Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (3): 223-236, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.223.236

Dual Cellular Automata on FPGA: An Image Encryptors Chip

Sundararaman Rajagopalan, Har Narayan Upadhyay, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

Corresponding Author: Sundararaman Rajagopalan, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

ABSTRACT

Secure data transmission plays a crucial role in today's world. While the data in the form of images are required extensively, the need to safeguard the original images has become inevitable. An image encryption based on the architecture of 14-bit and 8-bit cellular automata circuits has been proposed in this study. With the mighty pseudo randomness of two different cellular automata circuits, both shuffling and encryption operations were performed on grayscale images. The algorithm was implemented on Cyclone II EP2C35F672C6 FPGA. The proposed image encryption scheme on the reconfigurable hardware consumed a maximum of 11,675 logic elements (35% of total LEs) and 2,62,144 M4KRAM bits for encrypting the two grayscale secret images of size 128×128 that were stored in internal memory of the FPGA.

Key words: Cellular automata, FPGA based image encryption, information security

INTRODUCTION

The inventions of internet technology and subsequent improvements have shrunk the world of communication. The communication happens through a lot of mediums. Be it mobile phone as a carrier of information or social network as a medium of communicating one's personal thoughts, the development is phenomenal. While we are proud of the immense contribution of these items without which even our daily life would be difficult, there is also a concern regarding the extent with which the data sharing happens in a protected environment. Cryptography, steganography and watermarking have an important role in secure data transmission.

'Cryptography' is the process of scrambling the textual message so that it would be in a form that is very difficult to understand. Steganography (Amirtharajan and Rayappan, 2012a-d, 2013; Amirtharajan *et al.*, 2012, 2013a-j; Cheddad *et al.*, 2010; Janakiraman *et al.*, 2012a, b, 2014a, b; Luo *et al.*, 2011; Mohammad *et al.*, 2011; Salem *et al.*, 2011; Thien and Lin, 2003; Zhao and Luo, 2012) is information hiding science. 'Watermarking' is doing the job of copyright protection. 'Steganography' is being carried out in two domains namely spatial (Amirtharajan and Rayappan, 2012a-c; Chan and Cheng, 2004; Wu and Tsai, 2003; Janakiraman *et al.*, 2012a, b, 2013; Thanikaiselvan *et al.*, 2013b; Zhang and Wang, 2004) and Transform domains (Amirtharajan and Rayappan, 2012d; Qi and Wong, 2005; Thanikaiselvan *et al.*, 2012a-c, 2013a; Wong *et al.*, 2007).

Software as well as hardware based steganographic systems have been proposed in various earlier studies. As for as hardware based stego systems are concerned, FPGA (Rajagopalan *et al.*, 2012a, b, 2014a-d; Rajagopalan and Upadhyay, 2011; Janakiraman *et al.*, 2014a, b) and firmware (Janakiraman *et al.*, 2014b) based information hiding approaches have been reported. Towards implementing the security algorithms for wireless communication, OFDM based security approaches OFDM based information security (Praveenkumar *et al*., 2012a, b, 2013a, b, 2014a-j; Thenmozhi *et al*., 2012) have also been reported in earlier implementations.

Image encryption plays a pivotal role in the transmission of secret images of high importance. Various manipulations such as shuffling, complementing and other logical and arithmetic computations have been used for efficient encryption of images in different approaches. While most of the implementations which have been reported in the literature are software oriented, few more image encryption implementations have been carried out using FPGAs. The FPGA based image encryption methodologies were carried out on the grayscale images or RGB images that had been stored in internal or external memory of the FPGAs. The important advantage of FPGA based image encryption is that the specific bit stream and hardware are required for the proper retrieval of secret images.

FPGA offers multiple other benefits such as parallel processing, larger memories and high speed computation. The VLSI architecture of an efficient chaotic image encryption has been proposed in an earlier study (Yen and Guo, 2000; Azzaz *et al.,* 2009). An image and video encryption scheme based on SCAN algorithm have been implemented on Virtex XCV1000 FPGA (Dollas *et al*., 2003). Non-linear Cross-encryption Method for video images has been proposed in some of the approaches (JianBo *et al*., 2009). In another approach DCT based compression and encryption has been implemented on Virtex 5 FPGA (Jridi and Alfalou, 2010). A 2D cellular automata based image encryption algorithm has been implemented on Spartan 6 FPGA (Torres-Huitzil, 2013).

A dual cellular automata based image encryption on FPGA has been proposed in this study. The main advantage of this approach is that it employs a 14-bit Cellular Automata (CA) as a pixel position shuffler and 8-bit CA has been used to encrypt the secret pixel value. This approach provides complexity to the encryption by means of the possibilities to select 2^{14}-1 seed values which will dictate the encrypted image pixel order. The algorithm was implemented using Cyclone II EP2C35F672C6 FPGA. Internal M4KRAM was used to store the encrypted grayscale images of size 128×128.

METHODOLOGY

The proposed approach uses the pseudo randomness of cellular automata (Nandi *et al*., 1994) to scramble and encrypt the grayscale images. The Cellular Automata (CA) has a combination of cells (bits) whose next state will be decided by certain rules (Eslami *et al*., 2010; Wolfram, 1983). A maximum length sequence generating CA can be constructed by the combination of rules 90 and 150. For this approach, rules 90 and 150 have been employed in constructing the two CAs of 14-bit and 8-bit. The rules 90 and 150 are governed by the following Eq. 1-2:

$$R90 \rightarrow Si = S_{i-1} \oplus S_{i+1} \quad (1)$$

$$R150 \rightarrow Si = S_{i-1} \oplus S_{i} \oplus S_{i+1} \quad (2)$$

In the Eq. 1 and 2 S_i, S_{i-1} and S_{i+1} represent the states of present, previous and next cells. As per the rule 90 (R90), the present state of a cell is decided by the XOR operation between previous and next cell states and for rule 150 (R150), the present state of a cell will be decided by the XOR operation between present, previous and next cell states. At hardware level, these cell states can

