Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (4): 308-324, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.308.324

Galois Field Proficient Product for Secure Image Encryption on FPGA

S. Rajagopalan, H.N. Upadhyay, J.B. Balaguru Rayappan and R. 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

Information science has undoubtedly engulfed the world. While astonishing on such growth, at the same time the invention of new protocols and procedures to guard the information have been going on in an effective way. Many of the transactions use images for sharing information. Image encryption needs a definite attention in such circumstances. In this study, FPGA based spatial image encryption has been proposed. The suggested approach uses variable key with Galois Field (GF) multiplier over 2^8 for encrypting the 128×128 image which was stored in internal memory of Cyclone II EP2C35F672C6 FPGA. A maximum of 11, 161 LEs (34% of total LEs) were consumed for encrypting one of the secret images Gandhiji on FPGA. This image encryption approach took 1.310 milliseconds for encrypting the 128×128 grayscale images. The effects of using fixed and variable keys for encryption have also been analyzed.

Key words: Information security, FPGA based image encryption, galois field

INTRODUCTION

Secure communication has attained a significant position in today's world of rapid data transfer. Beginning from short message services offered by various telecom providers to the crucial confidential communication which happens in defense arena, the component of security finds an important assignment. Right from the initial days of internet communication, cryptography, steganography (Cheddad *et al*., 2010; Amirtharajan and Rayappan, 2012a-d, 2013; Amirtharajan *et al*., 2013a-j; Janakiraman *et al*., 2012a, b, 2014a, b; Luo *et al*., 2011; Mohammad *et al*., 2011; Salem *et al*., 2011; Ramalingam *et al*., 2014a, b; Thien and Lin, 2003; Zhao and Luo, 2012) and watermarking have become the warriors carrying the protection shield to guard secret information against the invaders.

Image steganography which has been employed to conceal the secret information in grayscale or RGB images has been implemented both in spatial (Chan and Chen, 2004; Amirtharajan *et al*., 2012; Thanikaiselvan *et al*., 2012a-c, 2013a, b; Wu and Tsai, 2003; Zhang and Wang, 2004; Janakiraman *et al*., 2012a, b, 2013; Amirtharajan and Rayappan, 2012a, c) as well as transform domains (Wong *et al*., 2007; Qi and Wong, 2005; Amirtharajan and Rayappan, 2012d). FPGA based and firmware based stego algorithm exist in the literature (Rajagopalan *et al*., 2012a, b, 2014a-d; Sundararaman and Upadhyay, 2011; Janakiraman *et al*., 2014a, b; Janakiraman *et al*., 2012c).

Due to the emergence of wireless communication technology, studies have also been suggested on secure wireless transmission of data (Thenmozhi *et al*., 2012; Praveenkumar *et al*., 2012a, b,

2013a, b, 2014a-j). Apart from textual and audio based information transfer, there is a growing option of image as a medium of information provider. Images are being used by many sections of people in daily life for sharing some important information. Those images reach out social media like facebook and have been viewed by even unauthorized people. Moreover, images related to meteorology, space and a country's security aspects have also been communicated between the concerned in secured environment.

Image encryption is the mostly required mechanism to safeguard the images of high importance on various occasions. It has been implemented in software as well as reconfigurable hardware like FPGA platforms in the past in various related studies (Yen and Guo, 2000; Azzaz *et al*., 2009; Dollas *et al*., 2003; JianBo *et al*., 2009; Jridi and Alfalou, 2010; Torres-Huitzil, 2013). Scrambling, transposition, logical and arithmetic manipulations on different recursions have been performed in spatial as well as transform domain to encrypt the images. Compared to the software based approaches, hardware platforms offer a number of advantages towards the protection of secret images. Specific bit stream and hardware dependency, high speed, internal as well as external memory, IP cores etc., are some of the benefits of FPGA based image encryption approaches.

In this study, spatial domain image encryption on Cyclone II FPGA EP2C35F672C6 has been proposed. This approach mainly uses a Galois finite Field (GF) (Grossschadl, 2001) over 2^8 multiplier architecture for encrypting the 128×128 grayscale image stored in M4KRAM of the FPGA. Every pixel was encrypted with the help of multiplication operation between the variable encrypted key and the pixel. Cellular automata generated the new key for every pixel to be encrypted. This study also analyses the impact of using fixed and variable keys for image encryption on FPGA.

METHODOLOGY

The image encryption technique proposed in this study is based on the finite field multiplication. A field of GF over 2^8 has been considered as the grayscale value of pixels range between [0, 255]. GF deals with numbers which are finite in nature and various manipulations result in the values which lie in the same field. Various arithmetic and trigonometric computations have been performed in finite fields. Galois field multipliers are being used extensively in coding theory and cryptography and various such studies have been reported. The popular elliptic curve cryptography uses Galois field multipliers as a part of the computation. Let A and B be two 8-bit values where $\{A,B\}\epsilon\{0,255\}$. The multiplication of A and B in Galois field has been performed as follows.

Let A = 23h = 0010 0011_2 and B = AAh = 1010 1010_2 be the 8-bit numbers. The Galois field products of these two numbers take 8 iterations. The GF multiplier uses logical AND, Galois field addition, left shift and subtraction with irreducible polynomial as main operations during the course of multiplication. As a main step, the multiplicand A will be ANDed with multiplier bit B(i), where $i\epsilon\{0,7\}$ during every iteration. The resultant bits of the AND operation will be XORed with the left shifted previous iteration result. If the left shift operation yields a value which exceeds 8-bit i.e., if MSB is 1 for the 9-bit value, the XORed value will be subtracted with a irreducible polynomial $x^8+x^4+x^3+x+1$ the binary equivalent of which is 100011011. The subtraction and addition operations in Galois field are performed by XOR operation.

