International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1327~1336
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1327-1336

A novel efficient multiple encryption algorithm for real time images

Shima Ramesh Maniyath, Thanikaiselvan V.
School of Electronics Engineering (SENSE), Vellore Institute of Technology (VIT), Vellore, India

Article Info

Article history:

Received Apr 7, 2019
Revised Oct 17, 2019
Accepted Oct 25, 2019

Keywords:

Arnold
DNA
NPCR
UACI

ABSTRACT

In this study, we propose an innovative image encryption Techniques based on four different image encryption Algorithm. Our methodology integrates scrambling followed by Symmetric and Asymmetric Encryption Techniques, to make the image meaningless or disordered to enhance the ability to confront attack and in turn improve the security. This paper mainly focused on the multiple encryption Techniques with multiple keys on a single image by dividing it into four blocks. So instead of using one Encryption method a combination of four different Encryption Algorithm can make our image more secure. The Encryption is done first by using DNA as secret key, second by using RSA, third by DES and fourth by Chebyshev. The pros and cons for all the Encryption methods are discussed here. Proposed methodology can strongly encrypt the images for the purpose of storing images and transmitting them over the Internet. There are two major benefits related with this system. The first benefit is the use of Different Algorithm with different keys. The second benefit is that even though we are using four different Algorithm for a single image, the time taken for encryption and decryption is few seconds only. Our method is methodically checked, and it shows an exceptionally high level of security with very good image quality.

Corresponding Author:

Thanikaiselvan V.,
Department of Communication Engineering,
School of Electronics Engineering,
Vellore Institute of Technology, Vellore, India
Email: Thanikaiselvan@vit.ac.in

1. INTRODUCTION

The key difference between various forms of technology is key size and strength. For secret communications militaries and governments has been using encryption for a very long period. Nowadays many forms of civilian communications are also using encryption for data security. Conversion of normal text into cipher text is the basic purpose of encryption. Encryption can make sure that data not reaches the wrong person, isn't altered during transmission and can be used to verify the identity of sender. Symmetric cryptography or shared secret encryption is one of the two ways of doing encryption in modern times. It has been used since ancient Egyptian times, is called symmetric cryptography or shared secret encryption [1]. In this method the data is scrambled into incomprehensible form by a secret Shared key.This is also called as private-key cryptography because the key used for encrypting and decrypting the data has to be secure. Anyone with knowledge of the shared key can decrypt the information. In short, sender encrypts the data with one key and sends it and data is decrypted by the receiver using the keys. Asymmetric encryption, or public-key cryptography, is different from the previous method because two keys and used for encryption and decryption. The first key called as the public key which is freely available to anyone is used to encrypt the data, whereas the recipient uses a private key to decrypt the message. Either of the methods should likely provide sufficient data security. Here we are using two Asymmetric Algorithm such as DNA and RSA and two symmetric Algorithm such as DES and Chebyshev Algorithm for a single image. The complexity in breaking each

Algorithm is equally difficult so that applying all the Algorithm on a single image proves the high level of security. Simulation results and Security analysis are provided

2. PROPOSED METHOD

The main aim of this method is to secure an image by using multiple encryption techniques.here we are using four encryption algorithms, both symmetric key and asymmetric key algorithms. In this method an image is divided into four blocks such as B1, B2, B3, B4.Asymmetric key algorithm like RSA and DNA is applied for B1 and B2. Symmetric key algorithm such as DES and Chebyshev for B3, B4 is mentioned in Figure 1.

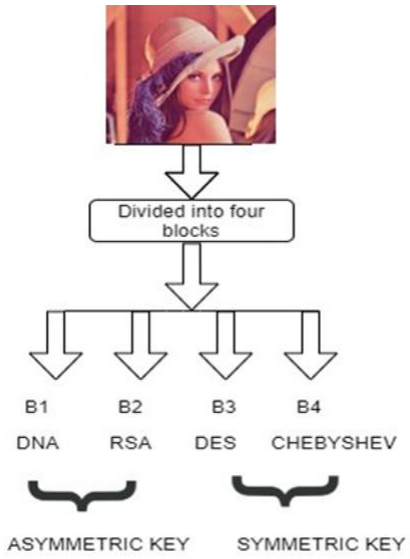

Figure 1. Block diagram of proposed method

2.1. Dividing into four blocks

An image of size 256 X 256 is divided into four blocks B1,B2,B3,B4 ,each of size 64 X 64 as shown in Figure 2. In that for B1,B2 image blocks we have applied Asymmetric key Encryption Algorithm and for B3 and B4 blocks Symmetric key Encryption Algorithm is applied.

