Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

OPEN ACCESS Research Journal of Information Technology

ISSN 1815-7432
DOI: 10.3923/rjit.2017.25.31

Research Article
Revolving of Pixels and Bits in Pixels-Plan (E) Tary Encryption

[1]R. Anushiadevi, [2]Padmapriya Praveenkumar, [2]John Bosco Balaguru Rayappan and [2]Rengarajan Amirtharajan

[1]School of Computing,
[2]School of Electrical and Electronics Engineering, SASTRA University, 613 401 Thanjavur, India

Abstract

Background: In current years, numerous algorithms of image encryption were considered and developed through diffusion and confusion, to secure the image against hackers. **Materials and Methods:** In this study a novel idea is proposed to encrypt and decrypt an image. Here two levels of encryption are used. In the first level the plane encryption is done, due to this there will be an absolute changes in the bits of each plane and in the second level the pixel encryption is done because of this the pixel values are changed. All these things makes harder to decrypt the image by the hackers in the channel. **Results:** The number of pixel change rate (NPCR) and Unified Average Changing Intensity (UACI) values are calculated to test the randomness of the encrypted images. Horizontal, vertical and diagonal correlations are tested to find the relationship between two adjacent pixels. To compare the pixel distribution of original and encrypted image histograms are plotted. **Conclusion:** The statistical analysis of data obtained from the results based on the proposed technique can offer a greater quality of information transmission security.

Key words: Information security, image encryption, NPCR, UACI

Received: August 23, 2016 Accepted: November 25, 2016 Published: December 15, 2016

Citation: R. Anushiadevi, Padmapriya Praveenkumar, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2017. Revolving of pixels and bits in pixels-plan (E) tary encryption. Res. J. Inform. Technol., 9: 25-31.

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, 613 401 Thanjavur, India

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Transmission of highly confidential data in a secured way has become a matter of great concern in the current days. The modern technology has made it effortless for a third person to hack the information. This drawback has given birth to the idea of communication via images. There have been a lot of studies by researchers on image encryption and decryption. Plenty of methods have been evolved. Since the method of plane encryption and pixel encryption proves to furnish extremely accurate results, its relevance to image encryption and decryption is highly appreciated[1-5].

The image can be decomposed by several number of bit planes using decomposition techniques. Some of the decomposition techniques are gray code bit plane decomposition (GCBD), binary bit plane decomposition (BBD)[1] and fibonacci p-codes bit plane decomposition[2-4]. The images are divided into several bit planes in which any one bit plane can act as secret key and for encryption, XOR operation is performed between the secret key planes with all other planes[5].

Image encryption through confusion and diffusion is performed using Matrix Reordering (MR) and simple XOR operation[6-10]. Pixel level scrambling can be done by using simple XOR operation[7,8]. The image is divided into several number of vectors and the number varies based on the key value 'K' and XOR operation is done between two neighbouring vectors to achieve the diffusion and each vector bits are circularly rotated right to achieve confusion[8,9]. Bit level permutation is done by using chaotic map in order to encrypt the image[9-11]. Images are encrypted by using value transformation and random permutation[10,12]. Optical XOR operation is performed between bit plane and key data by polarization encoding technique[13].

Image positions are changed and non-linear substitution and diffusion are applied for each row of the image[14,15]. This substitution and diffusion are repeated for 3 times to create an encrypted image chaos theory and vigenère cipher is used[12,15-17]. Chaotic sequences created by chaos are arranged as Vigenère then pixel positions are scrambled based on chaotic sequences[11,12,14,17-20]. Simple classifications on Image encryption are pixel level[7], plane level[8], matrix compressing[21-23] or chaotic sequences[24-27].

In pixel level and plane level encryption, the image data is encrypted using simple XOR and XNOR operations with high NPCR, UACI value[21-27]. Generally, the gray scale images are represented using 8 bits. In this study by using simple pixel and plane level encryption, a significant improvement can be achieved.

