Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (4): 291-307, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.291.307

Logic Elements Consumption Analysis of Cellular Automata Based Image Encryption on FPGA

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

There is a growing demand for techniques which improve the secure transmission of images of high confidentiality. The images captured by satellites and defense sensitive images handled by scientists need a strong protection when they are to be communicated for various applications. Image encryption algorithms need to be stronger in such cases. Various FPGA based image encryption algorithms have been proposed in the past to tighten the information security. This study analyses the hardware consumption issues of various 128×128 grayscale images which were encrypted with cellular automata circuits on Cyclone II EP2C35F672C6 FPGA. It was observed that the Logic Elements (LE) consumption varied for different test images considered in this encryption approach. This study analyses the performance of the image encryption algorithm on 15 different grayscale images based on technology schematic net lists, LE consumption, error metrics, Fast Fourier transform and histogram.

Key words: Image encryption, FPGA, cellular automata, LabVIEW

INTRODUCTION

Communication technology has seen its various incarnations over the years. It has created revolution and took the entire world by storm by means of making the once difficult thing to a door step item. However, be it personal communication or official communication, the one component which remains mandatory is security. Secure communication is the one which everyone is looking for. To counterattack the threats majorly posed by the hackers, various algorithms and approaches have been invented in the past and still the search is going on. The famous three forms of security providers are cryptography, Steganography (Cheddad *et al*., 2010; Amirtharajan and Rayappan, 2012a-d, 2013; Amirtharajan *et al*., 2012, 2013a-j; Janakiraman *et al*., 2012a, b, 2014a, b; Luo *et al*., 2011; Ramalingam *et al*., 2014a; Mohammad *et al*., 2011; Salem *et al*., 2011; Thien and Lin, 2003; Zhao and Luo, 2012) and watermarking. While the scrambling of the secret message is the job of cryptography (Ramalingam *et al*., 2014b), steganography conceals the information to be protected in a fictious cover which are mostly images, audio and video as other mediums using spatial (Chan and Cheng, 2004; Amirtharajan and Rayappan, 2012a; 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

domain techniques (Wong *et al*., 2007; Qi and Wong, 2005; Amirtharajan and Rayappan, 2012d). Copyright protection of electronic documents is being performed by a process called watermarking. Steganography has been implemented in software as well as hardware platforms (Rajagopalan *et al*., 2012a, b, 2014a-d; Sundararaman and Upadhyay, 2011; Janakiraman *et al*., 2012c, 2014a, b) and various related works have been reported in the past. Due to the advancements in wireless communication, approaches for secure wireless transmission have also been suggested (Thenmozhi *et al*., 2012; Praveenkumar *et al*., 2012a, b, 2013a, b, 2014a-l).

Images have become important in everyone's life. While personal image sharing happens in a large scale everyday through internet, the protection of the images occupies the center stage. Also various highly confidential images related to object, place etc., are being communicated between scientists and higher authorities which require utmost protection. Image encryption can play a pivotal role in secret transmission of images between the concerned. Image encryption has been implemented using software as well as hardware platforms (Yen and Guo, 2000; Azzaz *et al*., 2009; Dollas *et al*., 2003; JianBo *et al*., 2009; Jridi and Alfalou, 2010) in the different studies reported in the literature.

Image encryption on reconfigurable hardware like FPGA (Torres-Huitzil, 2013) requires some special attention. The encrypted bit stream of a specific FPGA carries the image to be protected. This is an important advantage where the confidential image can be retrieved only if a specific FPGA has been programmed with the specific bitstream. This study analyses the hardware implementation issues related to a cellular automata based image encryption technique. A 14-bit cellular automata was used to shuffle and encrypt the 128×128 grayscale image on Cyclone II EP2C35F672C6 FPGA. This study also focuses on analysis of logic elements utilization by various images while doing encryption.

METHODOLOGY

The image encryption proposed in this study deals with shuffling and encryption of the grayscale images using a 14-bit Cellular Automata (CA) with the rule combination R150-R90-R90-R90-R90-R90-R150-R90-R90-R90-R90-R90-R90-R150, where R90 and R150 represent rule 90 and rule 150, respectively. Cellular automata are pseudorandom pattern generators (Nandi *et al*., 1994) which consist of collection of cells or in hardware systems Flip-Flops. Cellular automata exhibits excellent pseudo randomness which produces the patterns with very minimum bit shifting in successive patterns. A maximum length sequence of 2^n-1 can be generated by constructing the CA with rule 90 and 150 (Eslami *et al*., 2010; Wolfram, 1983). As per rule 90, the XOR operation between previous and next cell states of current time step decides the present cell status of next time step. The XOR operation between previous, present and next cell states of current time step decides the present cell status of next time step in rule 150. The 14-bit CA considered in the proposed algorithm is shown in Fig. 1.