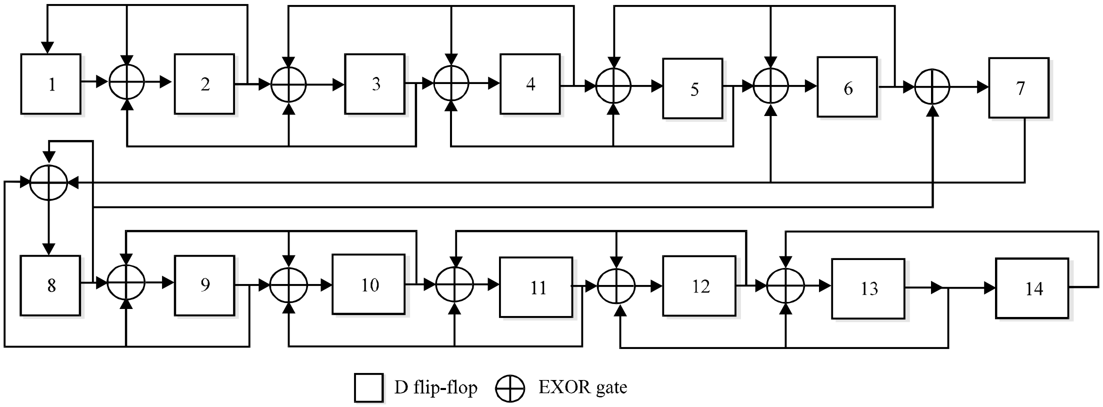


Fig. 1: 14-bit CA with R90-R150-R150-R150-R150-R150-R90- R150-R150-R150-R150-R150-R150-R90 pattern

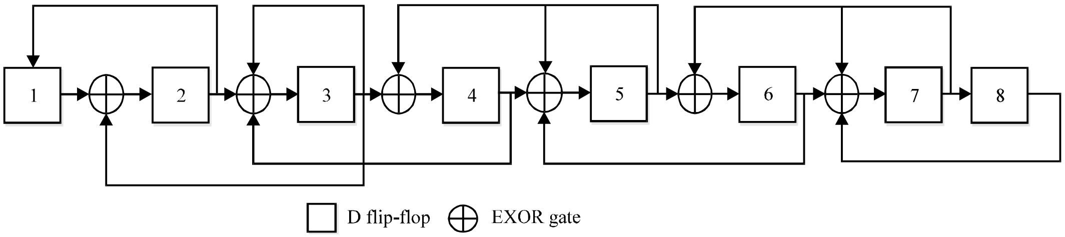


Fig. 2: 8-bit Cellular Automata with the combination R90-R90-R150-R90-R150-R90-R150-R90

modeled by a D-Flip Flop. Figure 1 shows the 14-bit CA which generates maximum length sequence. This 14-bit CA circuit has been constructed with the rule combination of R90-R150-R150-R150-R150-R150-R90-R150-R150-R150-R150-R150-R150-R90. The purpose of this CA is to scramble the order of pixels in the secret image by the order in which it generates the pseudorandom number. As the proposed approach uses 128×128 grayscale image for performing encryption, 14-bit CA has been used to generate 16383 pseudorandom numbers.

Apart from scrambling the image, the encryptions of the pixels were carried out using 8-bit CA which has been designed with the combination R90-R90-R150-R90-R150-R90-R150-R90. Figure 2 shows the 8-bit CA. During each clock cycle, two pseudorandom numbers were generated each with 14-bit CA and 8-bit CA. The 14-bit CA value decides the pixel value and 8-bit CA value has been used to perform encryption by means of XOR or XNOR operation with the selected secret pixel value.

The scrambling and encryption of the secret image of size 128×128 has been implemented on Cyclone II FPGA EP2C35F672C6. The image encryptors architecture on FPGA has used internal M4KRAM memory to store the encrypted images. Figure 3 shows the block diagram of the proposed image encryption system.

The images were stored and retrieved with the help of in system memory content editor of Quartus II 7.2 ISE version. This encryption approach was carried out on two 128×128 grayscale images. For the first image, XOR operation between pixel and 8-bit CA value was performed during encryption and for the second image XNOR operation was performed. The image scrambling order