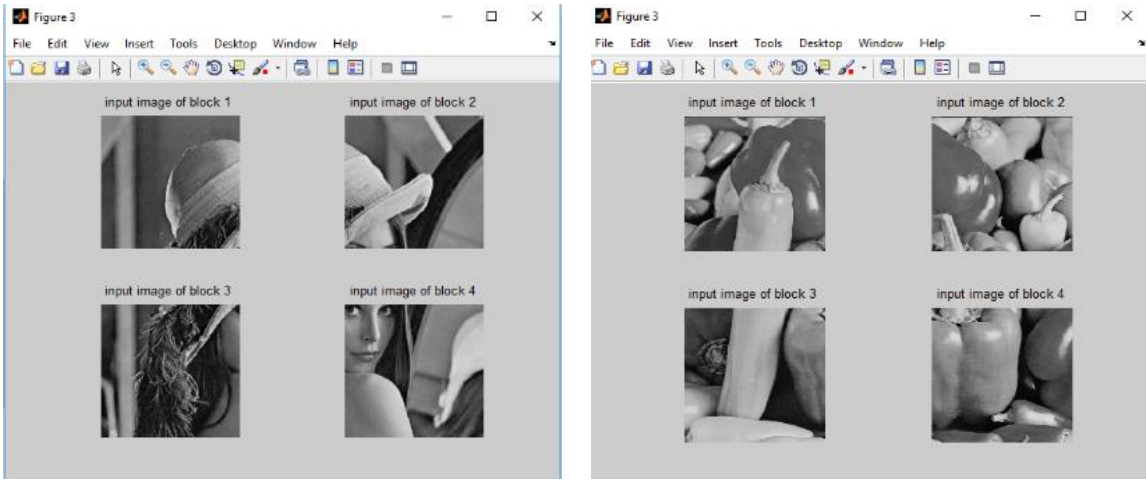

Figure 2. Two examples of images showing divided into Four blocks

2.2. RSA algorithm

RSA is a public-key encryption algorithm. It is normally the method used to encrypt the data sent over web, It is a kind of algorithm that can be used for data encryption as well as digital signature. Very complicated maths make RSA algorithm [2] safe and secure for its users.Since RSA algorithm uses factorization of prime numbers,wich very tough,it is difficult to break. Moreover, the public key used for encrypting the data is known to every one and is easy to share. Since RSA use a pair of keys it is considered as asymmetric algorithm unlike triple DES. The result of RSA encryption proves that lot of processing power and time is required for attackers to break it. The results for RSA in one block for both Encryption and Decryption is shown in the Figure 3.

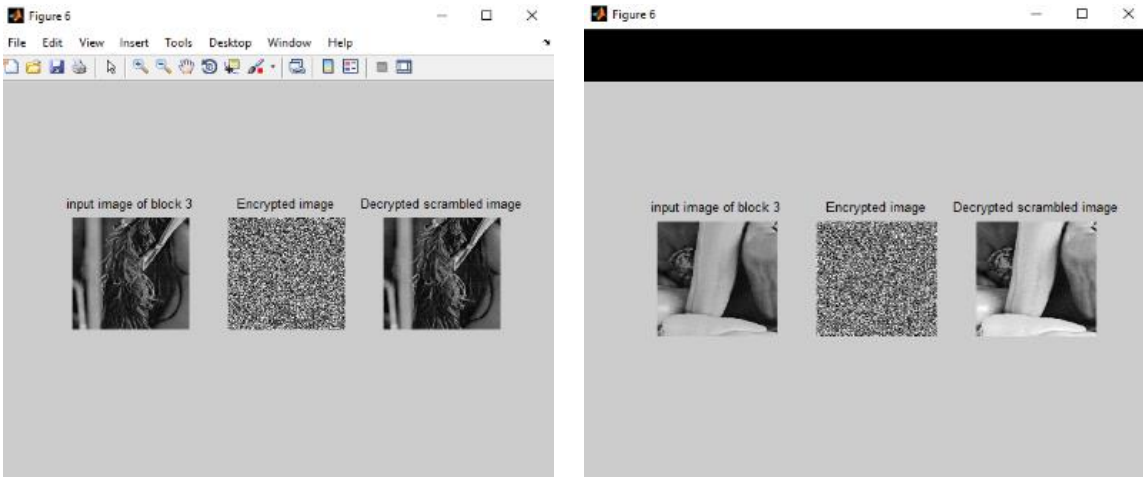

Figure 3. Results of RSA algorithm

2.3. DNA algorithm

Natural DNA sequence K1 is used to generate a frequency value and Arnold Cat Map [3, 4] is used to confuse the original image. Then, the other DNA sequence K2 is XORed creating a new image and three DNA templates accordingly [5]. The DNA template K3 is generated by the second DNA sequence after rotating K2 by 90º.Then, the DNA template K4 can be generated by further rotating K3 by 90º as shown in Figure 4. Four bases make up the grey value in this algorithm. Two binary digits are represented in one base ,in which A, G, C and T [6] are replaced by 00, 01, 10 and 11 by using DNA Digital Coding Technology [7, 8] for binary stream coding of the DNA sequences 0-255 is the range of gray value for any pixel, namely 00000000-11111111.The results of DNA Algorithm for two different images are mentioned in the Figure 5.