This image encryption method uses the same 14-bit CA for performing shuffling and encryption. The 14-bit CA pattern was used as internal memory address where the new pixel value has to be stored in FPGA. Also the encryption was implemented by XORing the least 8-bits of every newly generated 14-bit CA value with the new pixel value. The proposed image encryption of a 128×128 grayscale image was implemented on Cyclone II FPGA EP2C35F672C6 with Quartus II version 7.2 ISE. The pseudo code of the proposed algorithm is given as follows:

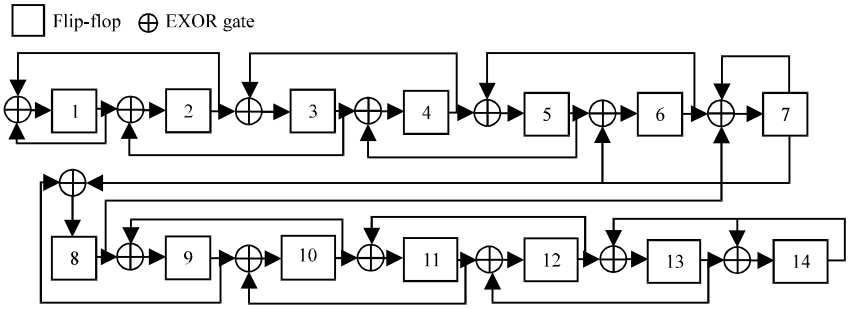

Fig. 1: A 14-bit CA circuit with the combination R150-R90-R90-R90-R90-R90-R150-R90-R90-R90-R90-R90-R90-R150

```
Convert the 128×128 2D grayscale image into row matrix;
Initialize the CA with a 14-bit non-zero seed value;
Wait until 50MHzclk'event and 50MHzclk = 1;
While (count <= 16384)
{
Generate the new 14-bit address with CA pseudorandom pattern;
Get the pixel value in sequential order ((i.e.,) from 1 to 16384);
Encrypt the pixel by XORing the pixel value with least significant 8-bits of CA pattern;
Store the encrypted pixel in the internal RAM address generated by 14-bit CA;
count = count + 1;
}
```

HARDWARE CONSUMPTION ANALYSIS

The CA based encryption approach was tested on 15 different secret images. The secret images are shown in Fig. 2a-o.

The histogram reports of secret images have been shown in Fig. 3a-o.

In order to understand the frequency variation of pixels in the secret images, FFT of secret images were computed using LabVIEW software. These FFT resultant images of corresponding secret images have been shown in Fig. 4a-o.

Figure 5a-o show the encrypted images, Fig. 6a-o display the histogram reports of encrypted images and Fig. 7a-o display the FFT of the encrypted images. The histogram report of the encrypted images look similar which indicates the complexity of encryption. The FFT of the encrypted images also look almost similar. This shows the uniformity in the frequency variation of encrypted images.

After encryption, the pixels of 128×128 grayscale image were stored in internal M4KRAM of Cyclone II FPGA. Table 1 shows the hardware consumption of 15 different images considered here. The Cyclone II FPGA EP2C35F672C6 which has been used for implementing this image encryption algorithm has 33,216 logic elements and 4,83,840 bits on internal RAM. All the 15 images consumed 167 registers and 1,31,072 bits for storing 128×128 grayscale image inside the FPGA during the encryption. But there was a difference in the usage of combinational functions. Of the 15 different images used in this algorithm, the maximum number of combinational functions were utilized by the 13th image in Table 1 (i.e.,) rice which used 11,781 functions. For encrypting the rice image, 11,798 LEs (36% of total LEs) have been utilized which is the maximum consumption compared to the other secret images.

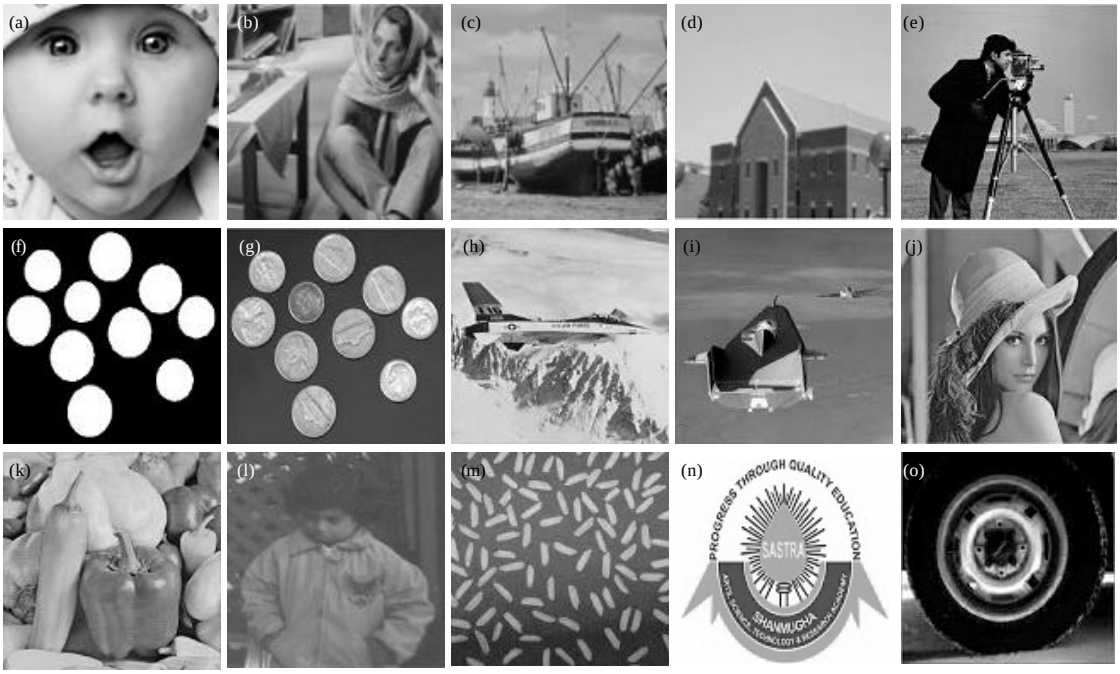

Fig. 2(a-o): Secret images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (i) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