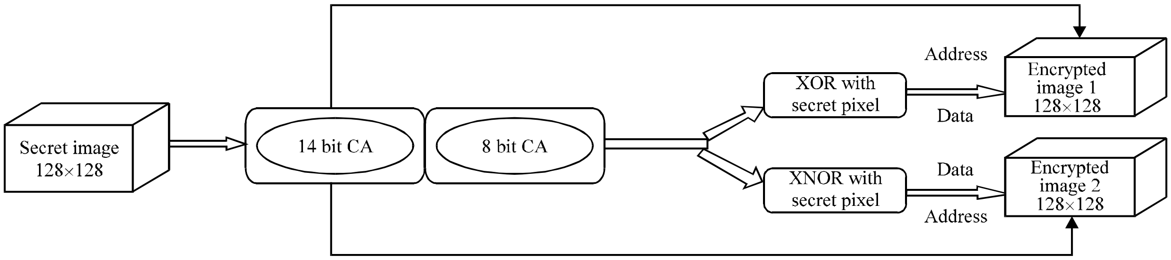
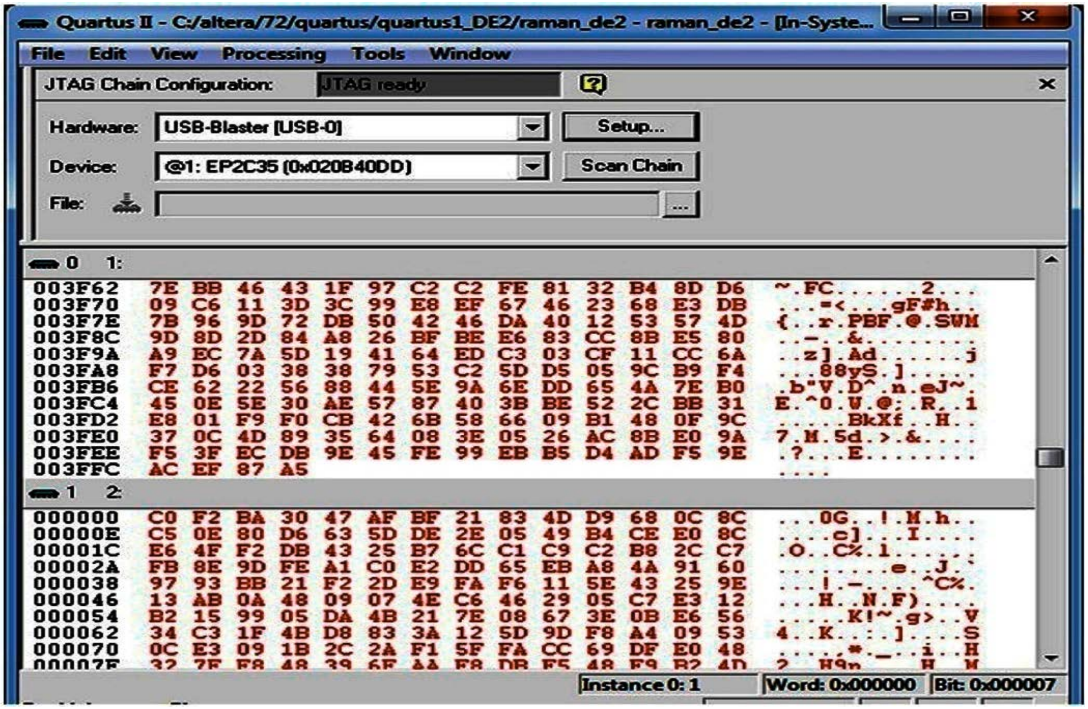


Fig. 3: Block diagram of the proposed image encryption system with two CAs


Quartus II - C:/altera/72/quartus/quartus1_DE2/raman_de2 - raman_de2 - [In-Syste...
File Edit View Processing Tools Window
Setup...
Scan Chain
...

JTAG Chain Configuration: JTAG ready

Hardware: USB-Blaster [USB-0]

Device: @1: EP2C35 (0x020B40DD)

File:

```
0  1:
003F62  7E BB 46 43 1F 97 C2 C2 FE 81 32 B4 8D D6   ~.FC......2...
003F70  09 C6 11 3D 3C 99 E8 EF 67 46 23 68 E3 DB   ...=<...gF#h..
003F7E  7B 96 9D 72 DB 50 42 46 DA 40 12 53 57 4D   {..r.PBF.@.SWM
003F8C  9D 8D 2D 84 A8 26 BF BE E6 83 CC 8B E5 80   ..-..&........
003F9A  A9 EC 7A 5D 19 41 64 ED C3 03 CF 11 CC 6A   ..z].Ad......j
003FA8  F7 D6 03 38 38 79 53 C2 5D D5 05 9C B9 F4   ...88yS.].....
003FB6  CE 62 22 56 88 44 5E 9A 6E DD 65 4A 7E B0   .b"V.D^.n.eJ~.
003FC4  45 0E 5E 30 AE 57 87 40 3B BE 52 2C BB 31   E.^0.W.@;.R,.1
003FD2  E8 01 F9 F0 CB 42 6B 58 66 09 B1 48 0F 9C   .....BkXf..H..
003FE0  37 0C 4D 89 35 64 08 3E 05 26 AC 8B E0 9A   7.M.5d.>.&....
003FEE  F5 3F EC DB 9E 45 FE 99 EB B5 D4 AD F5 9E   .?...E........
003FFC  AC EF 87 A5                                 ....
1  2:
000000  C0 F2 BA 30 47 AF BF 21 83 4D D9 68 0C 8C   ...0G..!.M.h..
00000E  C5 0E 80 D6 63 5D DE 2E 05 49 B4 CE E0 8C   ....c]...I....
00001C  E6 4F F2 DB 43 25 B7 6C C1 C9 C2 B8 2C C7   .O..C%.l....,.
00002A  FB 8E 9D FE A1 C0 E2 DD 65 EB A8 4A 91 60   ........e..J.`
000038  97 93 BB 21 F2 2D E9 FA F6 11 5E 43 25 9E   ...!.-....^C%.
000046  13 AB 0A 48 09 07 4E C6 46 29 05 C7 E3 12   ...H..N.F)....
000054  B2 15 99 05 DA 4B 21 7E 08 67 3E 0B E6 56   .....K!~.g>..V
000062  34 C3 1F 4B D8 83 3A 12 5D 9D F8 A4 09 53   4..K..:.]....S
000070  0C E3 09 1B 2C 2A F1 5F FA CC 69 DF E0 48   ....,*._..i..H
00007E  32 7F F8 48 39 6F AA F8 DB F5 48 F9 B2 4D   2..H9n......H..M
```

Instance 0: 1 Word: 0x000000 Bit: 0x000007

Fig. 4: Internal memory section of encrypted cameraman images

was same in both the cases. Figure 4 shows the internal memory section of two grayscale encrypted images stored in FPGA. The image encryption on FPGA was operated under 50 MHz clock. The image encryption operation has been controlled by a control signal ‘encrypt’ which is a toggle switch. When its position was at logic ‘1’, the encryption began. For encrypting each pixel, three clock cycles were needed. During the first cycle of 50 MHz, the 14-bit and 8-bit CA values have been generated. The second clock cycle has been used to choose the addresses of internal RAMs. These addresses were selected with the newly generated 14-bit CA values. In the third clock cycle the encryption of a pixel was performed for both the cases. In this clock cycle, XOR and XNOR operations between newly generated 8-bit CA value and the secret image pixel value were done for the two cases. The encrypted images were stored in two different sections of internal memory each with 16384 bytes capacity. In the same third clock cycle, the encrypted pixels were stored in the address generated by 14-bit CA value.