The Galois filed multiplication of 23 and AA will be computed as follows in eight iterations:

$$00000000+1\ (00100011) = 00000000+00100011 = 00100011$$

$$00100011+0\ (00100011) = 01000110+00000000 = 01000110$$

In the above second iteration, before Galois field addition the addend 00100011 has been left shifted by one bit and it becomes 01000110. In the same way, the left shift operation of addend precedes the Galois field addition (i.e.,) XOR in the remaining iterations. Also, in this iteration the second bit of B (i.e.,) '0' has been ANDed with all the bits of A:

$$01000110 + 1\ (00100011) = 10001100 + 00100011 = 10101111$$

$$10101111 + 0\ (00100011) = 101011110 + 000000000 = 101011110$$

In this fourth iteration, the addition resulted in 9-bit value. In this Galois field multiplication, left shifting the addend will not remove the MSB's which are '1' rather the resultant value becomes 9-bit with a '0' added at the LSB. For the next iteration this 9-bit has to be reduced to 8-bit with the help of irreducible polynomial $x^8+x^4+x^3+x+1$. Subtracting the binary equivalent of the polynomial with the 9-bit value 101011110 we get:

$$100011011-101011110 = 001000101$$

Here, subtraction has been done by XOR operation.

By neglecting the MSB '0', the new 8-bit value of fourth iteration is 01000101. Moving to next iteration:

$$01000101+1(00100011) = 10001010+00100011 = 10101001$$

$$10101001+0(00100011) = 101010010+000000000 = 101010010$$

Here, again the sixth iteration produces a 9-bit value. Reducing by subtraction with irreducible polynomial we get:

$$100011011-101010010 = 001001001$$

The new sixth iteration value is 01001001. Performing the seventh iteration:

$$01001001+1(00100011) = 10010010+00100011 = 10110001$$

$$10110001+0(00100011) = 101100010+000000000 = 101100010$$

Again subtracting the obtained 9-bit result 101100010 with the polynomial:

$$100011011-101100010 = 001111001$$

The final product result of the GF multiplication between 23 and AA is 01111001 (i.e.,) 79 h. This result has been shown in Fig. 1 which displays the model_sim simulation results of 8-bit GF multiplication between AA and four 8-bit values 23, 5F, B7 and FF. The encrypt array contains the product of the four operations {79 h, 31 h, EFh, EBh}. The verification of the product was done by log table and exponential look up tables given in (XILINX, 2003). The computation with the look up tables is as follows:

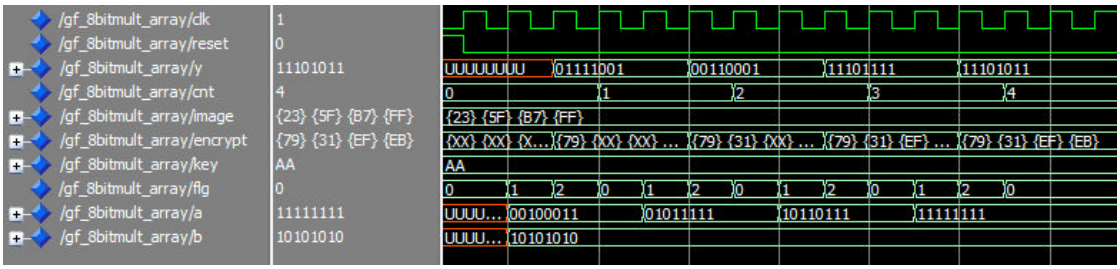

Fig. 1: Modelsim simulation results of a 8-bit GF multiplier array

$$\log GF(2^8)(A.B) = \log GF(2^8)(A) + \log GF(2^8)(B) \quad (1)$$

$$e(\log GF(2^8)(A.B)) = A.B \quad (2)$$

From the logarithmic LUTs:

$$\log GF(2^8)(A) = \log GF(2^8)(23h) = B5h$$

$$\log GF(2^8)(B) = \log GF(2^8)(AAh) = 1Fh$$

From the exponential LUT:

$$e(\log GF(2^8)(A.B)) = e(\log GF(2^8)(A)) + e(\log GF(2^8)(B)) = e^{D4h} = 79h$$

The proposed image encryption on 128×128 grayscale image has been performed by successive Galois multiplication of the pixel values and the modified key values. The key was initially kept fixed and GF multiplication of the entire pixels were carried out with the same key. As another approach, 8-bit pseudorandom keys were generated with 8-bit Cellular Automata (CA) R90-R90-R150-R90-R150-R90-R150-R90 (Nandi *et al*., 1994; Eslami *et al*., 2010; Wolfram, 1983). These keys were XORed and XNORed with the current pixel value to be encrypted in alternate clock cycles before multiplying with the pixel values of the secret image. The variable key approach resulted in better encryption compared to the fixed key approach which has been discussed in results and analysis section.

FPGA IMPLEMENTATION

The suggested image encryption approach was implemented in Cyclone II FPGA with various secret images of size 128×128. Initially an 8-bit GF multiplier was implemented using VHDL code and compiled in Quartus II ISE. Table 1 shows the logic elements consumption for an 8-bit GF multiplier on cyclone II FPGA. The multiplier took just one clock cycle of 50 MHz clock for computation which was achieved by employing process variables for quicker updation of results in every iteration. The multiplier took only 61 LEs out of 33,216 LEs.