MATERIALS AND METHODS

Proposed scheme: Plane level encryption and pixel level encryption have been implemented in this proposed scheme. The XOR and XNOR operations have been used to develop the encryption strategies[25,26]. This would ensure higher level of image security, since two levels of encryption techniques have been pursued. The experiment has been performed with the standard gray scale images, "Lena", "Cameraman", "Pepper" and "Baboon" of the same size.

Plane level encryption: In this encryption scheme, MSB and LSB planes are encrypted separately as shown in Fig. 1a and 1b, respectively. The plane level encryption algorithm is given. Here confusion and diffusion can be achieved with help of alternate XOR and XNOR operation.

Algorithm 1:

1: Initialize 'n' value as 8
2: If $|n-7|$ is odd
  2.1: n^{th} plane = n^{th} plane $\oplus$ $|n-7|^{th}$ plane
3: Else
  3.1: n^{th} plane = n^{th} plane XNOR $|n-7|^{th}$ plane
4: n = n-1
5: go to step 2 if 'n' value is not equal to 4
6: if 'n' is odd
  6.1: n^{th} plane = n^{th} plane $\oplus$ $|n+4|^{th}$ plane
7: Else
  7.1: n^{th} plane = n^{th} plane XNOR $|n+4|^{th}$ plane
8: n = n-1
9: go to step 7 if 'n' value is not equal to 0

Pixel level encryption: In the pixel level encryption scheme, the data bits of each pixel in the image is encrypted using data bits of other pixels in the image. The image is divided into two

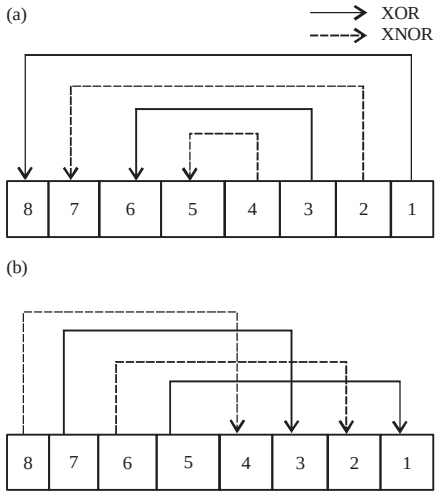

Fig. 1(a-b): Encrypting the (a) MSB plane and (b) LSB plane

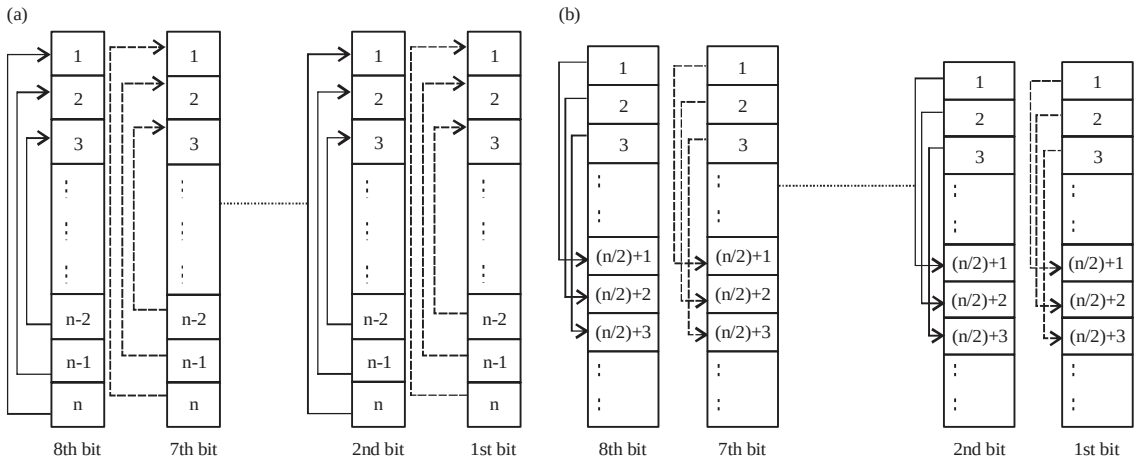

Fig. 2(a-b): (a) First half pixel's encryption and (b) Second half pixel's encryption

half's where the first and second half are encrypted separately as shown in Fig. 2a and b, respectively. Here the XOR operation is performed on even bits of pixels and XNOR operation is performed on odd bits of pixels. The pixel level encryption is given.