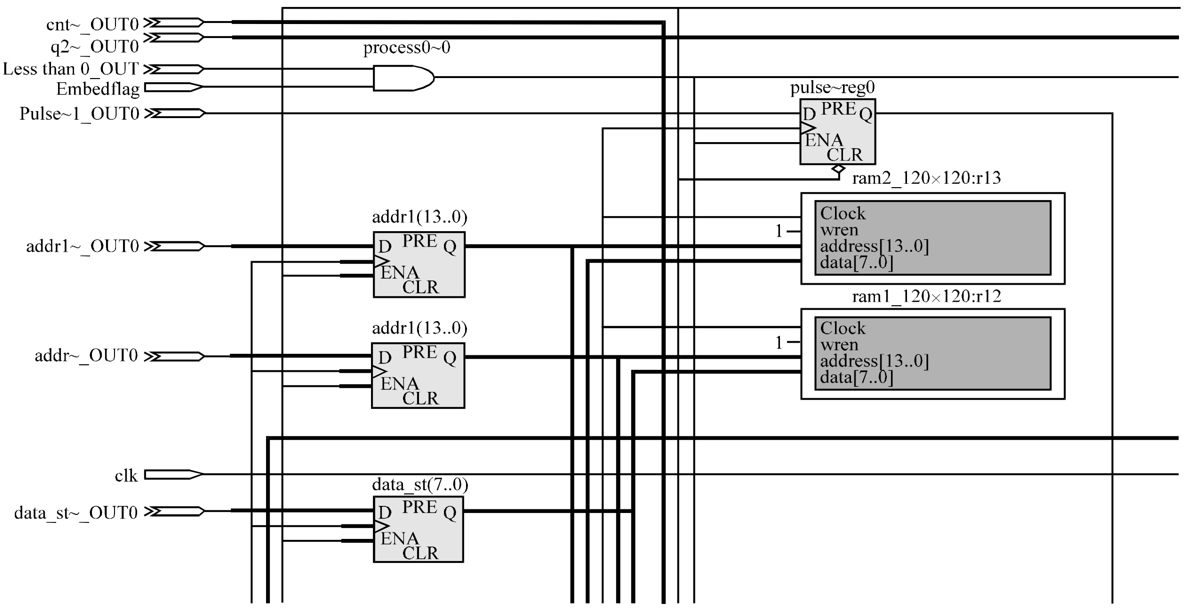


Fig. 5: RTL schematic section of the proposed algorithm

Table 1: Logic elements consumption for the proposed approach

	Total LEs				
	-------------------------------		Total combinational		
Image type	No.	%	functions	Total registers	Total memory (bits)
Gandhiji	11,226	34	11,200	230	262,144
Cameraman	9,089	27	9,063	230	262,144
Pepper	11,123	33	11,097	230	262,144
House	8,220	25	8,194	230	262,144
USC test boat	11,675	35	11,649	230	262,144

In this approach, the pixels were encrypted in the sequential order from 1-16384. But the encrypted pixels were scrambled and stored in the random locations by means of 14-bit CA value. Figure 5 shows the RTL schematic of the proposed image encryptors architecture on FPGA.

RESULTS AND DISCUSSION

Five 128×128 grayscale images namely Gandhiji, Cameraman, Pepper, House and USC test boat were used for testing the proposed dual CA image encryption algorithm. The secret images are shown in Fig. 6a-e. These images were converted to row vector for performing the encryption. After storing the encrypted images in the internal memory of FPGA, they were read back by writing them in a .hex file through in system memory content editor. Table 1 shows the hardware consumption by various secret images while executing the proposed algorithm on Cyclone II FPGA. The number of registers consumed were 230 for all the images. The total memory bits were 262,144 for storing two 128×128 grayscale images.