The proposed encryption mechanism was implemented on five secret images Gandhiji, cameraman, house, pepper and SASTRA logo. These secret images are shown in Fig. 2(a-e). The encrypted images were stored in the internal M4KRAM of cyclone II FPGA. A section

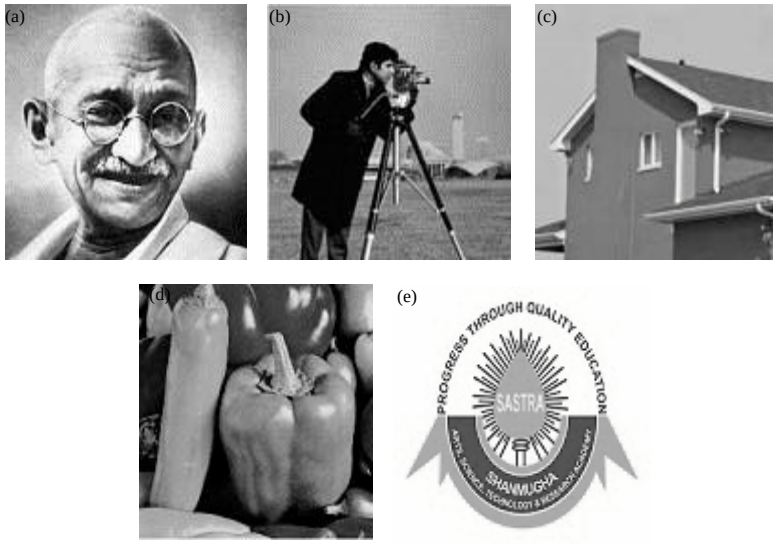

Fig. 2(a-e): Secret images (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

Table 1: Hardware consumption of 8-bit GF multiplier

Total LEs	Total combinational functions	Total registers	Total memory bits
61	57	17	0

Table 2: Synthesis report for various images for fixed key approach

Image type	Total LEs (%)	Total combinational functions	Total registers	Total memory bits
Gandhiji	11,107 (33)	11,070	178	131072
Cameraman	8,976 (27)	8,939	178	131072
House	8,121 (24)	8,084	178	131072
Pepper	11,010 (33)	10,973	178	131072
SASTRA logo	7,831 (24)	7,794	178	131072

Table 3: Synthesis report for various images for variable key approach

Image type	Total LEs (%)	Total combinational functions	Total registers	Total memory bits
Gandhiji	11,161(34)	11,124	194	131072
Cameraman	9,027(27)	8,990	194	131072
House	8,173(25)	8,136	194	131072
Pepper	11,066(33)	11,029	194	131072
SASTRA logo	7,888 (24)	7,851	194	131072

of internal memory having the encrypted Gandhiji image has been shown in Fig. 3. Figure 4 displays a cross section of technology schematic of image encryption algorithm.

The logic elements consumption has been shown in Table 2 and 3 for fixed and variable key approaches. The variable key based encryption approach consumes more logic elements compared to the fixed key approach. The variable key approach has an additional component of 8-bit cellular automata for PRPG and XOR and XNOR operations performed before GF multiplication. Comparing the test images considered, minimum of 7,831 LEs were taken by SASTRA logo image

