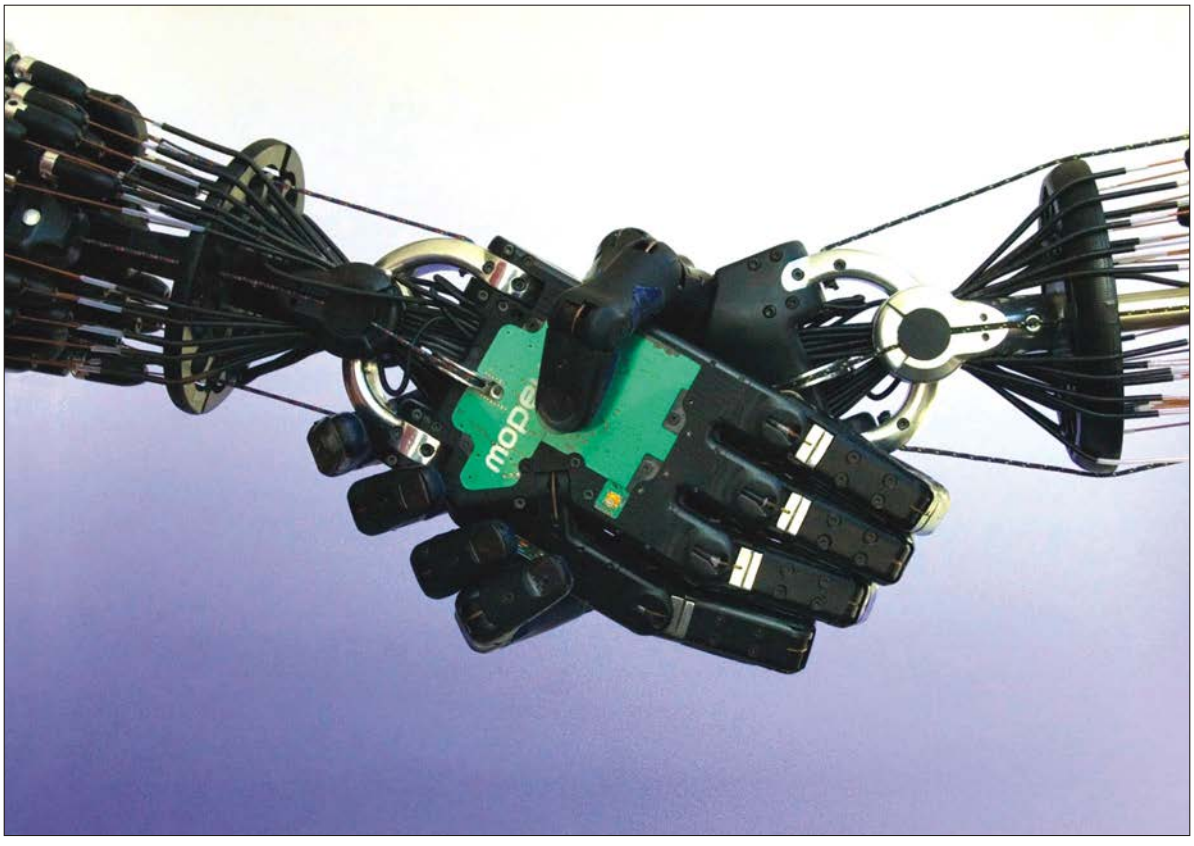

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 7 (3): 136-144, 2014
ISSN 1994-5450 / DOI: 10.3923/jai.2014.136.144

Why Information Security Demands Transform Domain, Compression and Encryption?

Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: Padmapriya Praveenkumar, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

With the advancement of technology and networking techniques, it is possible to transmit images at a lower bit rate and at the same time with high security. In order to fulfil the security needs of image transmission, several encryption, decryption and image encoding techniques have been put forward. The encryption discussed in this study is the PN (Pseudo Random Number) sequence based encryption using Joint Photographic Experts Group (JPEG) algorithm. In the proposed method, initially the image is portioned into blocks. Run length encoding is done for the level shifted image. Then Discrete Cosine Transform (DCT) and quantization was done and Difference of Quantized DC (DQDC) was calculated. Then the quantized blocks are shuffled based on the PN sequence and then the scrambled images are arranged in zigzag order. Then finally run length and Huffman lossless compression are done to eliminate the additional bits generated using PN codes. Metrics like correlation coefficient, Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR) were computed to prove the sternness of the proposed method.

Key words: Image encryption, information security, DQDC, PN sequence, UACI, NPCR

INTRODUCTION

With the increase in the usage of networking and internet for the usage of every possible thing, storing and transmission of data in a secured manner has become very inevitable (Praveenkumar *et al*., 2012a, b, 2013a-d, 2014a-n). Since it is possible for anyone to get an easy access to data, different techniques are used to reduce eavesdropping rate during the transmission. For this, we can use a major combination and collection of the present techniques (Amirtharajan and Rayappan, 2012a-c, 2013; Amirtharajan *et al*., 2013a-j) like Cryptography, Steganography and Watermarking.

Encryption of data at the transmission end and decryption at the receivers end ensures the safety of our data. Processing of image may not include very sensitive techniques as the change in the pixel contrast will not drastically change the entire message (Praveenkumar *et al*., 2014a, b; Rajagopalan *et al*., 2014e, f).

The original data is made unreadable by common man by secret key which helps in encrypting the message called as cipher image. Images convey more information than any written document. With improvement in network techniques, it has become possible to send and receive digital images via wireless communication.

Communication through free space makes it easy for anyone to interpret the transmitted data-wireless communication comes hand in hand with data security techniques (Praveenkumar *et al*., 2012a, b, 2013a-d, 2014a-n), technically known as information security methods like Cryptography (Praveenkumar *et al*., 2014a, b; Rajagopalan *et al*., 2014a-f), Steganography in spatial (Janakiraman *et al*., 2012, 2013, 2014) or transform domain (Ramalingam *et al*., 2014a, b; Rajagopalan *et al*., 2014a-d; Thanikaiselvan *et al*., 2012a-c, 2013a, b) and watermarking (Amirtharajan and Rayappan, 2013).

One of the security methods followed is the encryption of digital images (Borujeni and Eshghi, 2009; Loukhaoukha *et al*., 2012; Diaconu and Loukhaoukha, 2013). Carried out at the transmitter, encryption is the process of making the transmitted image unreadable to anyone, except the receiver, using a secret key or algorithm. It plays a vital role and it is maintained as a secret between the transmitter and receiver as anyone with the secret key or algorithm can decrypt the message. The encrypted image is called cipher image.

Encryption can be done by various methods (Borujeni and Eshghi, 2009; Loukhaoukha *et al*., 2012; Cheddad *et al*., 2010; Diaconu and Loukhaoukha, 2013; Praveenkumar *et al*., 2014a, b; Rajagopalan *et al*., 2014e, f). The most preferred methods are those which consume lesser time without compromising security. After an exhaustive literature survey, this study focuses on PN sequence based encryption along with JPEG and DCT.

MATERIALS AND METHODS

In this technique the working of the signal encryption as given in Fig. 1, goes as follows. The original data is made unreadable by common man by secret key which helps in encrypting the message called as cipher image. Here, PN sequence generation, using JPEG algorithm, is used for making the secret key. The image is divided into 8×8 block then the blocks are level shifted by a level of "2n-1", where, 2n is the maximum number of gray level.

Then it further undergoes Discrete Cosine Transform (DCT). After this, each block consist of 1 DC and 63 AC coefficients. Then the DC coefficients are quantized and difference between each block is taken and set as the new coefficient except for the first block which remains the same.