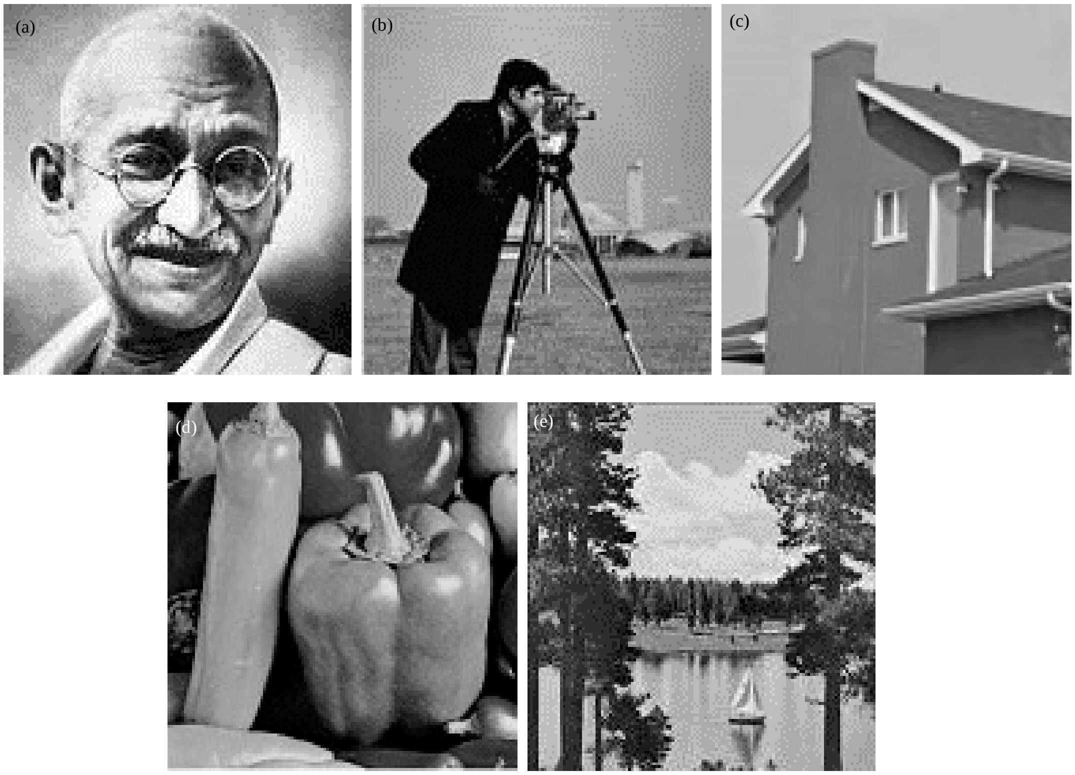


Fig. 6(a-e): Secret images, (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) USC test boat

Table 2: MSE and PSNR results of the encrypted images with XOR and XNOR encryption operations

	MSE		PSNR (dB)	
Image type	XOR	XNOR	XOR	XNOR
Gandhiji	10723	10652.80	7.82762	7.85617
Cameraman	9230.44	9310.56	8.47858	8.44105
Pepper	9419.71	9212.29	8.39043	8.48713
House	7618.82	7693.76	9.31193	9.26942
USC test boat	9727.69	9515.76	8.25071	8.34637

Table 2 shows the MSE and PSNR error metrics of the encrypted images. The highest PSNR was 9.31193 dB for house image with XOR based encryption operation and the lowest PSNR was 7.82762 dB for the cameraman test image which was encrypted with XOR operation. Figure 7 shows the chip planner view of the occupation of logic elements in Cyclone II FPGA for implementing the encryption of two USC test boat images with both XOR and XNOR based encryption approaches.

Figure 8a-e shows the encrypted secret images with XOR approach and Fig. 9a-e shows the encrypted secret images with XNOR approach.

Figure 10a-e displays the histogram results of secret images, Fig. 11a-e shows the histogram results of XOR based encryption and Fig. 12a-e displays the XNOR based encrypted secret

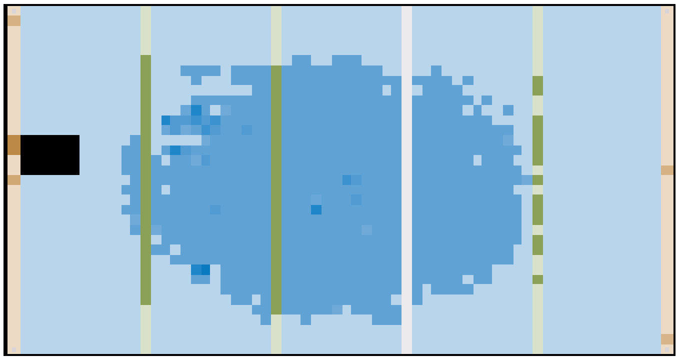


Fig. 7: Chip planner view of the USC test boat image encrypted on FPGA

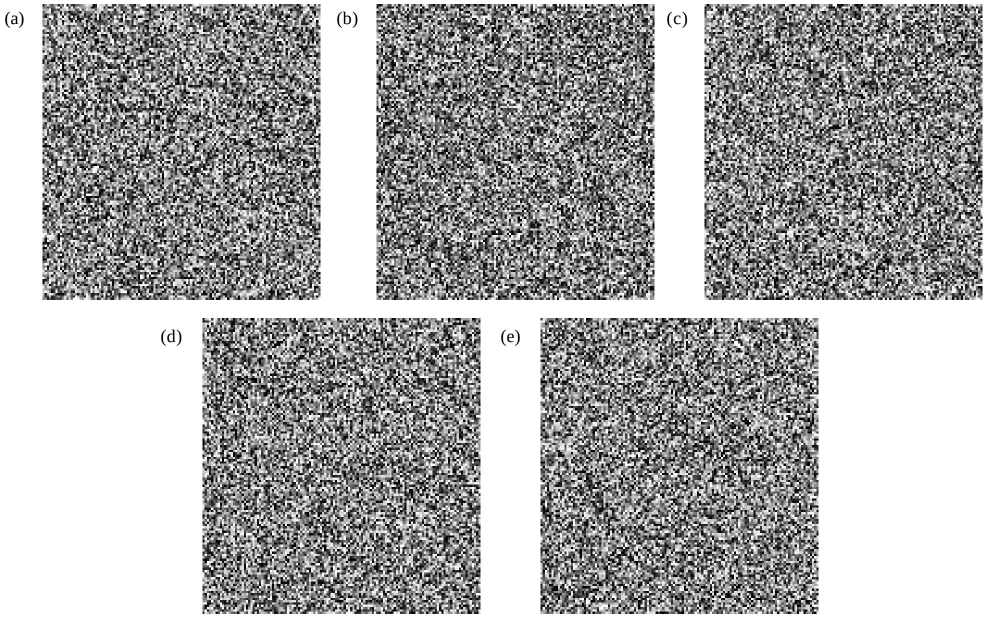


Fig. 8(a-e): Encrypted images with XOR operation (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) USC test boat