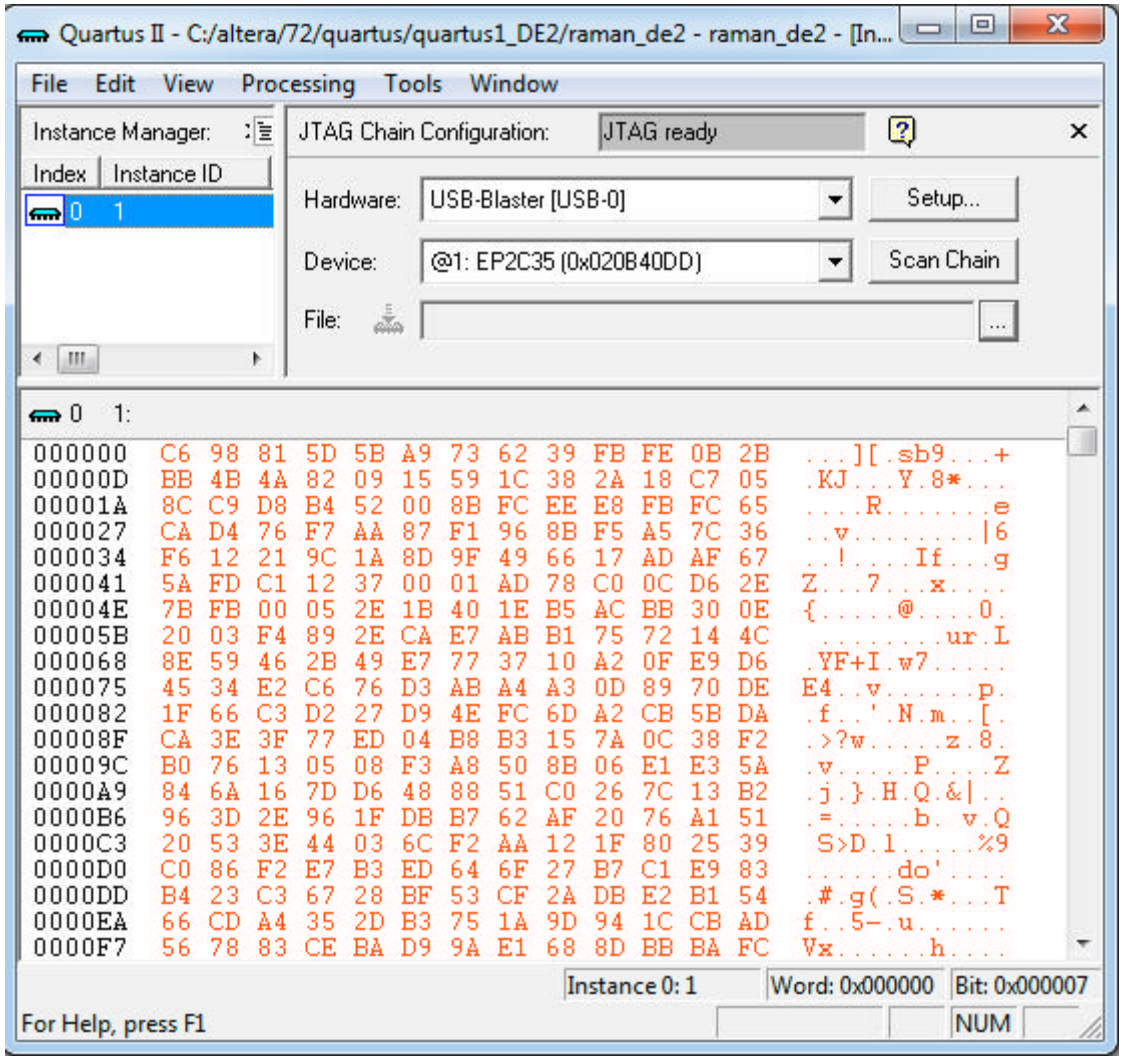

Fig. 3: FPGA internal memory with encrypted Gandhiji image

with fixed key approach while the variable key method consumed 7,888 LEs. The Gandhiji image took 11,107 LEs (34%) in the fixed key approach with the same image consuming 11,161 LEs for variable key approach. Even though, there was no change the memory consumption, the fixed key approach consumed 178 registers but variable key based encryption method used 194 registers for implementing the image encryption on FPGA.

Timing analysis: The fixed as well as variable key encryption approaches have been implemented on Cyclone II FPGA with 50 MHz clock.

For fixed key approach:

- No. of clock cycles needed for reading new pixel value = 1
- No. of clock cycles needed for GF multiplication of pixel and fixed 8-bit key = 1

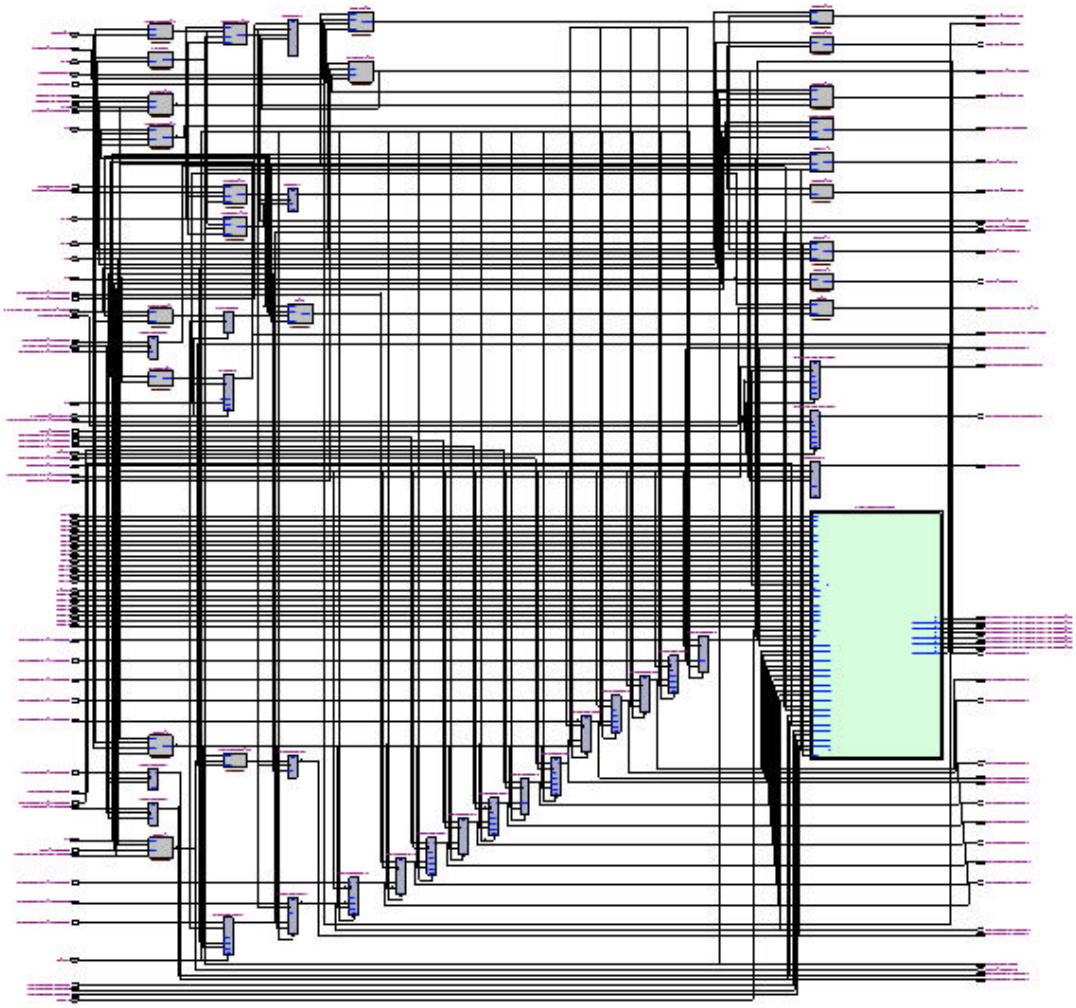

Fig. 4: Technology schematic cross section of variable key based encryption approach

- No. of clock cycles needed for writing the encrypted pixel in M4KRAM = 1
- Total No. of pixels = 16384
- Total clock cycles needed for encrypting the 128×128 image = 16384×3 = 49152
- Total time needed for encryption = 49152×20 ns = 983.040 μs

For variable key approach:

- No. of clock cycles needed for new 8-bit key generation with CA = 1
- No. of clock cycles needed for reading new pixel value and XOR/XNOR with key = 1
- No. of clock cycles needed for GF multiplication of pixel and variable 8-bit key = 1
- No. of clock cycles needed for writing the encrypted pixel in M4KRAM = 1
- Total No. of pixels = 16384

- Total clock cycles needed for encrypting the 128×128 image = 16384×4 = 65536
- Total time taken for encryption = 65536×20 ns = 1310.720 μs

RESULTS AND ANALYSIS

Table 4 and 5 show the error metrics in the form of MSE and PSNR of encrypted images under fixed key and variable key approach.