Table 1: Logic elements consumption for the proposed approach

Image type	Logic elements used	Total combinational functions	Total registers	Total memory bits
Baby	10,409 (31%)	10,392	167	131072
Barb	11,692 (35%)	11,675	167	131072
Boat	10,734 (32%)	10,717	167	131072
Building	7,578 (23%)	7,561	167	131072
Cameraman	9,810 (30%)	9,793	167	131072
Circles	5,132 (15%)	5,115	167	131072
Coins	8,761 (26%)	8,744	167	131072
Jet	10,468 (32%)	10,451	167	131072
Jet 1	8,439 (25%)	8,422	167	131072
Lena	11,152 (34%)	11,135	167	131072
Peppers	11,057 (33%)	11,040	167	131072
Pout	10,050 (30%)	10,033	167	131072
Rice	11,798 (36%)	11,781	167	131072
SASTRA logo	7,815 (24%)	7,798	167	131072
Tyre	10,021 (30%)	10,004	167	131072

Similarly the test image circles consumed only 5,115 combinational functions and thereby utilizing 5,132 LEs (just 15% of the total LEs). While doing comparison between these two extremes, it was clear that even though the total memory bits usage looked same, the properties of an image was a deciding factor in the netlist creation and LE consumption. When setting 10,000 as the threshold for logic elements consumption among these 15 images, there were 6 images that