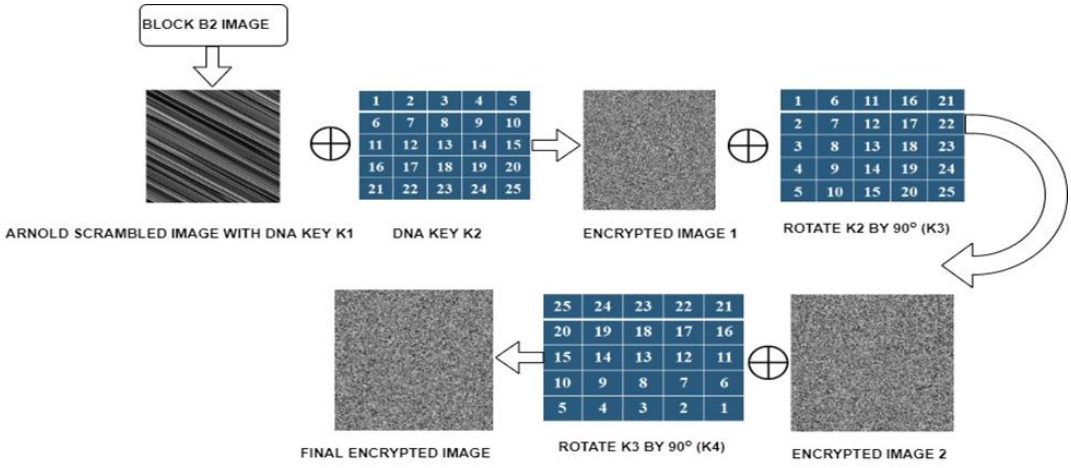

Figure 4. Block diagram of DNA Algorithm

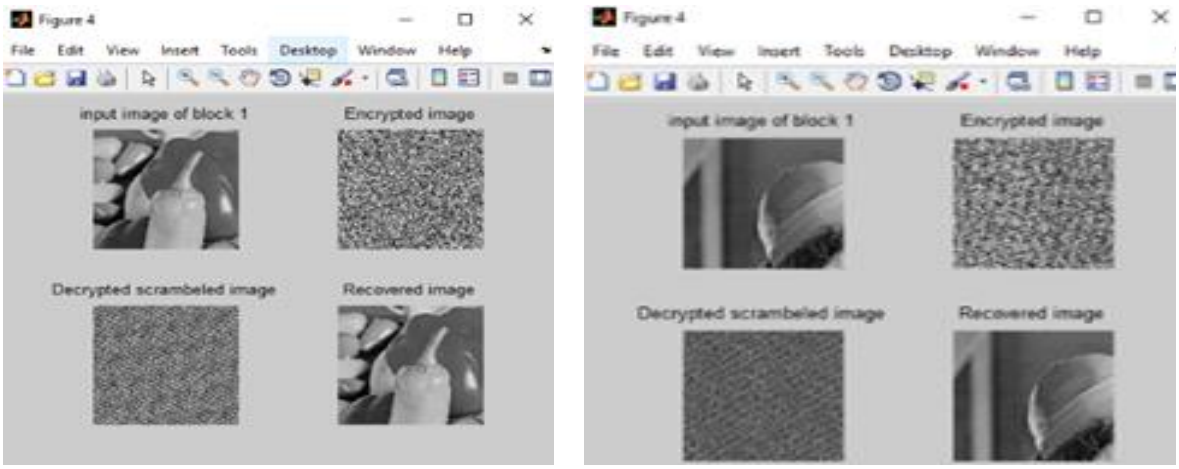

Figure 5. Results of DNA algorithm

2.4. DES algorithm

The Data Encryption Standard (DES) which is a symmetric block cipher was published by National Institute of Standards and Technology (NIST). It is an application of implementation of a Feistel Cipher [9], it uses 16 round Feistel structure and block size is 64-bit. 56 bits is the effective key length of DES, even though the key length is 64bit, since 8 of the 64 bits of the key are only used by the encryption algorithm as check bits only.S and P boxes makes up the DES function. The former transpose bits and latter substitute bits to generate a cipher. DES has proved to be a very well designed block cipher. No significant cryptanalytic attacks have been done on DES .The robustness of DES lies on two factors: The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. On such a number of keys, a brute force attack is impractical. Nobody has succeeded to find any weakness, even though cryptanalysis can be performed by exploiting the characteristic of DES algorithm.The results after applying DES Algorithm to Block B3 of two different input images are shown in Figure 6 .