Figure 5a-e show the histogram reports of various secret images considered in this image encryption algorithm. The fixed key approach uses the same 8-bit key for encrypting the entire pixels of grayscale images. This provides a problem in generating the encrypted images of high complexity. Because, if the secret image consists of maximum background or same grayscale repeated in most part of the images, the encrypted image will have same grayscale level in those areas of image. This is visible in Fig. 6e SASTRA logo image encrypted with fixed key approach. The histogram of SASTRA logo secret image also has two peaks in its report which reveals that the image has few grayscale values dominant. Figure 6a-e show the encrypted images with fixed key methodology of image encryption. Except Gandhiji and pepper images, the encryption quality was not good in cameraman, house and SASTRA logo images. Figure 7a-e show the corresponding histogram of encrypted images. It is also clear that the histogram is not uniform for all the images. In order to ensure high complexity and a strong reply to the attacks, the histogram uniformity is most important.

The second approach of variable key encryption mechanism solves this problem. As per this approach, the key changes during every new pixel taken for encryption and as a strong measure in alternate pixels XOR and XNOR operations were performed with the new pixel value before GF multiplication. Figure 8a-e show the encrypted images with variable key and their corresponding histogram have been presented in Fig. 9a-e. Now histogram plots look similar for all the five test images which shows the complexity of the variable key approach.

Table 6 and 7 show the horizontal, vertical and diagonal correlation of secret and encrypted images with fixed and variable key approaches. The correlation of pixels after encryption were very minimum compared to the secret image pixels. This statistical analysis shows the strength of the proposed image encryption on FPGA. The correlation coefficients of variable key approach were more close to 0 compared to the fixed key approach. Figure 10-12 show the

Table 4: MSE and PSNR results of the encrypted images for fixed key approach

Image type	MSE	PSNR (dB)
Gandhiji	10604.6	7.87585
Cameraman	9328.2	8.43283
House	8701.61	8.73481
Pepper	9029.61	8.57412
SASTRA logo	21586	4.78907

Table 5: MSE and PSNR results of the encrypted images for variable key approach

Image type	MSE	PSNR (dB)
Gandhiji	10840.8	7.78019
Cameraman	9269.82	8.46009
House	7612.45	9.31556
Pepper	9063.18	8.558
SASTRA logo	16863.2	5.8614

Table 6: Correlation coefficients of adjacent pixels of secret images

	Cover		
Image type	Horizontal	Vertical	Diagonal
Gandhiji	0.9161	0.9182	0.8588
Cameraman	0.9159	0.9526	0.8820
House	0.9349	0.9255	0.8812
Pepper	0.9166	0.9409	0.8770
SASTRA logo	0.6800	0.7165	0.6527

Table 7: Correlation coefficients of adjacent pixels of encrypted images with fixed and variable keys

	Encrypted with fixed key			Encrypted with variable key		
Image type	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Gandhiji	-0.0098	-0.0049	0.0046	0.0038	-0.0094	-0.0027
Cameraman	0.1201	0.1781	0.0445	-0.0137	-0.0064	0.0026
House	0.2377	0.1517	0.1165	-0.0221	-0.0006	0.0237
Pepper	-0.0051	-0.0028	0.0046	0.0039	-0.0097	-0.0114
SASTRA logo	0.2030	0.2036	0.1566	-0.0017	-0.0002	0.0047

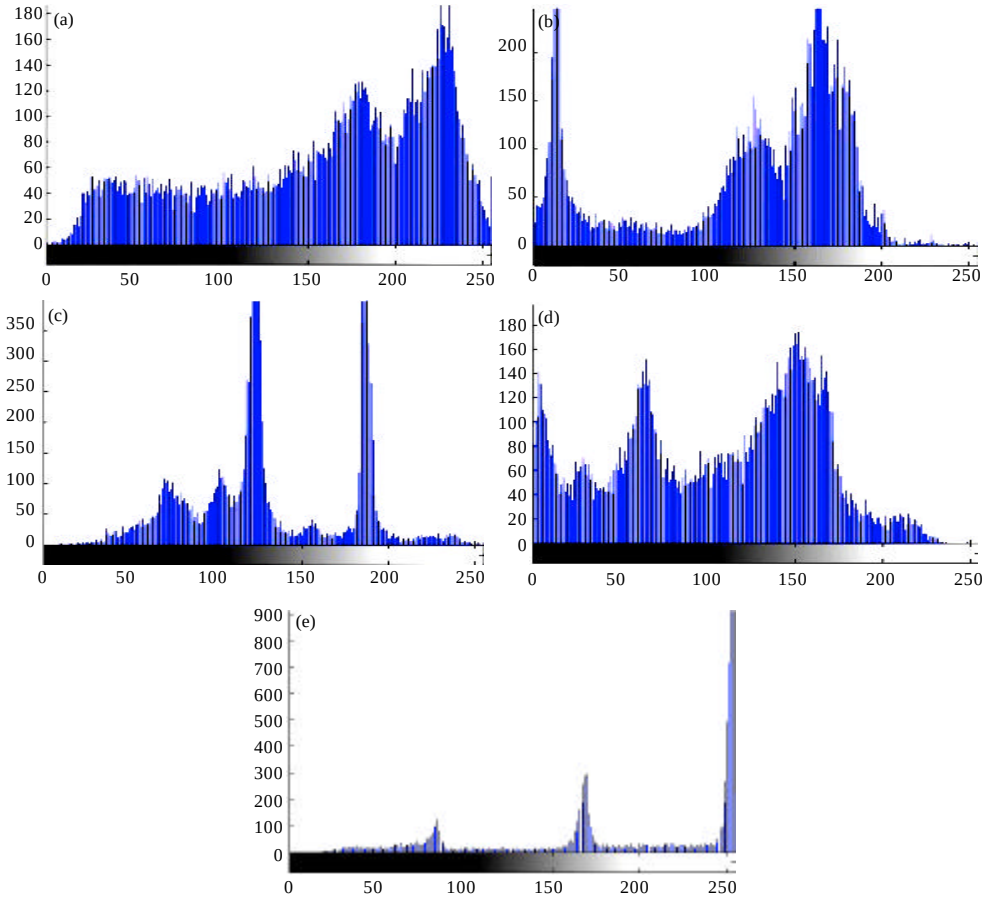

Fig. 5(a-e): Histogram of secret images (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