Algorithm 2:

1: convert each pixel into binary form
2: initialize k as 8
3: initialize 'n' value as total number of pixels 'm' value as 1
4: if k is even
  4.1: m^{th} pixel k^{th} bit = n^{th} pixel k^{th} bit $\oplus$ m^{th} pixel k^{th} bit
5: Else
  5.1: m^{th} pixel k^{th} bit = n^{th} pixel k^{th} bit XNOR m^{th} pixel k^{th} bit
6: m = m+1
7: n = n-1
8: go to step 4 if 'm' value and 'n' value are not equal
9: k = k-1
10: go to step 3 if k value is not equal to zero
11: initialize k as 8
12: initialize 'n' value as 1, 'm' value as (total number of pixels/2)
13: if k is even
  13.1: m^{th} pixel k^{th} bit = n^{th} pixel k^{th} bit $\oplus$ m^{th} pixel k^{th} bit
14: Else
  14.1: m^{th} pixel k^{th} bit = n^{th} pixel k^{th} bit XNOR m^{th} pixel k^{th} bit
15: m = m+1
16: n = n+1
17: go to step 13 if 'n' value are not equal to total number of pixels
18: k = k-1
19: go to step 12 if k value is not equal to zero

RESULTS AND DISCUSSION

The proposed method was simulated using jdk 1.6. The 256×256 lena image is given in Fig. 3a and its histogram is given in Fig. 3b. After first level encryption the encrypted lena image is given in Fig. 4a and its corresponding histogram is given in Fig. 4b. After second level, the encrypted lena image and its corresponding histogram are shown in Fig. 5a and 5b, respectively.