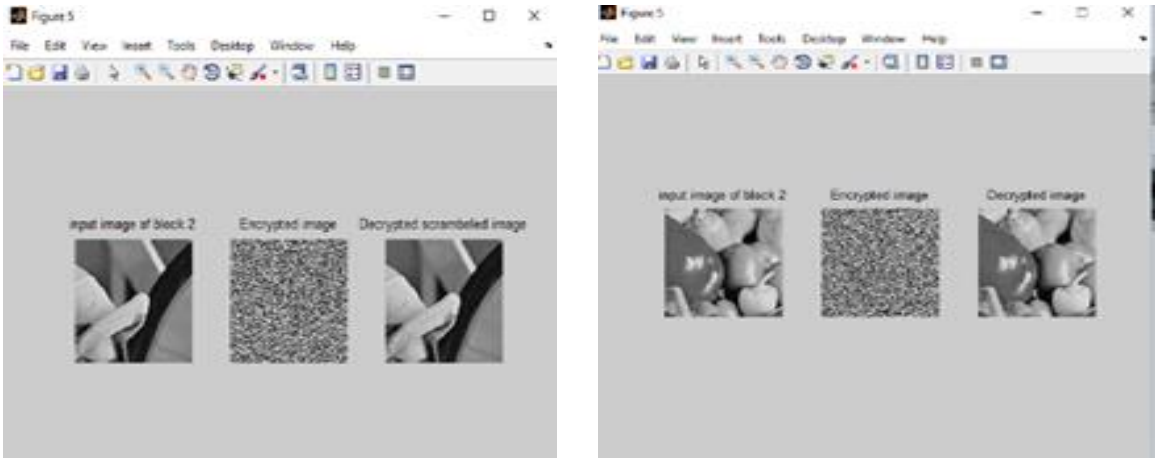

Figure 6. Results of DES algorithm

2.5. Chaos-based encryption algorithms

This Algorithm put forwards a substitute chaos-based digital image cryptosystem with three main features. First, the compound sine and cosine chaotic maps, is recommended through nonlinear dynamics analyses and is subsequently exploited as high-entropy random-bit sources for encryption. High degree of chaos is potentially offered over majority regions of the parameter spaces [10] by the Sine and cosine chaotic map. Second, to achieve faster encryption, prior to XOR operation, uncomplicated pixel shuffling and bit plane separations are used to performed image confusion and diffusion processes. Last, in order to enhance key space and key-sensitivity performances, for using as initial condition and control parameters the security key conversions from ASCII code to floating number are also presented.

Potentially rich dynamic behaviors as defined as [11] Xn+l=sin(axn) and Xn+l=cos(bxn), where the constants a and b are parameters associated with the frequencies of sine and cosine functions, respectively, have been offered by a section of trigonometric functions including sine and cosine maps [12, 13]. The chaotic regions is still not sufficient due to periodic characteristics, even though a high complexity in terms of nonlinear dynamics is offered by sine and cosine [14, 15]. Through the combination between sine and cosine maps the improvement of sine and cosine maps is given by,

$$X_{n+1} = \sin(axn) + \cos(bxn) \quad (1)$$

The two main groups of ASCII codes [16], ie Xm and Ym where m=1,2,3,…8,are made by the input security keys from users which is denoted in ASCII code with arbitrary 16 alphanumeric Character Defined as A=A1,A2,A3,A4,..AI6. Primary Conditions and the control parameters are set by using these groups. They will be converted into 48-bit binary representations denoted by BXI to BX48 and BY1 to BY48, respectively. Through binary representation the actual numbers RXm and RYm are consequently formed as shown below.

$$RYm = (B\,Y1 \times 20 + B\,Y2 \times 21 + \ldots\ldots + B\,Y48 \times 247)/248 \quad (2)$$

$$RXm = (B\,X1 \times 20 + B\,X2 \times 21 + \ldots\ldots + B\,X48 \times 247)/248 \quad (3)$$

The initial conditions and the control parameters as a result can be achieved by

$$am = (RXm \times RYm) \bmod 1 \quad (4)$$

$$bm = (RYm \times RYm+1) \bmod 1 \quad (5)$$

Figure 7 shows the proposed encryption and decryption algorithms using compound sine and cosine maps.

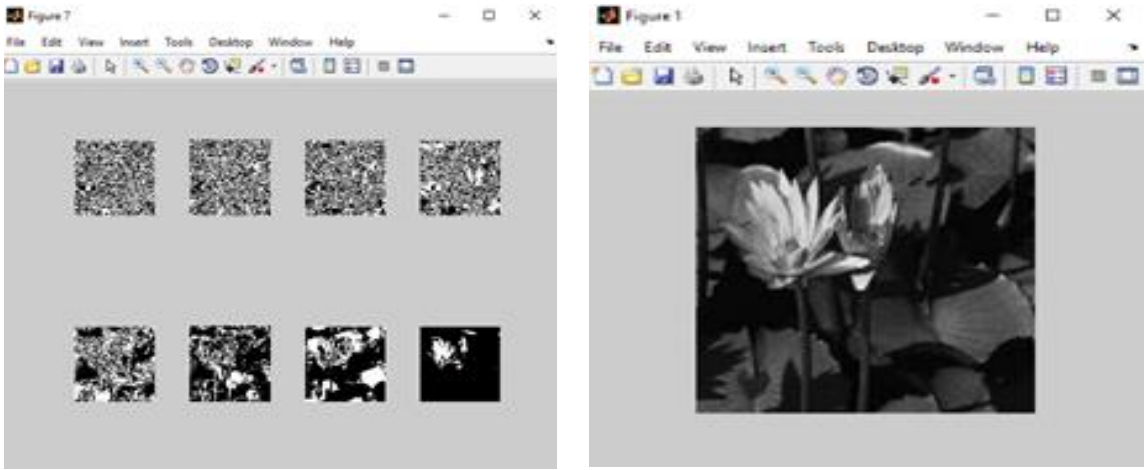

Figure 7. Results of CHAOS-BASED algorithm

2.6. Combined encrypted image

The Final Encrypted image is obtained after combining the results of all the four Algorithm. The result for combined encrypted image for two input images is shown in the Figure 8.