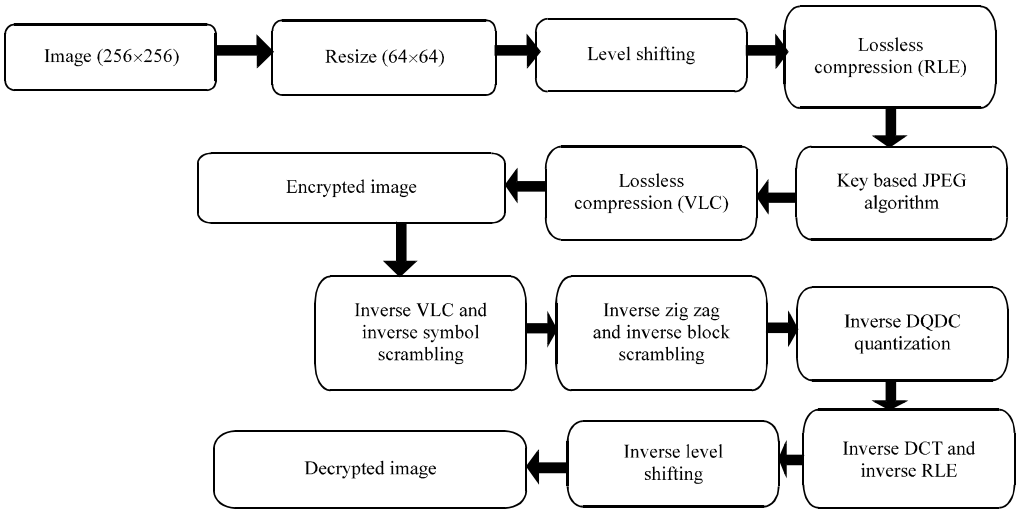

Fig. 1: Block diagram of the proposed scheme

Hence, the quantization results are now a relative one. Then the process of Run Length Encoding (RLE) is done to get rid of the zeroes which is a process that converts all the repeating values into a 2 byte value with the first byte contain the number of repetition and the second consists of the value repeated.

Another lossless technique, Huffman coding, can also be used for the same, in which each pixel is provided with a code of variable length. In addition to the JPEG algorithm, scrambling methods are also used to improve NPCR and UACI. This scrambling used can also be split in two-block scrambling (each position of 8×8 block is changed in accordance with PN sequence) and symbol scrambling (each pixel is changed according to the PN sequence generated).

Hence, this method helps us to encrypt the message which can be decrypted by knowing the key algorithm. The difficulty of eavesdropping is directly proportional to the complexity of the key algorithm we prepare. Hence, the data is secured.

RESULTS AND DISCUSSION

In the proposed scheme, 10 test images of size 256×256 were considered and implemented using MATLAB. The computed correlation coefficient, NPCR and UACI were estimated and compared with the available literature as given in Table 1. Figure 2a and b provides the original and level shifted camera man image, respectively.

Figure 3a, b and c denotes the 8×8 DCT terms, quantization matrix of Fig. 3a and the final rounded result of the first 8×8 matrix. Figure 4a and b provides the symbol and the block scrambled images, respectively.

Figure 5a and b provides the final encrypted image and its histogram, respectively. From the histogram it is revealed that uniform distribution of pixels escapes attacks from hackers:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} A(i,j)}{B \times C} \times 100$$

Table 1: Computed metrics of the proposed scheme

	Correlation coefficient				
Images	HC	VC	DC	NPCR	UACI
Cameraman	-0.0001	-0.0132	-0.0006	99.8047	37.4000
Peppers	-0.00009	-0.0014	-0.00054	99.7070	26.4711
Moon	-0.0089	-0.0090	-0.000054	98.8770	24.4031
Autumn	-0.1210	-0.1675	-0.1879	99.7314	37.6644
Board	-0.006478	-0.007	-0.01234	99.8779	32.1745
Shadow	-0.0769	-0.00121	-0.00012	99.9268	36.9001
Coins	-0.03609	-0.000023	-0.001210	99.8047	33.6296
Fabric	-0.6712	-0.1865	-0.00002	99.9023	30.9107
Pears	-0.654	-0.5098	-0.09091	99.9756	34.3795
Lena proposed	-0.001	-0.0023	-0.00012	99.7656	33.4675
Lena (Borujeni and Eshghi, 2009)	0.005	0.011	0.023	99.7	29.30
Lena (Loukhaoukha *et al*., 2012)	0.0068	0.0091	0.0063	99.5	28.62
Lena (Diaconu and Loukhaoukha, 2013)	0.0002	0.0006	0.0043	99.6	30.50