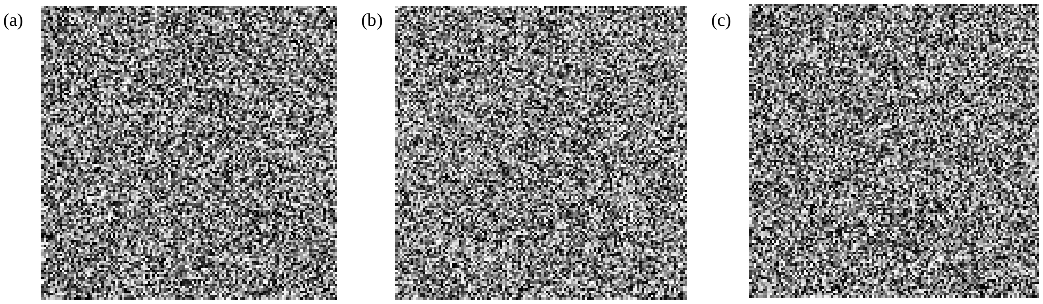


Fig. 9(a-e): Continue

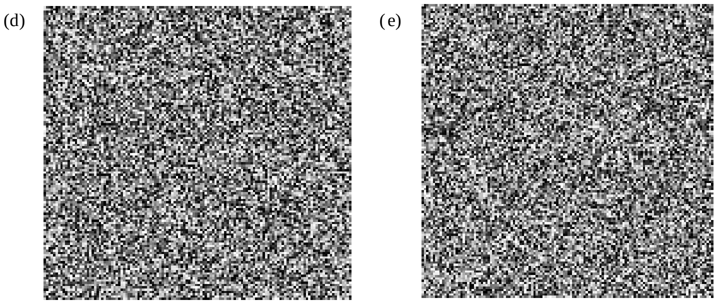


Fig. 9(a-e): Encrypted images with XNOR operation (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) USC test boat

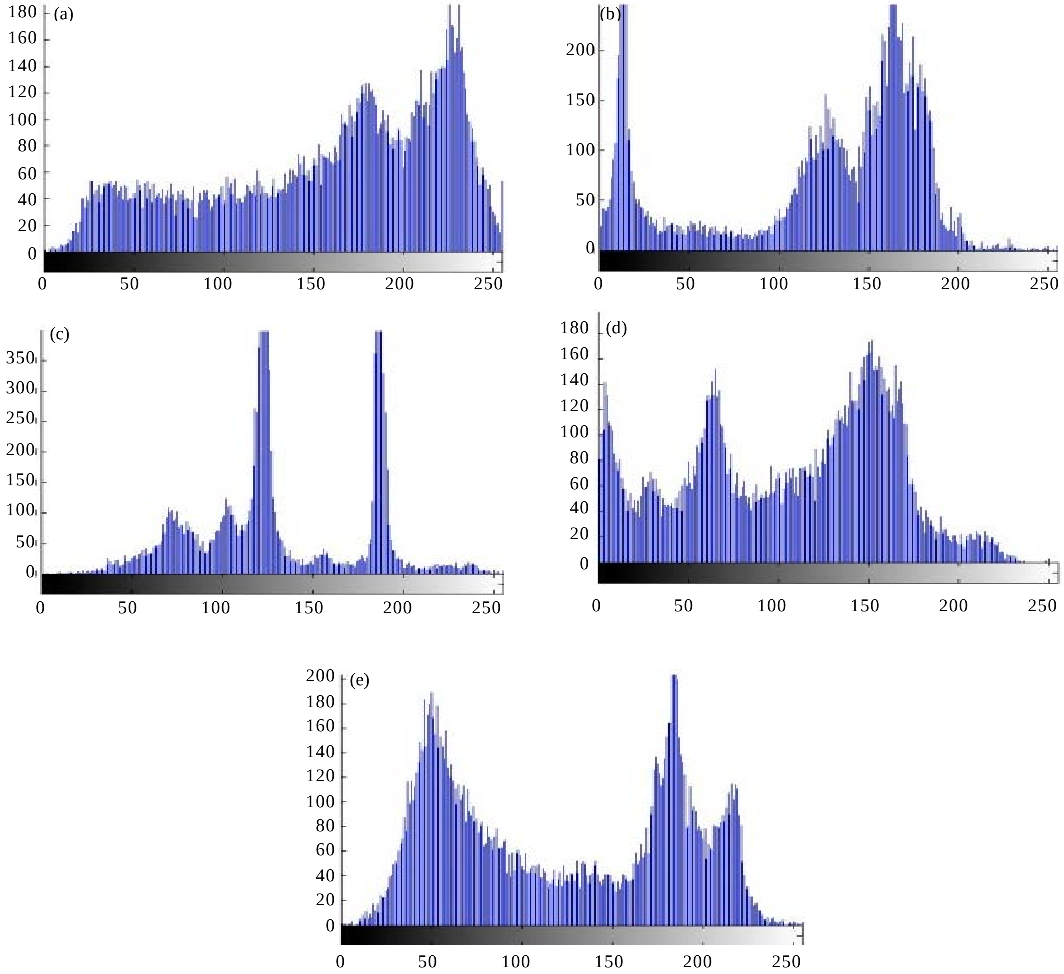


Fig. 10(a-e): Histogram of secret images (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) USC test boat