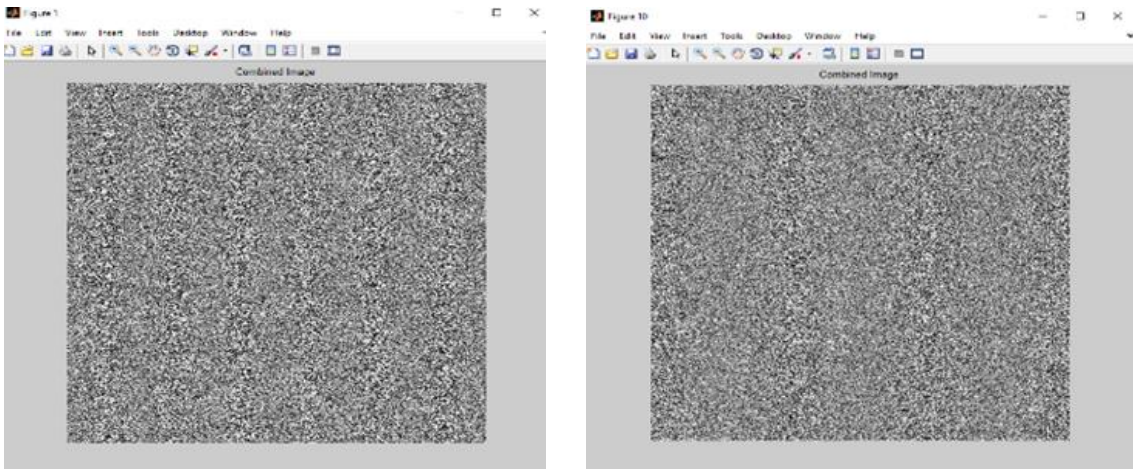

Figure 8. Results of combined image

3. EXPERIMENTAL RESULTS

3.1. Security analysis

Security analysis of the method is mandatory to ensure robustness of any cryptography technique. Below we illustrate some of the analysis of the implemented technique.

3.1.1. Histogram analysis

The frequency of each pixel in an image is depicted by a Histogram [17]. Uniformity in frequency distribution of the pixel values is essential for any secret image [18]. Figure 9 shows the histogram of the plain image and secret image respectively. The goodness of the cipher image is indicated from the image that, the frequency distribution of the plain image varies a lot compared to the secret image histogram which is evenly distributed.

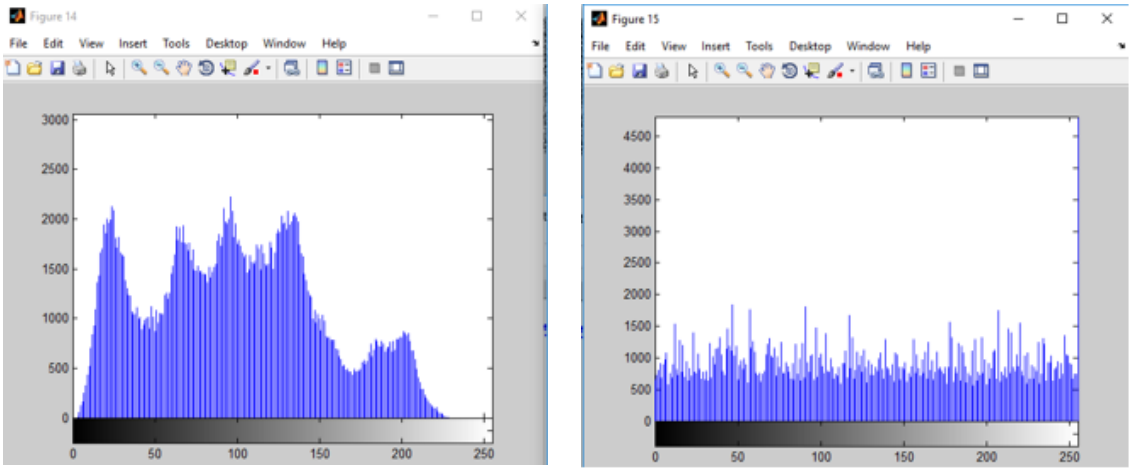

Figure 9. Histogram analysis of original image and encrypted image

3.1.2. Correlation analysis

Very high correlation in pixel values with their neighboring pixel values are observed is Normal images that we see every day. Very low Correlation [19] to its neighbor pixel value should be very low for a good cipher image. 3000 pixel values were randomly chosen from the input image and was plotted against the neighboring pixel values in vertical, diagonal and horizontal direction as shown in Figure 10. It is evident from the figure that, pixel plot of the cipher image is spread everywhere compared to that of the original image. This figure signifies the Confusion and diffusion property required for a cipher image. In Table 1, correlation coefficient color channel of plane image and cipher image along horizontal, vertical and diagonal direction is given.