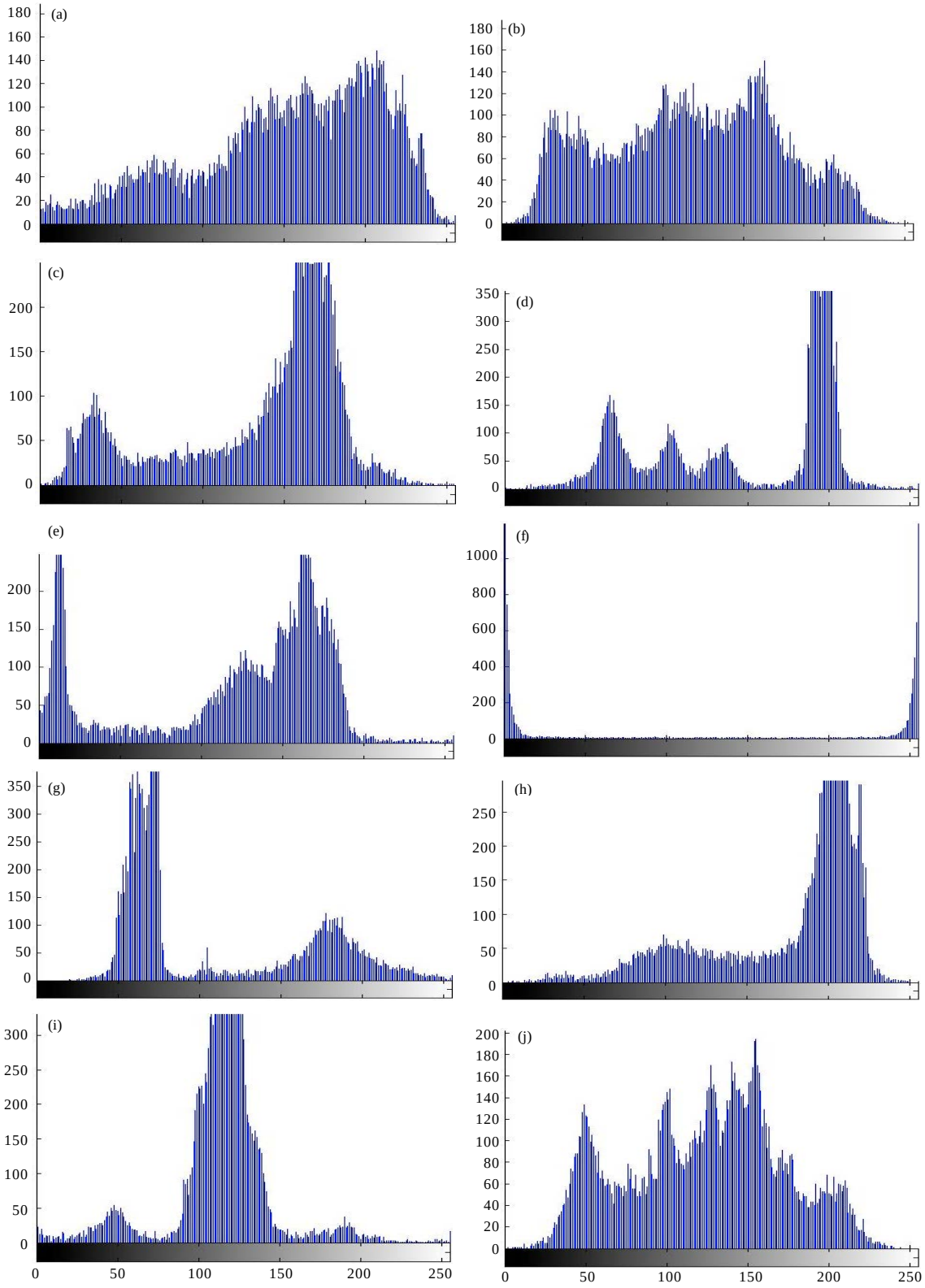

Fig. 3(a-o): Continue

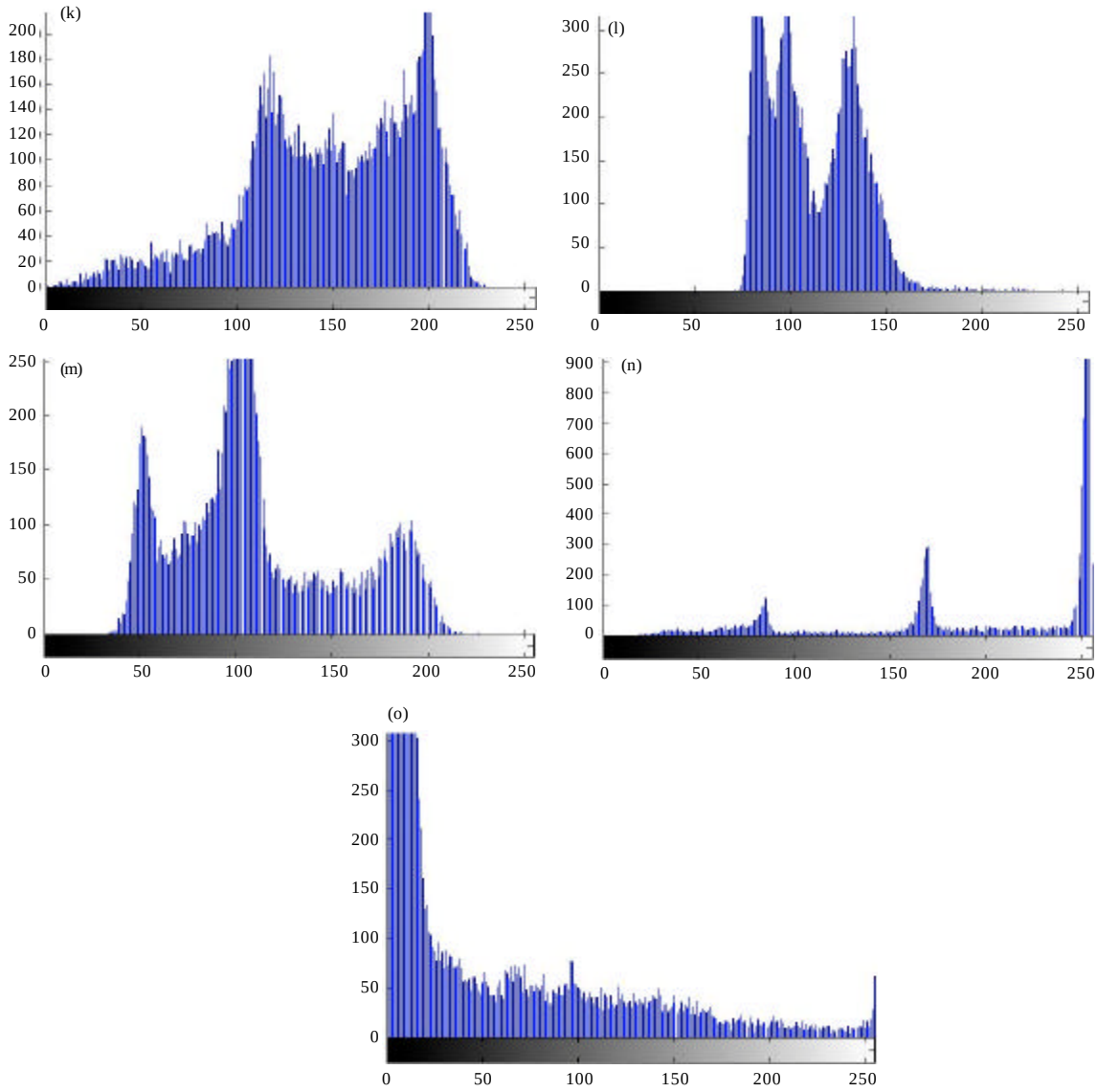

Fig. 3(a-o): Histograms of secret images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (i) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

consumed less than 10,000 and remaining 9 images utilized greater than 10,000 LEs. Table 2 displays the error metrics MSE and PSNR of the secret and encrypted images. Figure 8 shows the snapshot of a section of LabVIEW block diagram used to plot FFT of the secret and encrypted images and error metrics calculation.