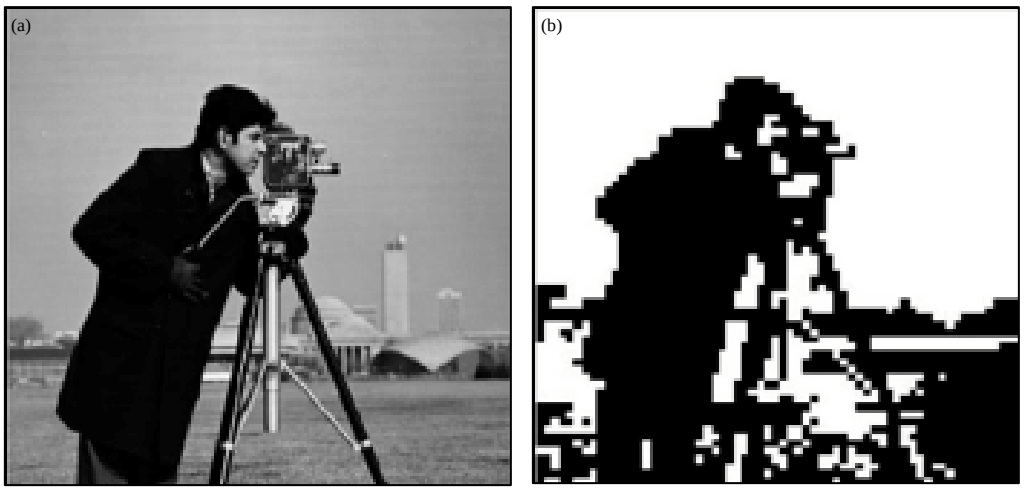

Fig. 2(a-b): (a) Original cameraman image and (b) Level shifted image of original cameraman

$$\begin{bmatrix} 313 & 56 & -27 & 18 & 78 & -60 & 27 & -27 \\ -38 & -27 & 13 & 44 & 32 & -1 & -24 & -10 \\ -20 & -17 & 10 & 33 & 21 & -6 & -16 & -9 \\ -10 & -8 & 9 & 17 & 9 & -10 & -13 & 1 \\ -6 & 1 & 6 & 4 & -3 & -7 & -5 & 5 \\ 2 & 3 & 0 & -3 & -7 & -4 & 0 & 3 \\ 4 & 4 & -1 & -2 & -9 & 0 & 2 & 4 \\ 3 & 1 & 0 & -4 & -2 & -1 & 3 & 1 \end{bmatrix} \div \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} = \begin{bmatrix} 20 & 5 & -313 & & & & & -210 \\ -3 & -2 & 1 & 2 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig. 3(a-c): (a) 8×8 DCT terms, (b) Quantization matrix of 8×8 DCT and (c) Final rounded result