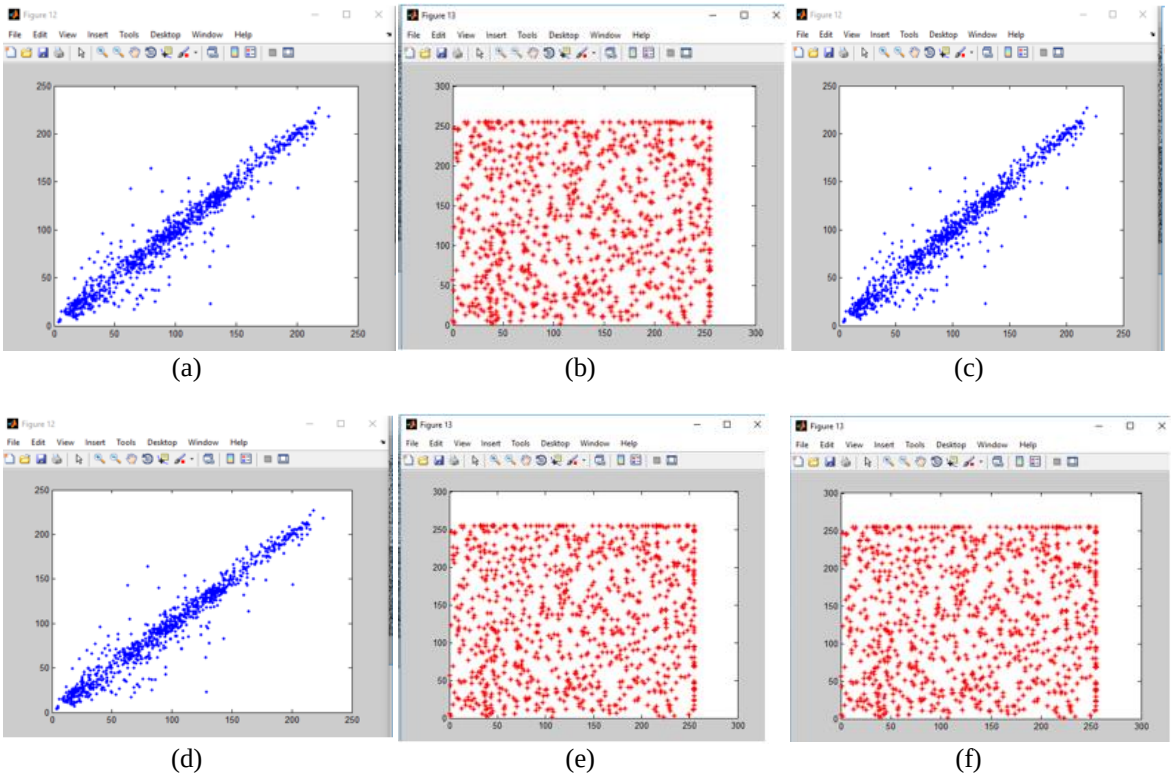

Figure 10. (a) Correlations of two horizontal adjacent pixels of original image and (b) Encrypted image. (c) Correlations of two Vertical adjacent pixels of original image and (d) Encrypted image. Correlations of two diagonal adjacent pixels of (e) original image and (f) Encrypted image

Table 1. Security Analysis Results

Sl No	Image Name	Size	NPCR	UACI	Correlation	PSNR	Mean square error	SC
1	Lena.bmp	256X256	98.6	33.1	-0.04	7.959	1.04e+4	1
2	Flower.jpg	260X394	98.5	32.9	-0.002	6.86	1.33Xe+4	1
3	Girl.jpg	480X640	98.73	33.2	-0.063	7.12	1.26e+4	1
4	Peper.jpg	512X512	98.7	33.2	-0.041	8.45	9.285e+3	1
5	Hat.jpg	256X256	98.74	33.4	-0.00084	8.374	9.491e+3	1
6	Bird.jpg	256X256	98.519	32.8	0.055	8.66	8.8464e+03	1
7	Fruit.jpg	256X256	98.5897	33.7	0.069082	8.1626	9.9270e+03	1
8	Dog.jpg	429x500	98.6126	33.4	0.069948	7.3502	1.1969e+04	1
9	Baboon.jpg	256X256	98.7534	33.3	0.012153	9.1002	7.9994e+03	1
10	Puppy.jpg	429x500	98.7442	33.6	0.0034558	9.0539	8.0851e+03	1

3.1.3. NPCR

The number of pixels change rate (NPCR) [20, 21] is used to how the change of a single pixel in the original image affects the encrypted image with the proposed algorithm distinctly. Different pixel number percentage between the two images is measured by NPCR. The NPCR [22, 23] is calculated as follows:

$$NPCR = \frac{(1-\sum_{ij} D(i,j))}{wh} \times 100\% \quad (6)$$

Where D(i,j) denotes a two-dimensional array. C1(i,j) and C2(i,j) are the two encrypted images of the same original image with two different keys, D(i,j)=1 for C1(i,j)= C2(i,j),and D(i,j)=0 when C1(i,j) ≠ C2(i,j). Results of NPCR for the proposed scheme is given in Table 1. NPCR is over 99%. It implies with respect to small changes in keys the proposed encryption scheme is very sensitive.