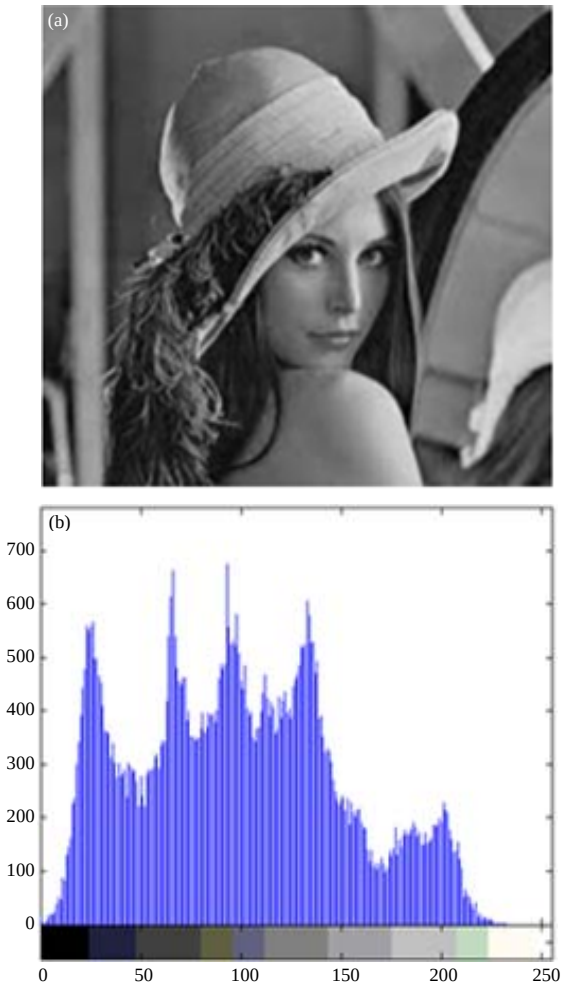

Fig. 3(a-b): (a) Lena image and (b) Histogram of Lena image

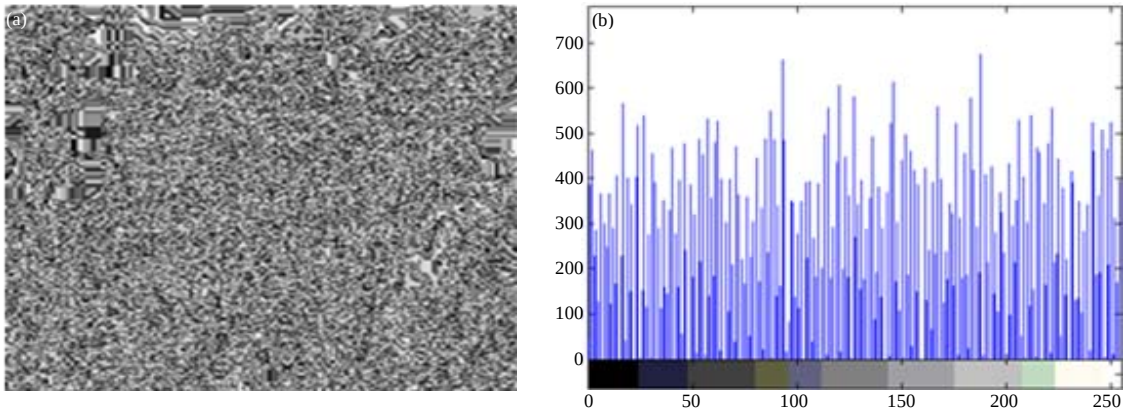

Fig. 4(a-b): (a) First level encrypted Lena and (b) Histogram of first level encrypted Lena

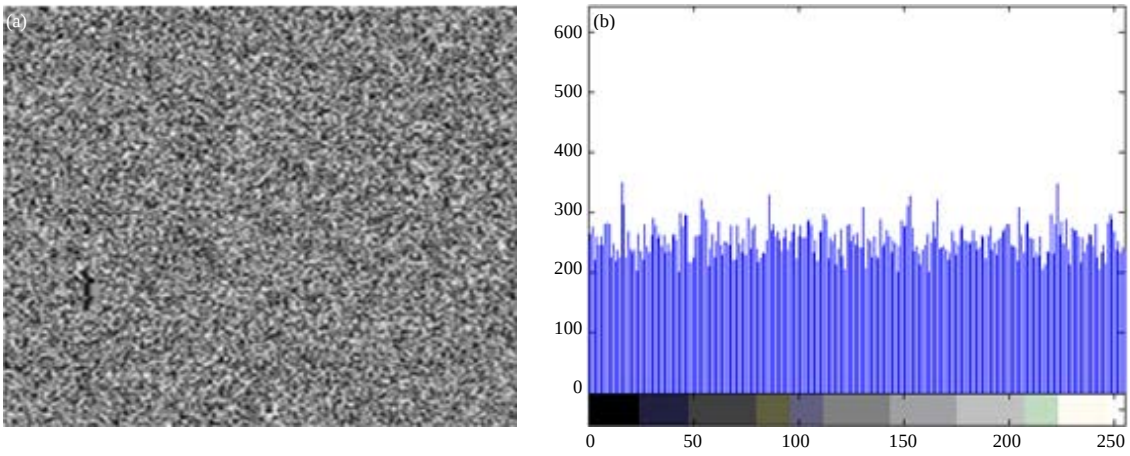

Fig. 5(a-b): (a) Second level encrypted Lena and (b) Histogram of second level encrypted Lena

Table 1: Comparison of correlation with the previous studies

Algorithm	HC	VC	DC
Proposed method	0.0091	0.0142	0.0150
Sankaran and Krishna[19]	0.0052	0.0539	0.1141
Paul *et al.*[23]	0.0056	0.0920	0.0749

Table 2: Comparison of NPCR with the previous studies

Algorithm	NPCR
Proposed method	99.6246
Zhou *et al.*[16]	99.5860
Huang *et al.*[17]	99.5780
Diaconu and Loukhaoukha[27]	99.6078

In the proposed method the correlation between pixels for encrypted lena image is better than[19,23] as given in Table 1.

The NPCR is for lena image good when comparing to the other algorithms[16,17,27] and it is shown in Table 2.

The 256×256 cameraman image is given in Fig. 6a and its histogram in Fig. 6d. After first level encryption the encrypted cameraman image and its corresponding histogram is given in Fig. 6b and e, respectively. The second level encrypted cameraman image and its corresponding histogram is given in the Fig. 6c and f, respectively.