Let us consider the two images Rice and Circles which consumed 36 and 15% of the total LEs, respectively. The histogram of Rice image has been shown in Fig. 3m and that of Circles image has been displayed in Fig. 3f. The centralized grayscale distribution of pixels is apparently visible in the histogram of Rice image whereas the histogram of Circles image reveals the presence of very less number of mid range pixels i.e., approximately between the grayscale values 25 and 237. As

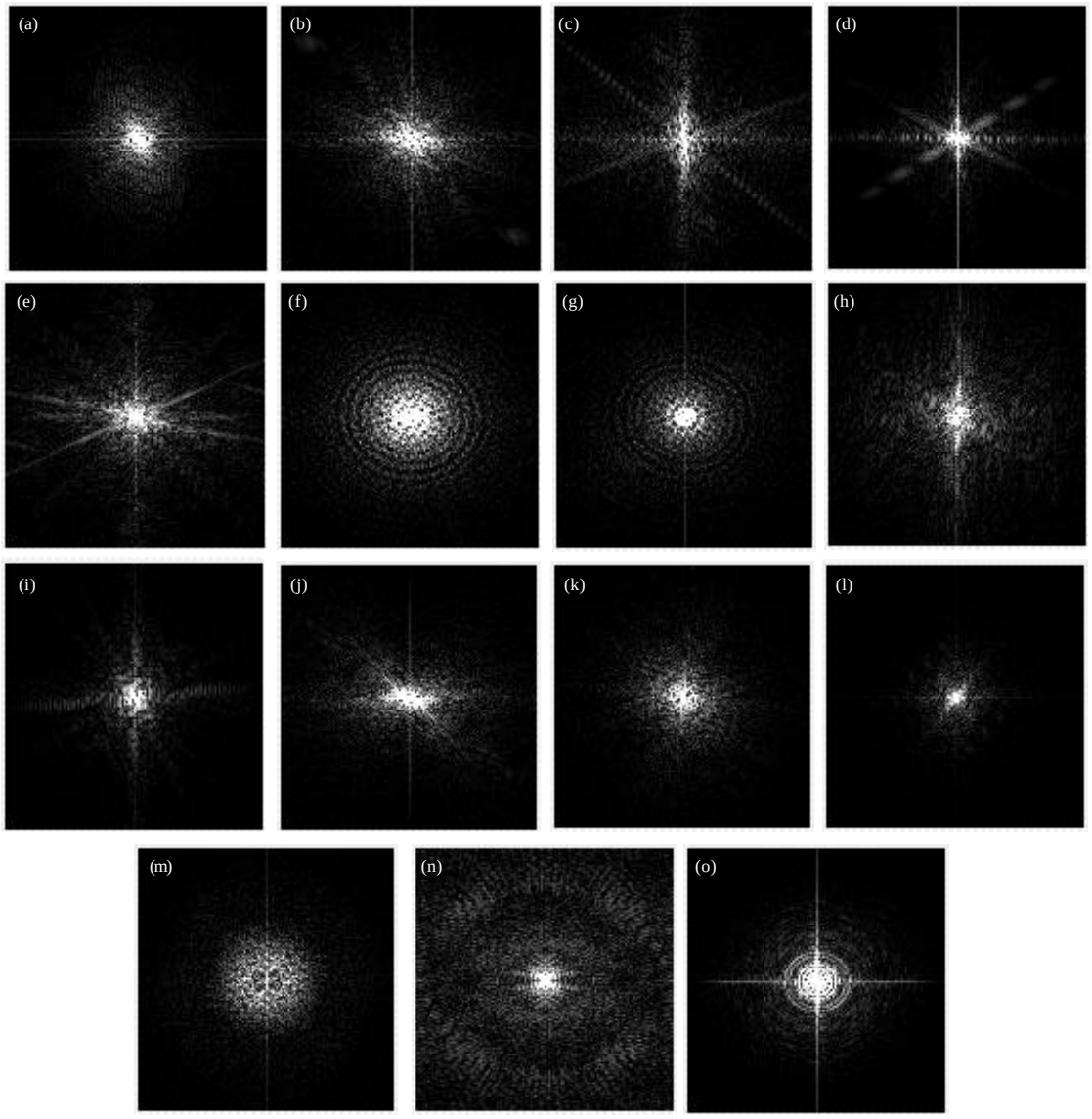

Fig. 4(a-o): FFT of secret images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (I) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

per the histogram report obtained from the LabVIEW, the minimal grayscale value in rice image was 34 and the maximum was 226. But for Circles image, the minimum grayscale value was 0 and maximum being 255. Also the Circles image contains 6913 pixels having a grayscale value "0" and 2532 pixels having a grayscale value of "255". Figure 9 shows the chip planner view of the image encryption of tyre image on FPGA.