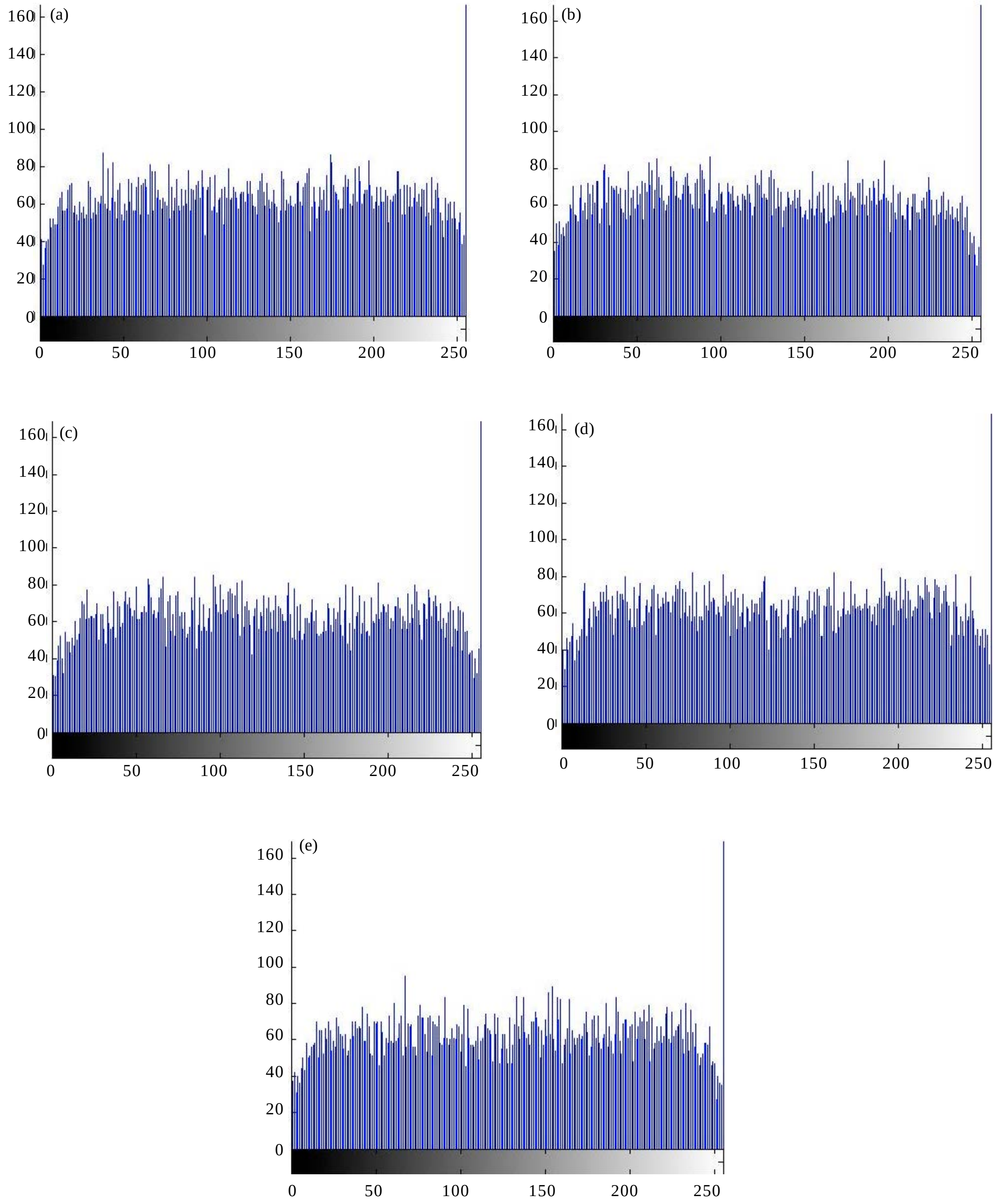


Fig. 11(a-e): Histogram of XOR based encrypted images (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) USC test boat

images' histogram plots. It has been observed that the histogram plots are approximately similar for all the five test secret images. This increases the security and may provide a tough challenge to the crypt analysis as detection of secret images will be a tedious process.