The 256×256 pepper image is given in Fig. 7a and its histogram in Fig. 7d. After first level encryption the encrypted pepper image and its corresponding histogram is given in Fig. 7b and e, respectively. The second level encrypted pepper image and its corresponding histogram is given in the Fig. 7c and f, respectively.

The 256×256 baboon image is given in Fig. 8a and its histogram in Fig. 8d. After first level encryption the encrypted baboon image and its corresponding histogram is given in Fig. 8b and e, respectively. The second level encrypted baboon image and its corresponding histogram is given in the Fig. 8c and f, respectively.

Table 3 provides the NPCR, UACI and correlation values of the proposed scheme for different images when comparing to the other algorithms[20-22].

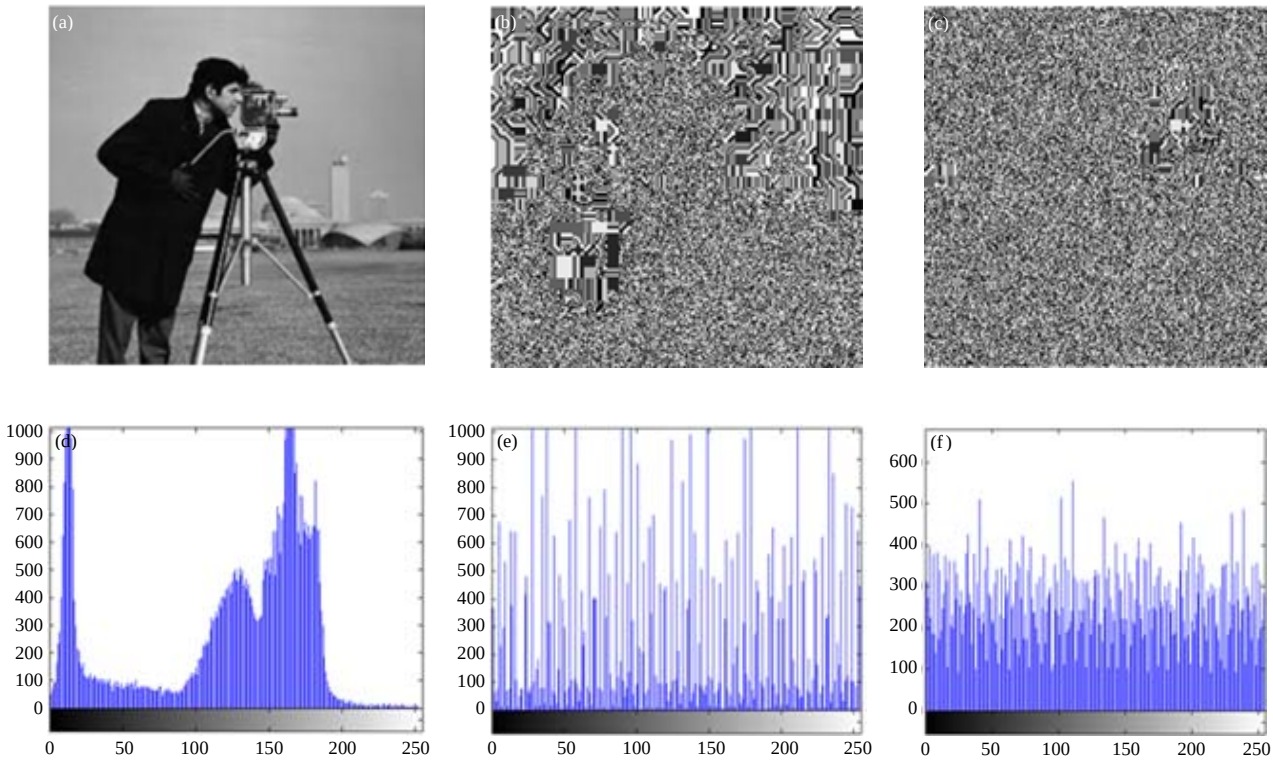

Fig. 6(a-f): (a) Cameraman image, (b) Encrypted image after level 1, (c) Encrypted image after level 2, (d) Histogram of cameraman, (e) Histogram after level 1 and (f) Histogram after level 2