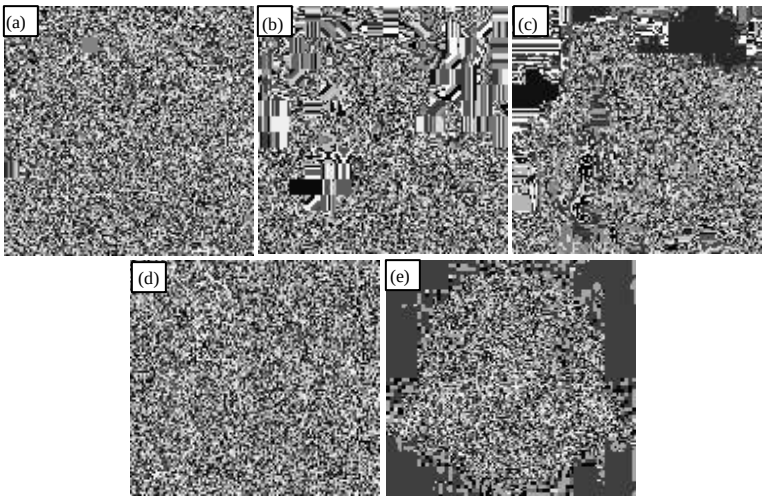

Fig. 6(a-e): Encrypted images with single key (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

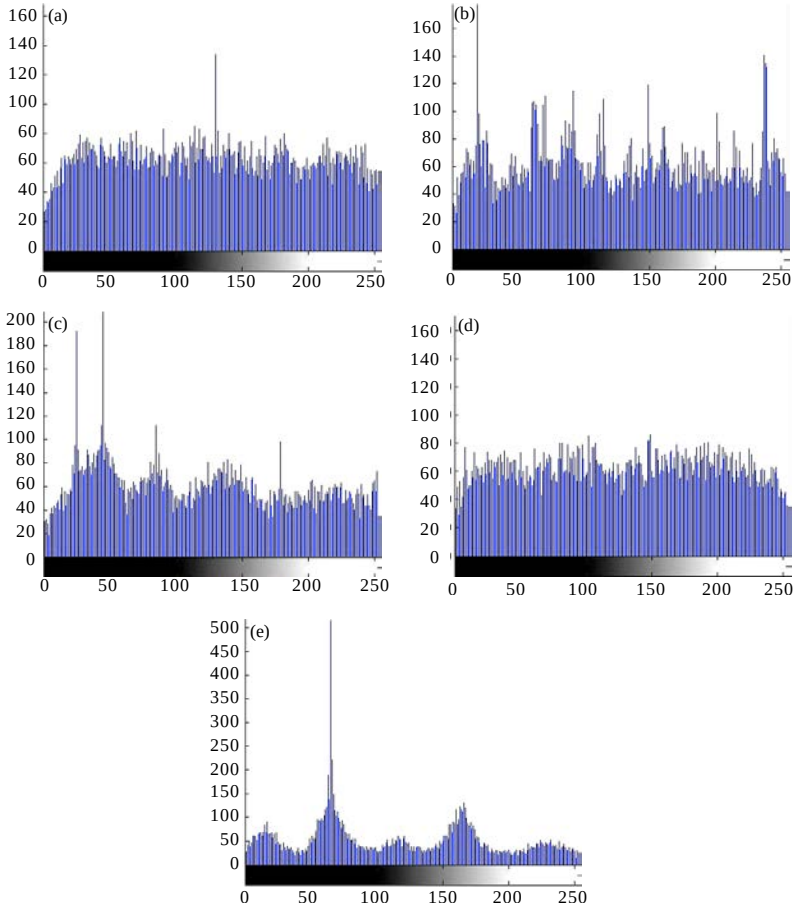

Fig. 7(a-e): Histogram of encrypted images single key (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

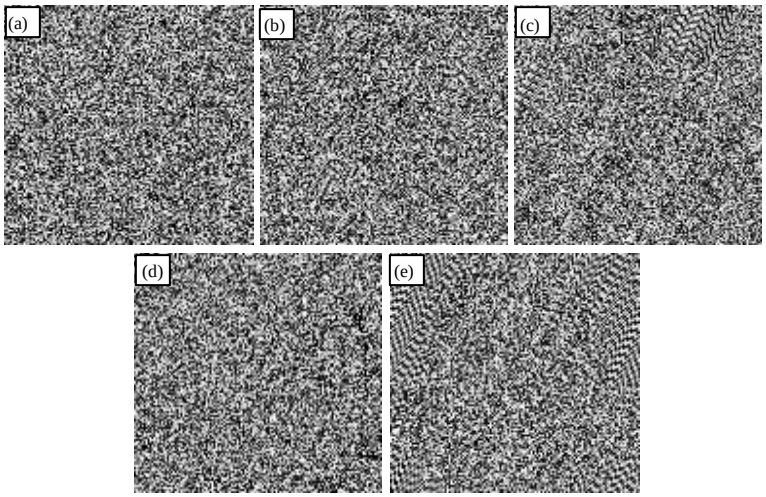

Fig. 8(a-e): Encrypted images with multiple keys (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