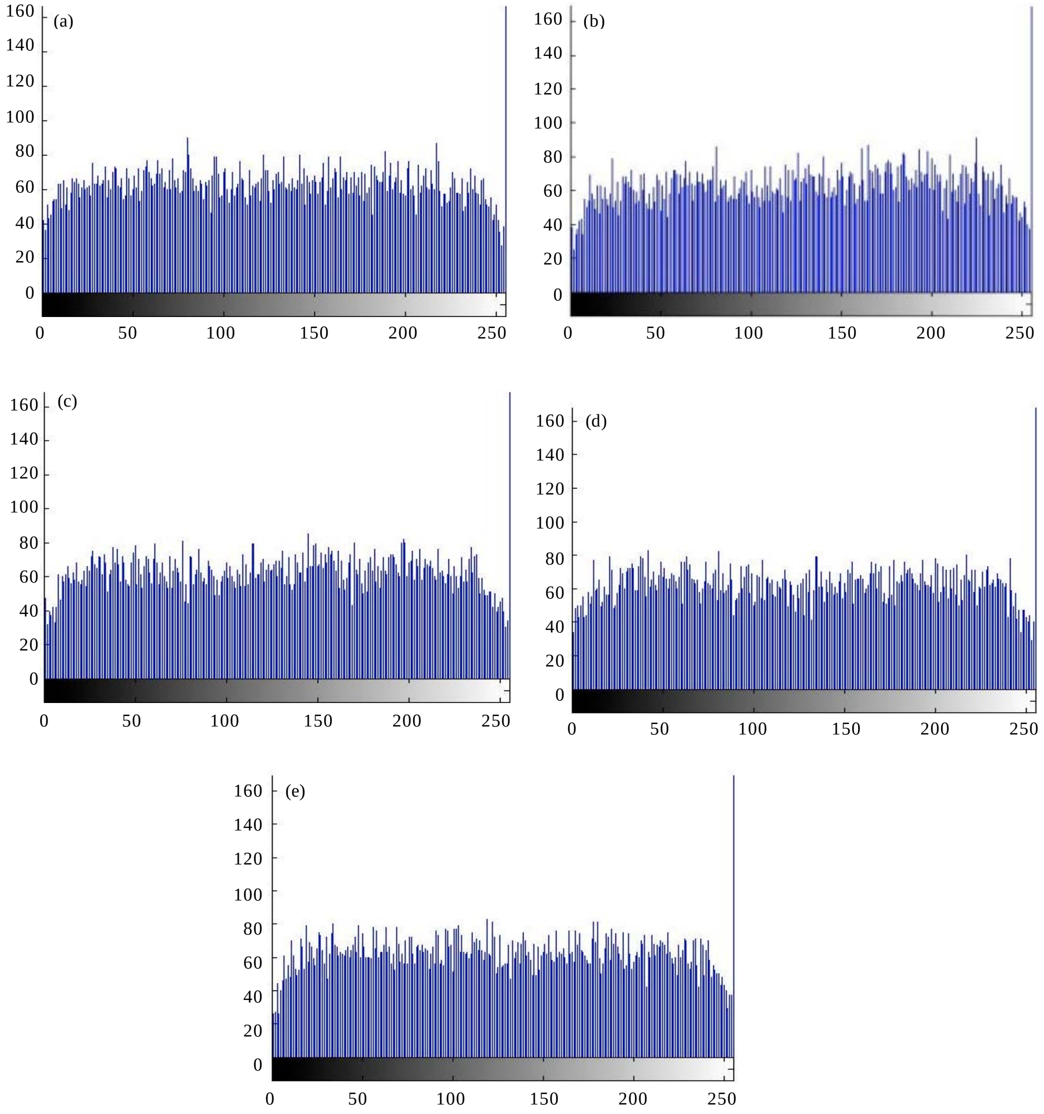


Fig. 12(a-e): Histogram of XNOR based encrypted images (a) Gandhiji, (b) Cameraman, (c) House (d) Pepper and (e) USC test boat

CONCLUSION

This study proposes a FPGA based image encryption with cellular automata. The important advantage of the proposed approach was the utilization of two different CAs one with 14-bit width and the other with 8-bit width for performing the secret image scrambling and encryption process. The CA provides 2^{14}-1 different seed values for beginning the scrambling operation which makes the encryption process a complex one. The proposed algorithm was implemented on Cyclone II FPGA which consumed 11,675 LEs (35%) for encrypting the USC test boat secret image which is the maximum consumption in the test images considered for encryption. The future study can be extended to analysis of multi-key CAs, LFSR based image encryption for enhanced security.

ACKNOWLEDGMENT

Authors wish to acknowledge SASTRA University, Thanjavur for extending infrastructural support to carry out the study.

REFERENCES

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

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. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. 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.

Azzaz, M.S., C. Tanougast, S. Sadoudi, A. Bouridane and A. Dandache, 2009. FPGA implementation of new Real-time Image Encryption based switching chaotic systems. Proceedings of the IET Irish Signals and Systems Conference, June 10-11, 2009, Dublin, Ireland, pp: 1-6.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recogn., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Dollas, A., C. Kachris and N. Bourbakis, 2003. Performance analysis of fixed, reconfigurable and custom architectures for the SCAN image and video encryption algorithm. Proceedings of the 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, April 9-11, 2003, Napa, CA, USA., pp: 19-28.

Eslami, Z., S.H. Razzaghi and J.Z. Ahmadabadi, 2010. Secret image sharing based on cellular automata and steganography. Pattern Recognit. 43: 397-404.

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

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

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., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

JianBo, X., L. Wei, Z. Liwang and P. Li, 2009. A new non-linear cross-encryption method for video images. Proceedings of the International Forum on Information Technology and Application, Volume 2, May 15-17, 2009, Chengdu, China, pp: 239-242.

Jridi, M. and A. Alfalou, 2010. A VLSI implementation of a new simultaneous images compression and encryption method. Proceedings of the IEEE International Conference on Imaging Systems and Techniques, July 1-2, 2010, Thessaloniki, Greece, pp: 75-79.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

Nandi, S., B.K. Kar and P.P. Chaudhuri, 1994. Theory and applications of cellular automata in cryptography. IEEE Trans. Comput., 43: 1346-1357.

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

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. 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, 2014b. 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, 2014c. 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, 2014d. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

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

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

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

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

Qi, X. and K. Wong, 2005. An adaptive DCT-based mod-4 steganographic method. Proceedings of the IEEE International Conference on Image Processing, Volume 2, September 11-14, 2005, Genoa, Italy, pp: II-297-II-300.

Rajagopalan, S. and H.N. Upadhyay, 2011. Stego system on chip with LFSR based information hiding approach. Int. J. Comput. Appl., 18: 24-31.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012a. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and seek in silicon: Performance analysis of Quad block Equisum Hardware Steganographic systems. Proc. Eng., 30: 806-813.

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.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

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. In: Global Trends in Information Systems and Software Applications, Krishna, P.V., M.R. Babu and E. Ariwa (Eds.). Springer, USA., ISBN: 9783642292156, pp: 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., 10.1155/2013/464107

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inform. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn., 36: 2875-2881.

Torres-Huitzil, C., 2013. Hardware realization of a lightweight 2D cellular automata-based cipher for image encryption. Proceedings of the IEEE 4th Latin American Symposium on Circuits and Systems, February 27-March 1, 2013, Cusco, Peru, pp: 1-4.

Wolfram, S., 1983. Statistical mechanics of cellular automata. Rev. Mod. Phys., 55: 601-644.

Wong, K., X. Qi and K. Tanaka, 2007. A DCT-based Mod 4 steganographic method. Signal Process., 87: 1251-1263.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Yen, J.C. and J.I. Guo, 2000. Efficient hierarchical chaotic image encryption algorithm and its VLSI realization. IEE Proc. Vision Image Signal Process., 147: 167-175.

Zhang, X. and S. Wang, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett., 25: 331-339.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.