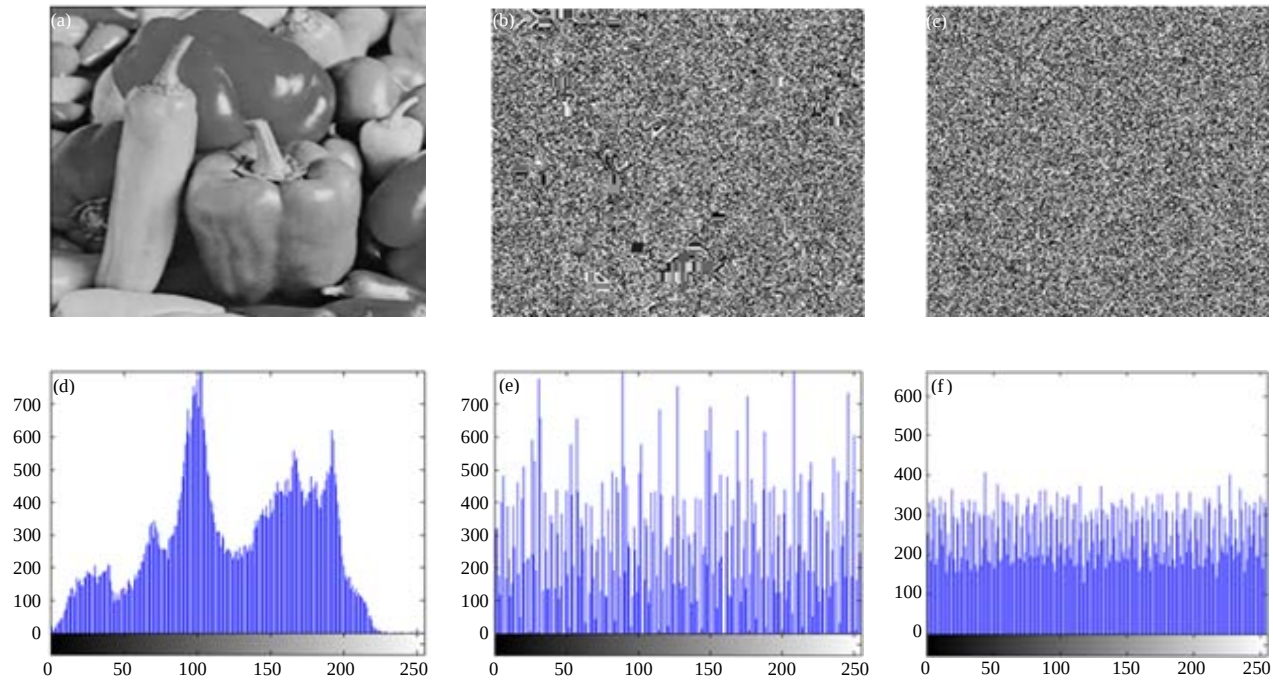

Fig. 7(a-f): (a) Pepper image, (b) Encrypted image after level 1, (c) Encrypted image after level 2, (d) Histogram of pepper, (e) Histogram after level 1 and (f) Histogram after level 2