Table 3 shows the detailed resource usage summary of the image encryption of rice and circles image. The parameters in the Table 3 depict the netlist elements present in the technology schematics generated during the synthesis and compilation of the image encryption algorithms

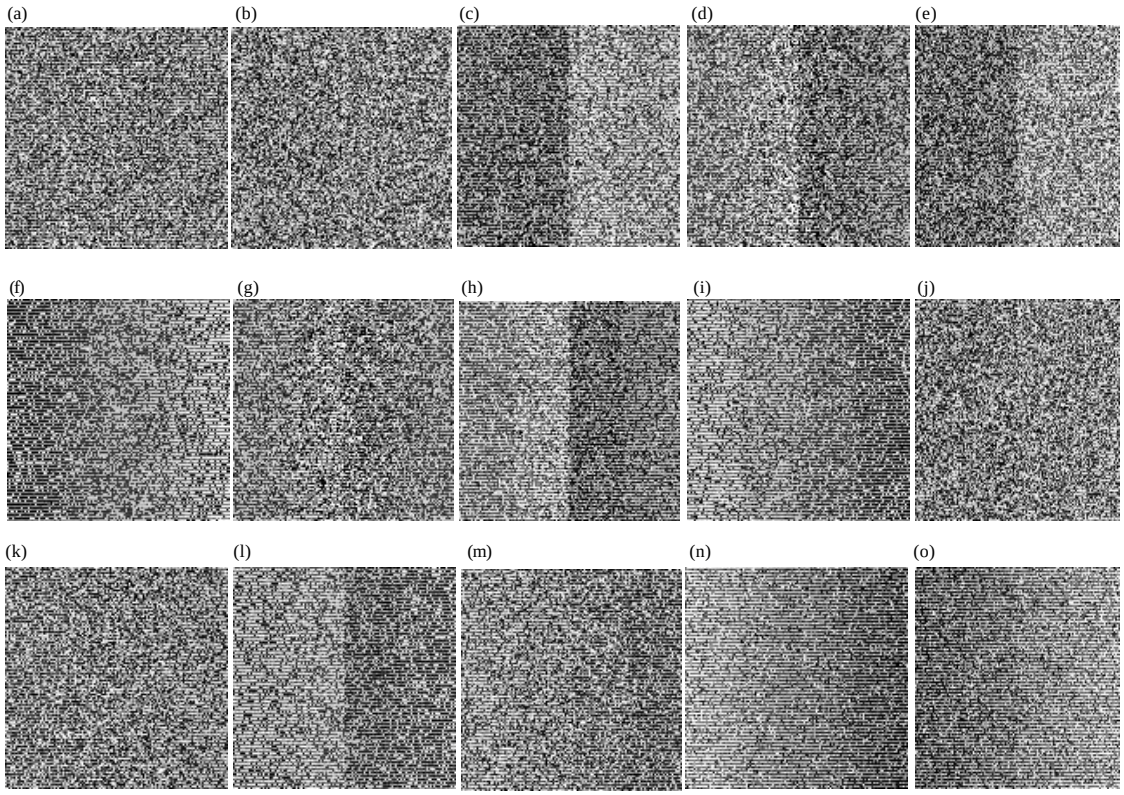

Fig. 5(a-o): Encrypted images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (i) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

Table 2: MSE and PSNR results of the encrypted images

Image type	MSE	PSNR (dB)
Baby	9419.51	8.39052
Barb	8368.58	8.90428
Boat	8730.93	8.72020
Building	9446.84	8.37794
Cameraman	8655.34	8.75796
Circles	20877.70	4.93398
Coins	9247.10	8.47075
Jet	10162.00	8.06100
Jet 1	6842.00	9.77897
Lena	7601.72	9.32168
Peppers	8006.96	9.09612
Pout	6190.38	10.21360
Rice	7473.17	9.39576
SASTRA logo	16773.00	5.88469
Tyre	14780.40	6.43395

