd IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1245-1250, 2019
26. 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
27. Anees A, Siddiqui A M and Ahmed F, "Chaotic substitution for highly autocorrelated data in encryption algorithm," Communications in Nonlinear Science and Numerical Simulation, Elsevier, Vol.19, No.9, 2014, pp. 3106-3118
28. 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
29. Prajwalasimha S N and Bhagyashree 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
30. Xingyuan Wang, Xiaoqiang Zhu and Yingqian Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," IEEE Access Lett., Vol. 6, 2018, pp. 23733-23746.
31. 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