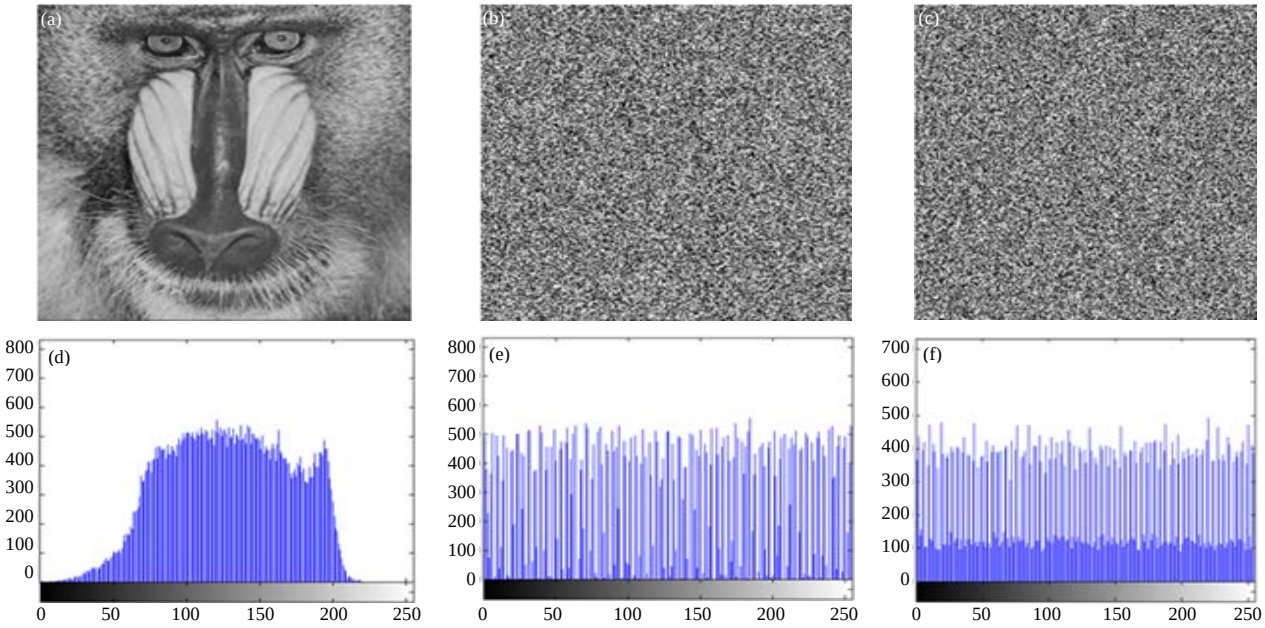

Fig. 8(a-f): (a) Baboon image, (b) Encrypted image after level 1, (c) Encrypted image after level 2, (d) Histogram of baboon, (e) Histogram after level 1 and (f) Histogram after level 2

Table 3: NPCR, UACI and correlation values of proposed scheme

Image	NPCR	UACI	HC	VC	DC
Proposed Lena	99.6246	30.2119	0.0091	0.0142	0.0150
Zhou *et al.*[21] (Lena)	-	-	0.0846	0.0583	0.0931
Zhou *et al.*[22] (Lena)	-	-	0.0198	0.0141	0.0026
Proposed cameraman	99.6353	30.9294	0.0222	0.0337	0.0247
Proposed baboon	99.6216	27.6614	-1.2491e-04	7.0289e-04	0.0067
Proposed pepper	99.615	29.27	0.0060	0.0021	0.0119
Al-Hazaimeh *et al.*[20] (Pepper)	99.60	12.75	0.0520	0.0501	0.0504

CONCLUSION

An image-encryption scheme based on plane level and pixel level using XOR method is presented. The decryption is reverse method of encryption. The advantages and the necessity of the diffusion and confusion in this proposed scheme is demonstrated the simulation results shown is effective, robust and secure to encrypt and decrypt the images high security and computation complexity has been achieved due to the two level encryption process. In future, by using chaotic system can randomize the plane and pixel level encryption. This method is also applicable for colour images.

SIGNIFICANCE STATEMENTS

- A novel dual level image encryption algorithm is proposed
- Encryption at plane and pixel level is done as the first and second layer, respectively
- High security and computation complexity has been achieved

REFERENCES

1. Zhou, Y., K. Panetta, S. Agaian and C.L.P. Chen, 2013. (n, k, p)-Gray code for image systems. IEEE Trans. Cybernet., 43: 515-529.
2. Agaian, S., J. Astola, K. Egiazarian and P. Kuosmanen, 1995. Decompositional methods for stack filtering using Fibonacci p-codes. Signal Process., 41: 101-110.
3. Zhou, Y., K. Panetta, S. Agaian and C.L.P. Chen, 2012. Image encryption using P-Fibonacci transform and decomposition. Optics Commun., 285: 594-608.
4. Gevorkian, D.Z., K.O. Egiazarian, J.T. Astola and O. Vainio, 1995. Parallel algorithms and VLSI architectures for stack filtering using Fibonacci p-codes. IEEE Trans. Signal Process., 43: 286-295.
5. Zhou, Y., W. Cao and C.L.P. Chen, 2014. Image encryption using binary bitplane. Signal Process, 100: 197-207.