3.1.4. UACI

The difference in average intensity between the plain and secret image [24], is measured by unified average changing intensity (UACI). Sensitivity of the scheme of encryption to minute changes in the input image is 0.01% as evident from results obtained from NPCR [25, 26]. The rate influence due to change of one pixel is very low as shown in UACI. Estimation result. The results proves only a negligible change in the secret image is brought by a swift change in original image. Resistivity of the proposed algorithm against a differential image is proved.

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M \times N} \frac{|ca_i - cb_i|}{255} \quad (7)$$

Where Cai and Cbi are the ith pixels of the cipher image

3.1.5. Structural similiarity

SSIM Image degradation is considered as a perceived Change in structural information in SSIM, which is a perception-based model. The Structural Similarity (SSIM) Index quality assessment index is based on the computation of three terms, namely the luminance term, the contrast term and the structural term. The overall index is a multiplicative combination of the three terms

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_X^2 + \sigma_y^2 + C_2)} \quad (8)$$

Where μ_x denotes the Average of x, μ_y denotes the Average of y,$\sigma 2X$ denotes the Variance of x, $\sigma 2y$ represents the Variance of y, σ_{xy} represents the Covariance of x and y

3.1.5. MSE and PSNR

PSNR [27, 28] (Peak Signal-to-Noise Ratio) is often introduced to quantitatively evaluate the similarity between two images in digital image processing applications. Mathematically, measurement of quality of compressed image against originalis defined as PSNR, with a higher value signifying better quality. Mean squared error is calculated first before computing PSNR, using the following equation:

$$MSE = \frac{\sum_{i=1}\sum_{j=1} (G'(i,j) - G(i,j))^2}{W \times H} \quad (9)$$

$$PSNR = 20 \log_{10} \frac{(255)}{\sqrt{MSE}} \quad (10)$$

4. CONCLUSION

Encrypting / decrypting technique and Including digital signature and inclusion of digital signature to the cipher image is presented in this paper. The aim is to provide integrity and authenticity to the output image. The results of the Security Analysis for 10 different images of the proposed algorithm are very close to the optimal value.

REFERENCES

[1] Li, S.; Chen, G.; Zheng, X. "*Chaos-based encryption for digital images and videos,"* In Multimedia Security Handbook; Furht, B.,Kirovski, D., Eds.; CRC Press: Boca Raton, FL, USA, pp.133–167, 2004.

[2] Odeh, A., K. Elleithy, M. Alshowkan, and E. Abdelfattah, "Quantum key distribution by using public key algorithm (RSA)," *IEEE*, 2013.