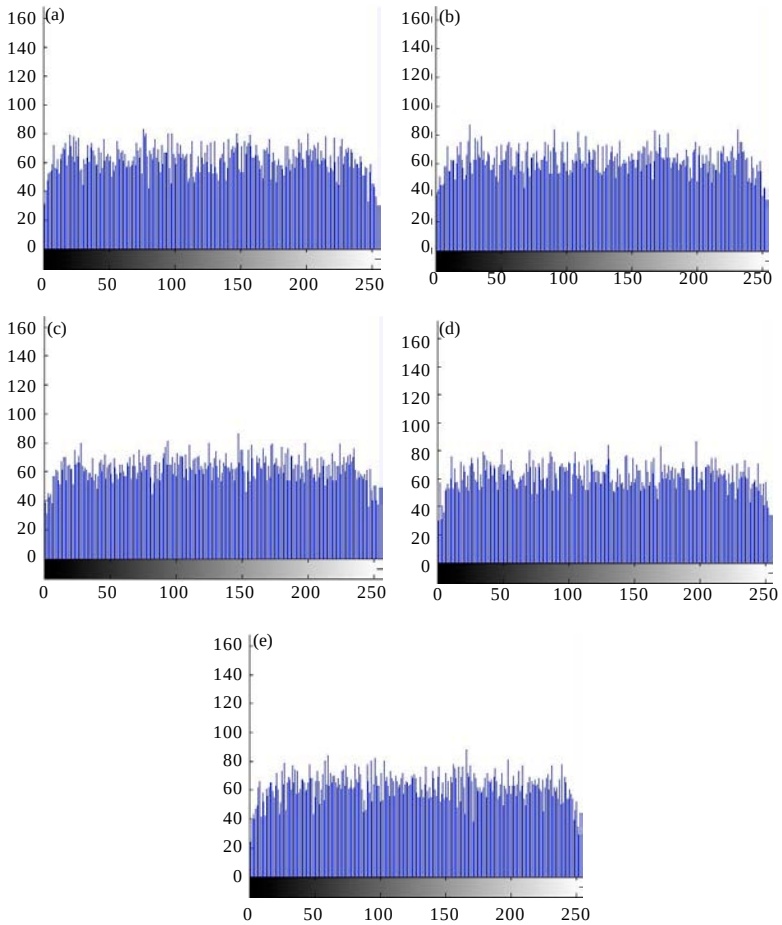

Fig. 9(a-e): Histogram of encrypted images with multiple keys (a) Gandhiji, (b) Cameraman, (c) House, (d) Pepper and (e) SASTRA logo

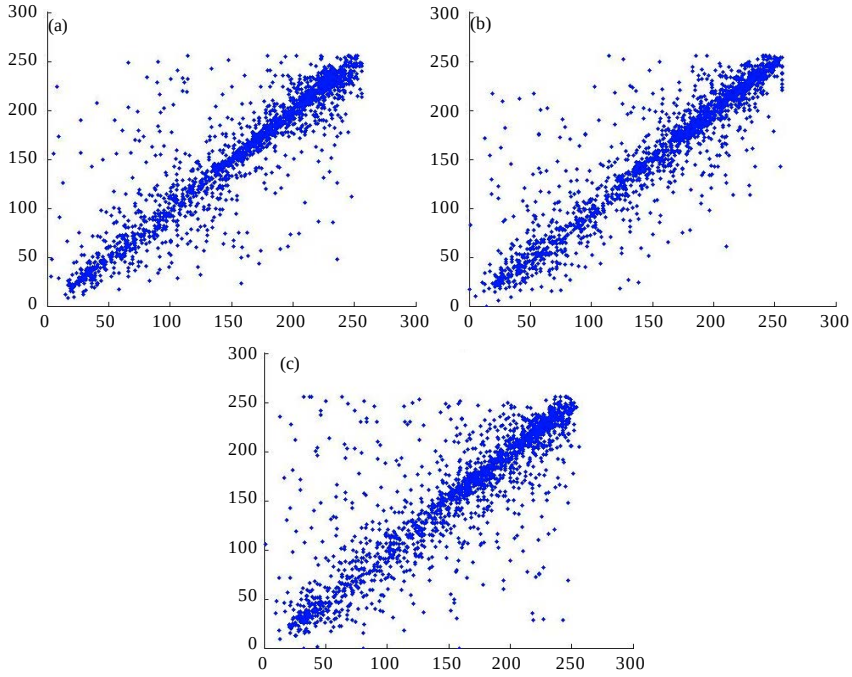

Fig. 10(a-c): Correlation of pixels in secret image Gandhiji (a) Horizontal, (b) Vertical and (c) Diagonal

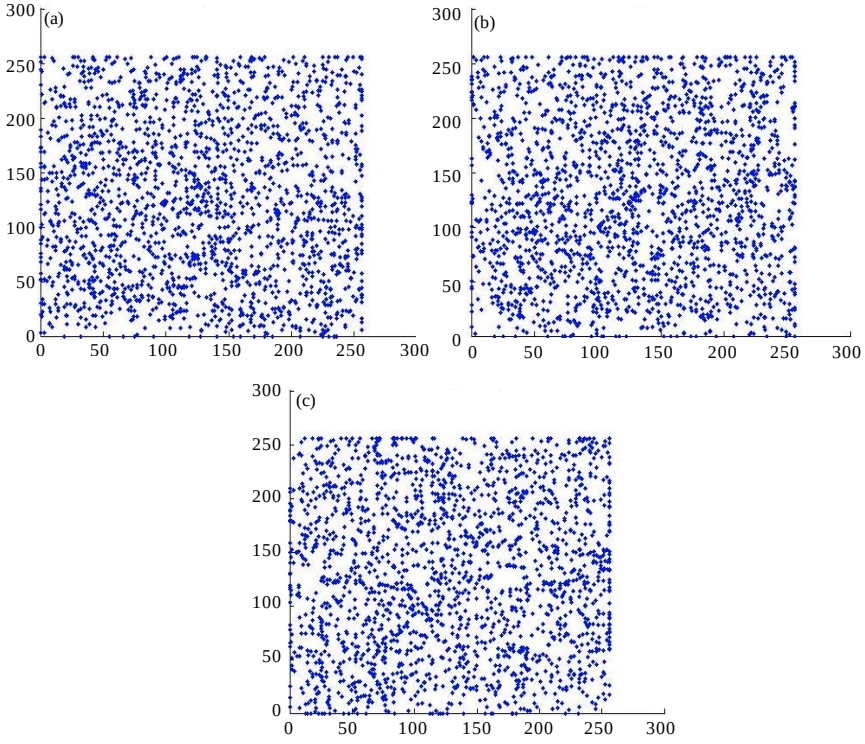

Fig. 11(a-c): Correlation of pixels in fixed key encrypted image Gandhiji (a) Horizontal, (b) Vertical and (c) Diagonalal