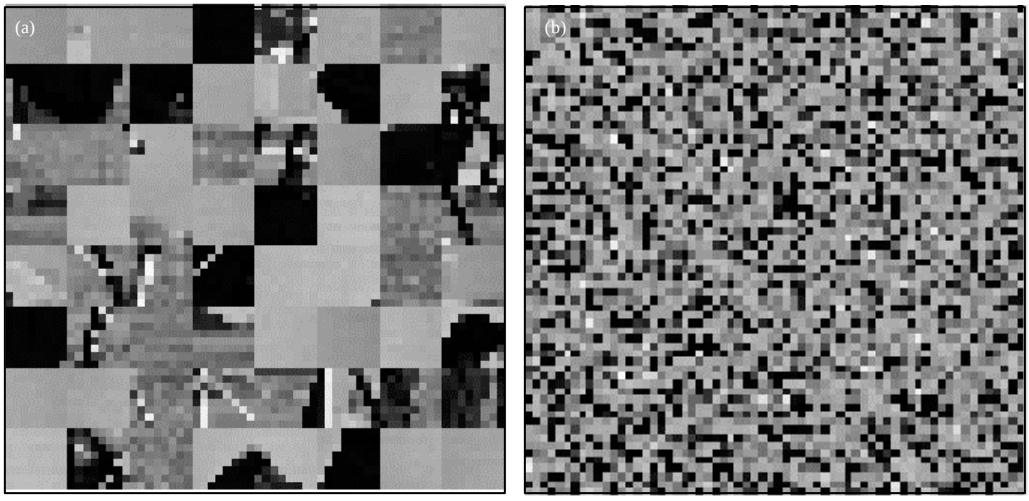

Fig. 4(a-b): (a) Block scrambled level shifted image of original cameraman and (b) Symbol scrambled block scrambled image of level shifted image of original cameraman

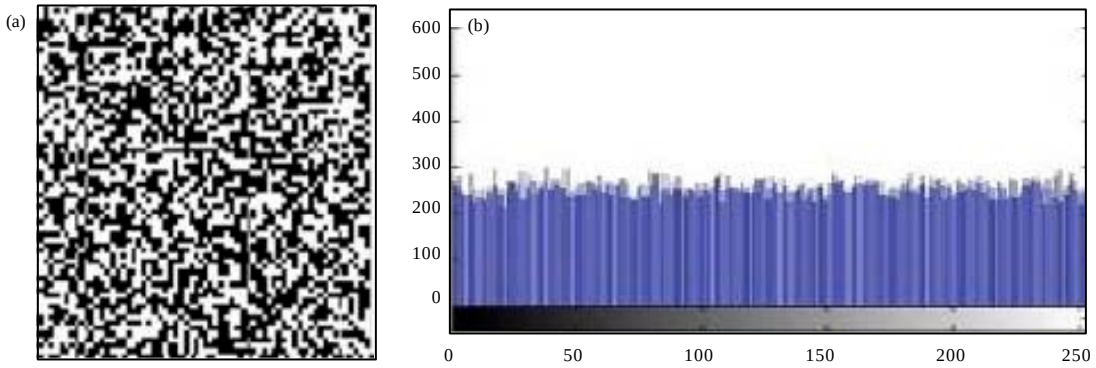

Fig. 5(a-b): (a) Final encrypted image and (b) Histogram of final encrypted image

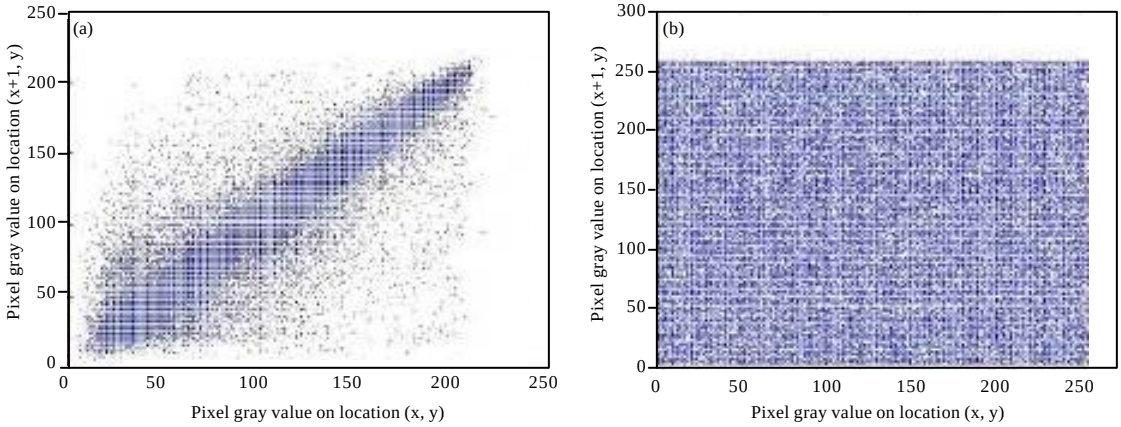

Fig. 6(a-b): Horizontal distribution of pixel of the, (a) Original image and (b) Encrypted image

where, B, C represents the rows and columns of the original and the encrypted images. If the entire pixel values in the original and the encrypted images are same then A(i, j) = 0 otherwise 1:

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{M}\frac{\text{mod}\,(x_1(i,\,j)-x_2(i,\,j))}{225}\right]\times\frac{100}{A\times B}$$

where, $x_1(i, j)$ and $x_2(i, j)$ represents the original and the encrypted images:

$$\text{Correlation coefficient} = \frac{n.\sum xy-\sum x\sum y}{\sqrt{\left(n\sum x^2-(\sum x)^2\right)\left(n\sum x^2-(\sum x)^2\right)}}$$

where, n denotes the pair of pixels and x, y represents the pixel values in the original and the encrypted images, respectively.

Figure 6a, 7a and 8a provides the pixel distribution along the horizontal, vertical and on diagonal basis of the original cameraman image. Figure 6b, 7b and 8b provides the pixel

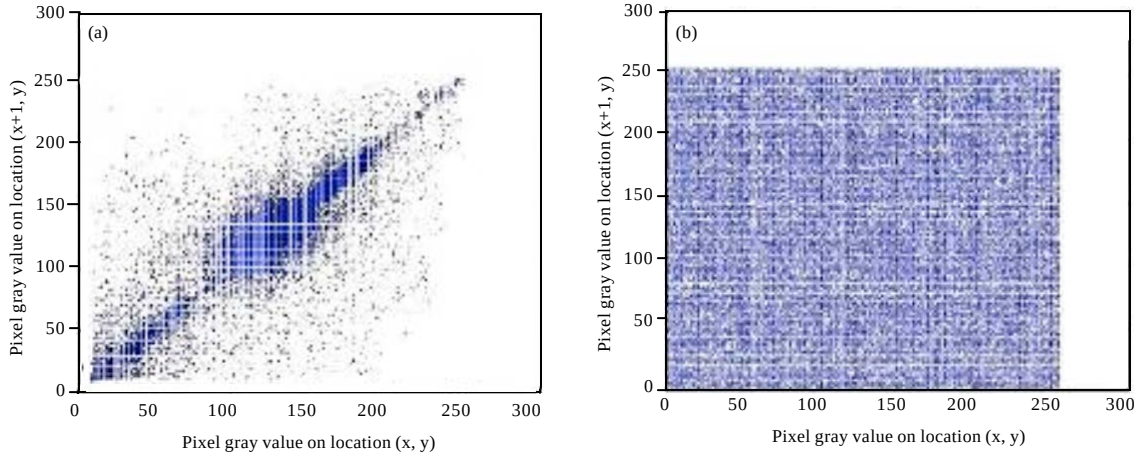

Fig. 7(a-b): Vertical distribution of pixel of the, (a) Original image and (b) Encrypted image