[3] Zhang Y, He L, Fu B. "Research on DNA cryptography. In: Applied cryptography and network security," p. 357, 2012.
[4] WeiX, GuoL , ZhangQ, ZhangJ, LianS, "A novel color image encryption algorithm based on DNA sequence operation and hyper chaotic system," J SystSoftw, 85:290–9, 2012.
[5] Shima Ramesh Maniyath, Thani kaiselvan V," A Novel DNA based Encryption Algorithm for Multimedia information" *COMPUSOFT, An international journal of advanced computer technology*, 5 (1), Volume-V, Issue-I, ISSN:2320-0790, January 2016.
[6] S. Kayalvizhi, S. Malarvizhi , "A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operations," *Multimedia Tools and Applications*, April 2019.
[7] Heping Wen, Simin Yu, Jinhu Lü, "Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos," MDPI, Entropy 2019, 21, 246; doi: 10.3390/e21030246
[8] Shima Ramesh Maniyath,Thanikaiselvan .V, *"Robust & Lightweight Image Encryption Approach using Public Key Cryptosystem," Springer International Publishing AG, CSOC 2018, AISC 765*, pp. 63–73, 2019.
[9] Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security," *International Journal of Scientific & Engineering Research*, Volume 4, Issue 7, July-2013.
[10] S. Maksuanpan, T. Veerawadtanapong, w. San-Urn, "Robust Digital Image Cryptosystem Based on Nonlinear Dynamics of Compound Sine and Cosine," *ICACT 2013*, January 2013.
[11] Shuliang Sun , Yongning Guo, Ruikun Wu, "A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping," *IEEE Access*, Vol. 7, 2019.
[12] G. Lee and N. H. Farhat "Parametrically Coupled Sine Map Networks," *Electrical Engineering Department*, University of Pennsylvania, Philadelphia, PA, USA, 15 December 2000.
[13] Y.B. Mao, G. Chen, S.G. Lian, "A novel fast image encryption Scheme based on the 3D chaotic baker map," *Int. J.Bifurcat Chaos*, Vol. 14, No. 10, pp.3613–3624, 2004.
[14] Swapnil Shrivastava, "A Novel 2D Cat Map based Fast Data Encryption Scheme," *International Journal of Electronics and Communication Engineering*, ISSN 0974-2166 Volume 4, Number 2, pp. 217-223, 2011.
[15] Wei Feng and Yi-Gang He, "Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling," *IEEE Photonics Journal,·* Volume 10, Issue 6, Dec 2018.
[16] Priyanka Vora, Kranti Sonawane, Sneha Phulpagar, A.P.Ydav, "Data Security Using Colours and Armstrong Numbers," *International Journal of Electronics and Communication Engineering*, ISSN 0974-2166 Volume 9, Number 1, pp. 13-18, 2016.
[17] Wei Feng, Yigang He, Hongmin Li, Chunlai Li, "Cryptanalysis and Improvement of the Image Encryption Scheme Based on 2D Logistic-Adjusted-Sine Map," *IEEE Access*, volume 7, 2019.
[18] S. Liu, J. Sun, Z. Xu and J. Liu, "Analysis on an Image Encryption Algorithm," *2008 International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing*, Shanghai, pp. 803-806, 2008.
[19] Puneet Kaushik, Mohit Jain, Aman Jain, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm," *International Journal of Electronics and Communication Engineering*, ISSN 0974-2166 Volume 11, Number 1, pp. 31-37, (2018).
[20] Shima Ramesh Maniyath and R. Geetha, "ECC Encrypted Secure Reversible Data Hiding On Real Time Images With Enhanced Security" *ARPN Journal of Engineering and Applied Sciences*, Vol. 14, No. 15, August 2019.
[21] Wei Fenga, Yi-Gang Heb, Hong-Min Lic, Chun-Lai Li, "Cryptanalysis of the integrated chaotic systems based image encryption algorithm", *Optik - International Journal for Light and Electron Optics*, Vol. 186, Pages 449-457, 2019.
[22] Dhiraj P. Girase, "A Secure Smartphone Based Voting System with Modified EVM Using Elliptic Curve Cryptography," *International Journal of Electronics and Communication Engineering*, ISSN 0974-2166 Volume 8, Number 1, pp. 91-98, 2015.
[23] Sundararaman Rajagopalan, Shriramana Sharma, Sridevi Arumugham, Har Narayan Upadhyay, John Bosco Balaguru Rayappan, Rengarajan Amirtharajan, "YRBS coding with logistic map – a novel Sanskrit Aphorism and chaos for image encryption," *Multimedia Tools and Applications*, Volume 78, Issue 8, pp 10513–10541, April 2019,
[24] Rasul Enayatifar, Abdul Hanan Abdullah, Ismail Fauzi Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *ELSEVIER, Optics and Lasersin Engineering*, Vol. 56, pp. 83-93, 2014.
[25] Lu Xu, Xu Gou, Zhi Li∗, Jian Li, "A novel chaotic image encryption algorithm using block scrambling and Dynamic index based diffusion," *ELSEIVER Optics and Lasers in Engineering*, Vol. 91, pp. 41-52, 2017.
[26] Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System" *ELSEVIER Signal Processing*, Vol. 141, pp. 217-227, 2017.
[27] Elaheh Vaferi, Reza Sabbaghi-Nadooshan, "A new encryption algorithm for color images based on total chaoticshuffling scheme," *ELSEVIER, Optik*, Vol. 126, pp. 2474–2480, 2015.
[28] Miao Zhang, Xiaojun Tong, "Joint image encryption and compression scheme based on IWT and SPIHT," *ELSEVIER Optics and Lasers in Engineering*, Vol. 90, pp. 254–274, 2017.

BIOGRAPHIES OF AUTHORS

Shima Ramesh Maniyath, currently working as an Assistant professor in MVJ College of Engineering, Bangalore. I have completed my B.Tech in Electronics and Communication Engineering from Govt College of Engineering Kanuur, Kerala in the year 2009. Completed my Masters in Embedded System from Amrita Viswa Vidyapeedam, Bangalore in the year 2011. Registered my PhD in 2016 in Information Security from Vellore Institute of Technology, Vellore Under the Guidance of Dr. Prof Thanikaiselvan V

Dr. Thanikaiselvan V. received his Ph.D degree in the field of Information security form VIT university, Vellore, Tamilnadu, India, in the year 2014. He received M.Tech in Advanced Communication Systems from SASTRA University, Thanjavur, in 2006 and B.E in Electronics and Communication Engineering form Bharathidasan University, Trichy, in 2002. Currently he is working as HoD and Associate Professor in Department of Communication Engineering under the School of Electronics Engineering, VIT University, Vellore. His teaching and research interest includes Digital communication, Wireless communication, Digital signal and Image Processing, Wireless Sensor Networks and Information Security. So far he has published 50 research articles in peer reviewed Scopus indexed journals and 5 Scopus indexed conference papers. Currently he is guiding 4 Ph.D candidates in the areas of Information Security and Digital Image Processing. He has supervised more than 100 UG and PG projects.