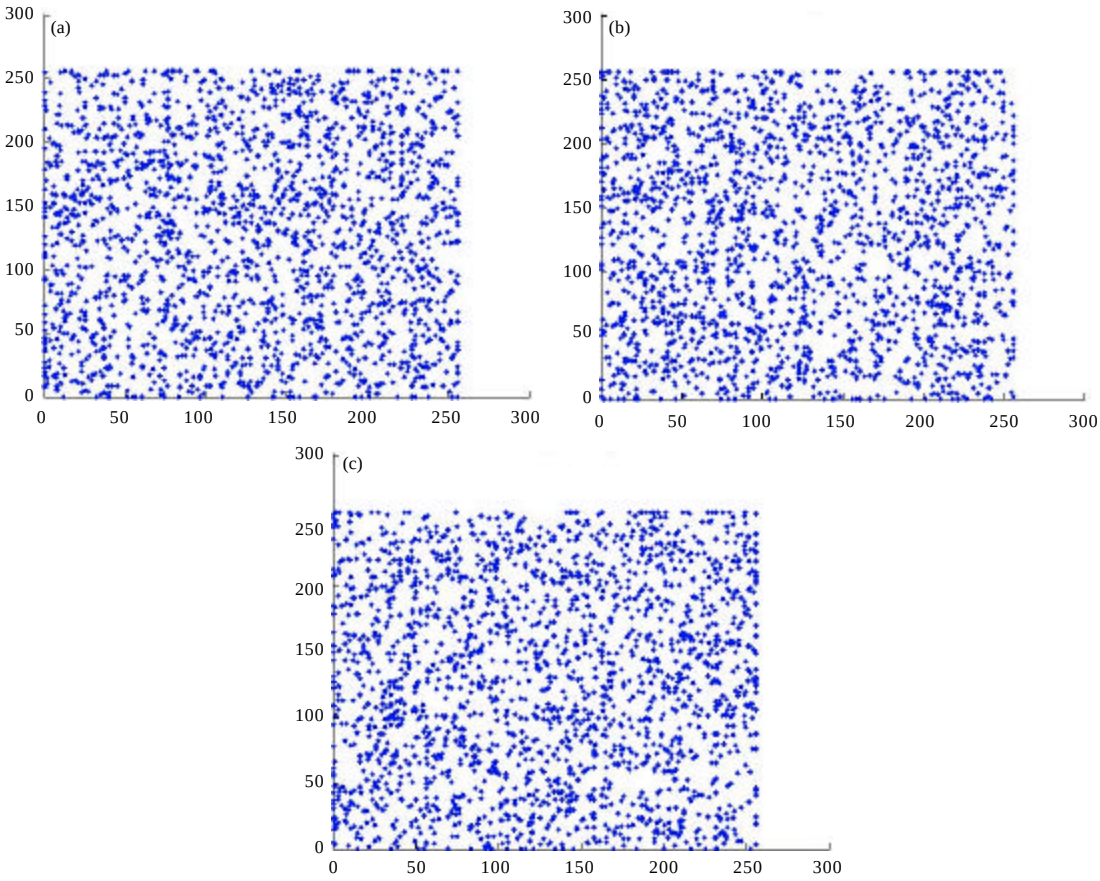

Fig. 12(a-c): Correlation of pixels in variable key encrypted image Gandhiji (a) Horizontal, (b) Vertical and (c) Diagonal

correlation images of 2000 randomly selected pixels of Gandhiji secret and encrypted images. The distribution of pixels after encryption is widespread and is visible in the correlation images.

CONCLUSION

A variable key based spatial image encryption on Cyclone II FPGA has been proposed in this study. The approach uses Galois field multiplication and cellular automata combination for providing the encryption of pixels of 128×128 grayscale images. The limitation of fixed key approach has also been discussed in this study. The proposed system can be a standalone image encryption chip which will improve the security of image sharing over the existing image encryption schemes by its specific bit stream dependency.

ACKNOWLEDGMENT

The authors wish to acknowledge SASTRA University for providing infrastructural support to carry out this study.

REFERENCES

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

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., 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, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

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

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. 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, 2013c. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

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

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

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

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013g. 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, 2013h. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

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

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

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 Recognit., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P. Mc 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.

Grossschadl, J., 2001. A low-power bit-serial multiplier for finite fields GF(2^m). Proceedings of the IEEE International Symposium on Circuits and Systems, Volume 4, May 6-9, 2001, Sydney, NSW, pp: 37-40.

Janakiraman, S., A.A. Mary, J. Chakravarthy, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Pixel bit manipulation for encoded hiding-An inherent stego. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

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

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012c. 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. Pal 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. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

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

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

Praveenkumar, P., M. Nagadinesh, P. L akshmi, 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, 2014a. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

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

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

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. 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, 2014e. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

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

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

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

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., 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. Procedia Eng., 30: 806-813.

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

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

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

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

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

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

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.

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

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. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

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

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

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

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 Recognit., 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 Mod4 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.

XILINX, 2003. CoolRunner-II CPLD galois field GF(2^m) multiplier. XAPP371 (Version 1.0), XILINX®, September 26, 2003. http://www.xilinx.com/support/documentation/application_notes/xapp371.pdf

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.