6. Sivakumar, T. and R. Venkatesan, 2013. A novel image encryption approach using matrix reordering. WSEAS Trans. Comput., 12: 407-418.
7. Hu, J. and F. Han, 2009. A pixel-based scrambling scheme for digital medical images protection. J. Network Comput. Appl., 32: 788-794.
8. Al-Husainy, M.A.F., 2012. A novel encryption method for image security. Int. J. Secur. Appl., 6: 1-8.
9. Liu, H. and X. Wang, 2011. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun., 284: 3895-3903.
10. Al-Khassaweneh, M. and S. Tawalbeh, 2013. A value transformation and random permutation-based coloured image encryption technique. Int. J. Inform. Comput. Secur., 5: 290-300.
11. Wen, C., Q. Wang, X. Liu and F. Huang, 2013. An image encryption algorithm based on scrambling and chaos. J. Inform. Comput. Sci., 10: 5725-5733.
12. Li, S., Y. Zhao, B. Qu and J. Wang, 2013. Image scrambling based on chaotic sequences and Veginere cipher. Multimedia Tools Applic., 66: 573-588.
13. Han, J.W., C.S. Park, D.H. Ryu and E.S. Kim, 1999. Optical image encryption based on XOR operations. Optical Eng., 38: 47-54.
14. Behnia, S., A. Akhshani, H. Mahmodi and A. Akhavan, 2008. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals, 35: 408-419.
15. Wong, K.W., B.S.H. Kwok and C.H. Yuen, 2009. An efficient diffusion approach for chaos-based image encryption. Chaos Solitons Fractals, 41: 2652-2663.
16. Zhou, X., J. Ma, W. Du and Y. Zhao, 2011. Ergodic matrix and hybrid-key based image cryptosystem. Int. J. Image Graphics Signal Process., 3: 1-9.
17. Huang, X., G. Ye and K.W. Wong, 2013. Chaotic image encryption algorithm based on circulant operation. Abstr. Applied Anal. 10.1155/2013/384067.
18. Zhao, H., H.X. Wang and J. Wang, 2011. An improved bit shuffling pixels-based image scrambling method. Optoelectron. Lett., 7: 74-76.
19. Sankaran, K.S. and B.V.S. Krishna, 2011. A new chaotic algorithm for image encryption and decryption of digital color images. Int. J. Inform. Educ. Technol., 1: 137-141.
20. Al-Hazaimeh, O.M., N. Alhindawi, S.M.A. Hayajneh and A. Almomani, 2014. HENON chaotic map-based new digital image encryption algorithm. MAGNT Res. Rep., 2: 261-266.
21. Zhou, N., A. Zhang, F. Zheng and L. Gong, 2014. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt. Laser Technol., 62: 152-160.
22. Zhou, N., A. Zhang, J. Wu, D. Pei and Y. Yang, 2014. Novel hybrid image compression-encryption algorithm based on compressive sensing. Optik-Int. J. Light Electron Opt., 125: 5075-5080.
23. Paul, A.J., P. Mythili and K.P. Jacob, 2011. Matrix based Cryptographic procedure for efficient image encryption. Proceedings of the IEEE Recent Advances in Intelligent Computational Systems, September 22-24, 2011, India, pp: 173-177.
24. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Medical data sheet in safe havens-a tri-layer cryptic solution. Comput. Biol. Med., 62: 264-276.
25. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Pixel scattering matrix formalism for image encryption-a key scheduled substitution and diffusion approach. AEU-Int. J. Electron. Commun., 69: 562-572.
26. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Triple chaotic image scrambling on RGB-a random image encryption approach. Secur. Commun. Networks, 8: 3335-3345.
27. Diaconu, A.V. and K. Loukhaoukha, 2013. An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. Math. Prob. Eng. 10.1155/2013/848392.