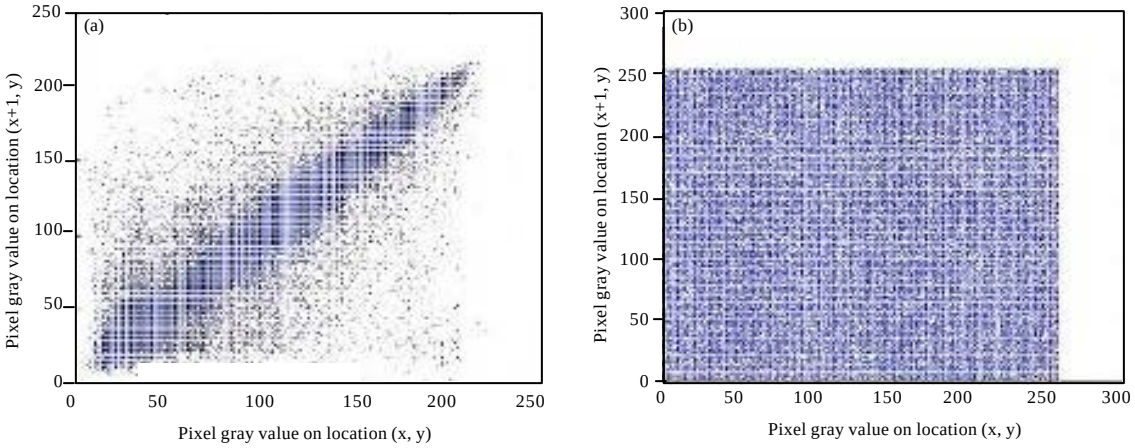

Fig. 8(a-b): Diagonal distribution of pixel of the (a) Original image and (b) Encrypted image

distribution along the horizontal, vertical and on diagonal basis of the encrypted cameraman image. From the uniform pixel distribution along the three axes reveals that unknown user cannot gain knowledge about the proposed scheme.

CONCLUSION

In the proposed scheme, encryption algorithm that uses PN sequence along with JPEG and DCT scrambling are utilized to enhance the security of the system multi-fold. Negative correlation coefficient, NPCR of 99.7 and UACI of 33.4 determines the firmness of estimated scheme and found to be better with the available literature. The future study can be extended to colour images and making use of digital watermarking and even can be extended by implementing selective quantization.

REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013a. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013b. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013c. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013e. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013f. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013g. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013h. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013i. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013j. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Borujeni, S.E. and M. Eshghi, 2009. Chaotic image encryption design using Tompkins-Paige algorithm. Math. Prob. Eng. 10.1155/2009/762652

Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. A hash-based image encryption algorithm. Opt. Commun., 283: 879-893.

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., Vol. 2013 10.1155/2013/848392

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., S. Rajagopalan, K. Thenmozhi, H.N. Upadhyay and J. Ramanathan *et al*., 2013. Captivating CODEC Stego (CCS): A cover on camouflage. Res. J. Inform. Technol., 5: 160-170.

Janakiraman, S., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014. Audio fingerprint indicator in embedded platform: A way for hardware steganography. J. Artif. Intell., 7: 82-93.

Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A secure image encryption algorithm based on Rubik's cube principle. J. Electr. Comput. Eng. 10.1155/2012/173931

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013a. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Convolution and viterbi EN (DE) coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013c. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013d. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhunisha, K. Thenmozhi and R. Amirtharajan, 2014a. Image Zoning→ encryption. Res. J. Inform. Technol., 6: 368-378.

Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan, 2014b. Rubik's cube blend with logistic map on RGB: A way for image encryption. Res. J. Inform. Technol., 6: 207-215.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014h. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014i. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014j. Coded crypted converted hiding (C^8H)-a stego channel. J. Applied Sci., 14: 1786-1797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014k. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014l. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Amirtharajan, R.S. Janani, K. Thenmozhi and J.B.B. Rayappan, 2014m. Multi (Carrier+Modulator) adaptive system: An anti fading stego approach. J. Applied Sci., 14: 1836-1843.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014n. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014a. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014d. Modeling combo PR generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

Rajagopalan, S., H.N. Upadhyay, J.B. Balaguru Rayappan and R. Amirtharajan, 2014e. Galois field proficient product for secure image encryption on FPGA. Res. J. Inform. Technol., 6: 308-324.

Rajagopalan, S., H.N. Upadhyay, J.B. Balaguru Rayappan and R. Amirtharajan, 2014f. Logic elements consumption analysis of cellular automata based image encryption on FPGA. Res. J. Inform. Technol., 6: 291-307.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inform. Syst. Software Applic., 270: 212-221.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013a. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013b. A graph theory practice on transformed image: A random image steganography. Sci. World J., Vol. 2013. 10.1155/2013/464107