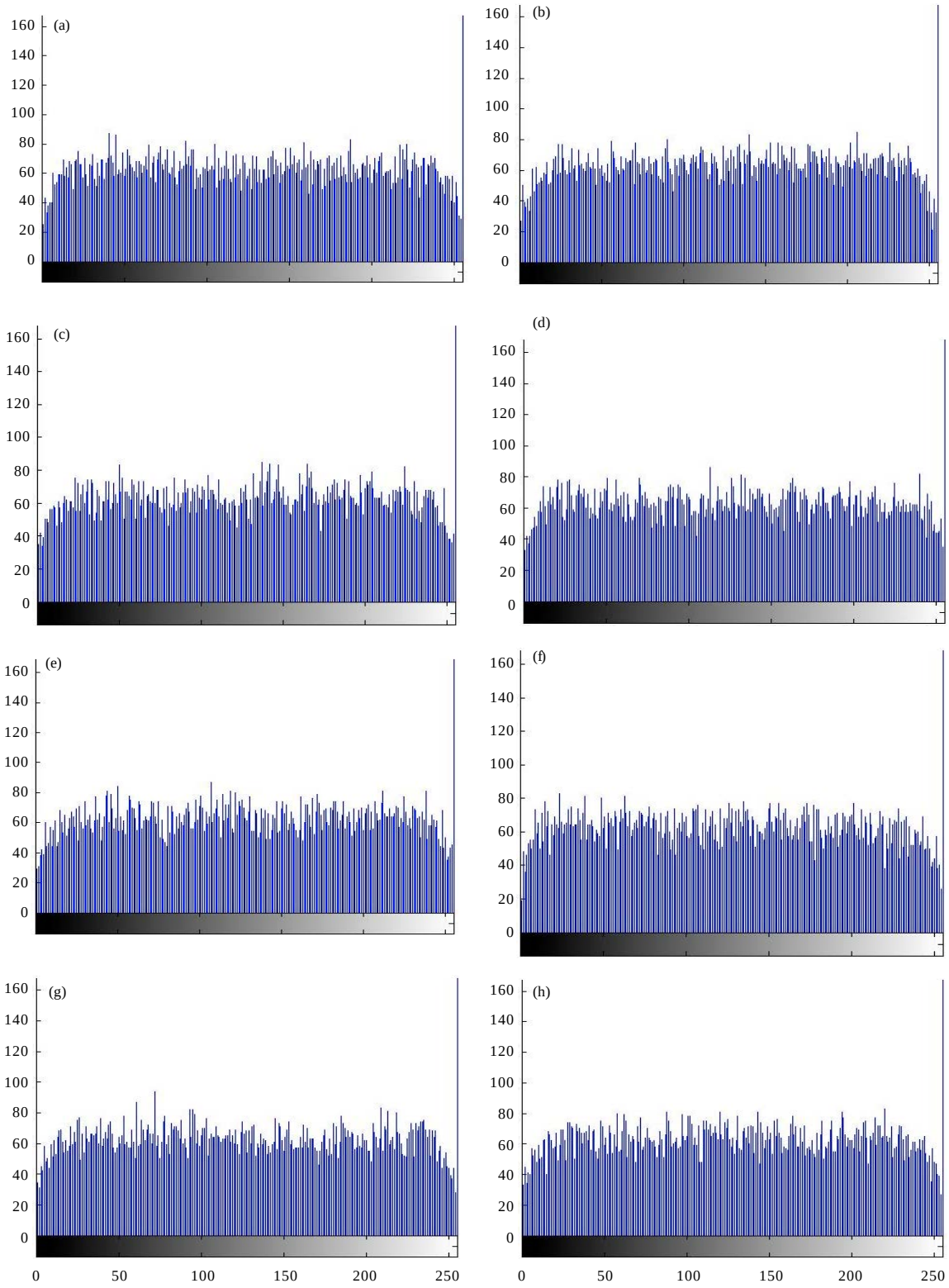

Fig. 6(a-o): Continue

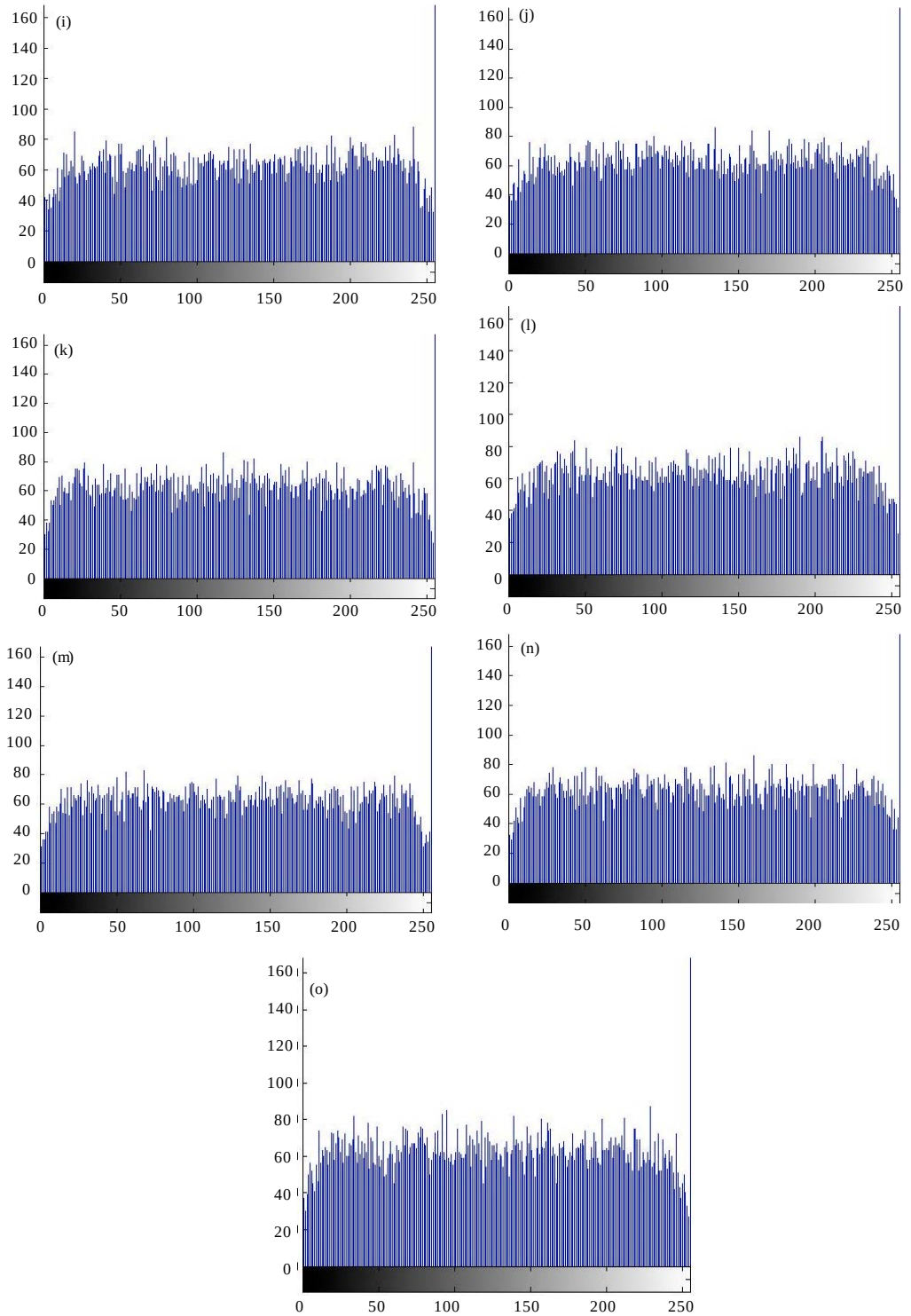

Fig. 6(a-o): Histograms of encrypted images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (i) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

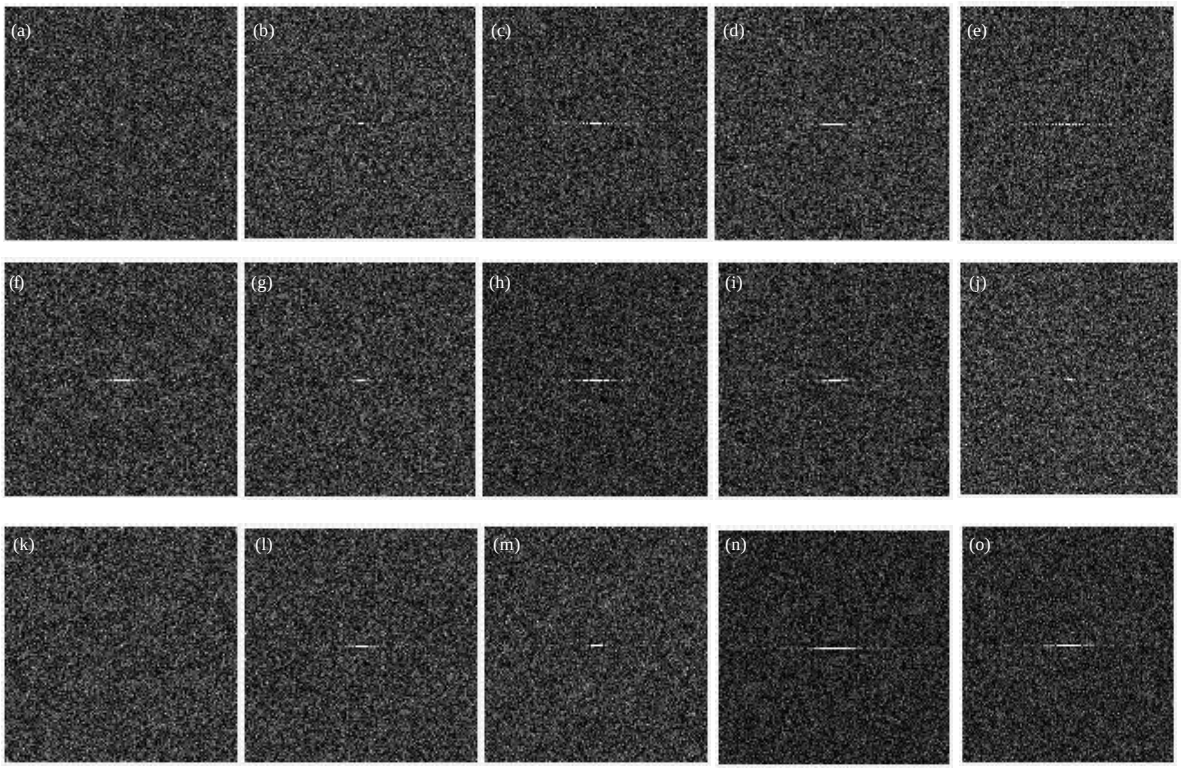

Fig. 7(a-o): FFT of encrypted images of (a) Baby, (b) Barb, (c) Boat, (d) Building, (e) Cameraman, (f) Circles, (g) Coins, (h) Jet1, (I) Jet2, (j) Lena, (k) Peppers, (l) Pout, (m) Rice, (n) SASTRA logo and (o) Tyre

Table 3: Analysis and synthesis resource usage in technology schematics

Parameter	Rice image	Circles image
Estimated total logic elements	11781	5115
Total combinational functions	11781	5115
Logic elements usage by No. of LUT inputs		
4 input functions	11180	4527
3 input functions	466	426
<= 2 input functions	135	162
Logic elements by mode		
Normal mode	11744	5078
Arithmetic mode	37	37
Total registers	167	167
Dedicated logic registers	167	167
I/O registers	167	0
I/O pins	7	7
Total memory bits	131072	131072
Maximum fan-out	4298	1906
Total fan-out	47957	21279
Average fan-out	4	4

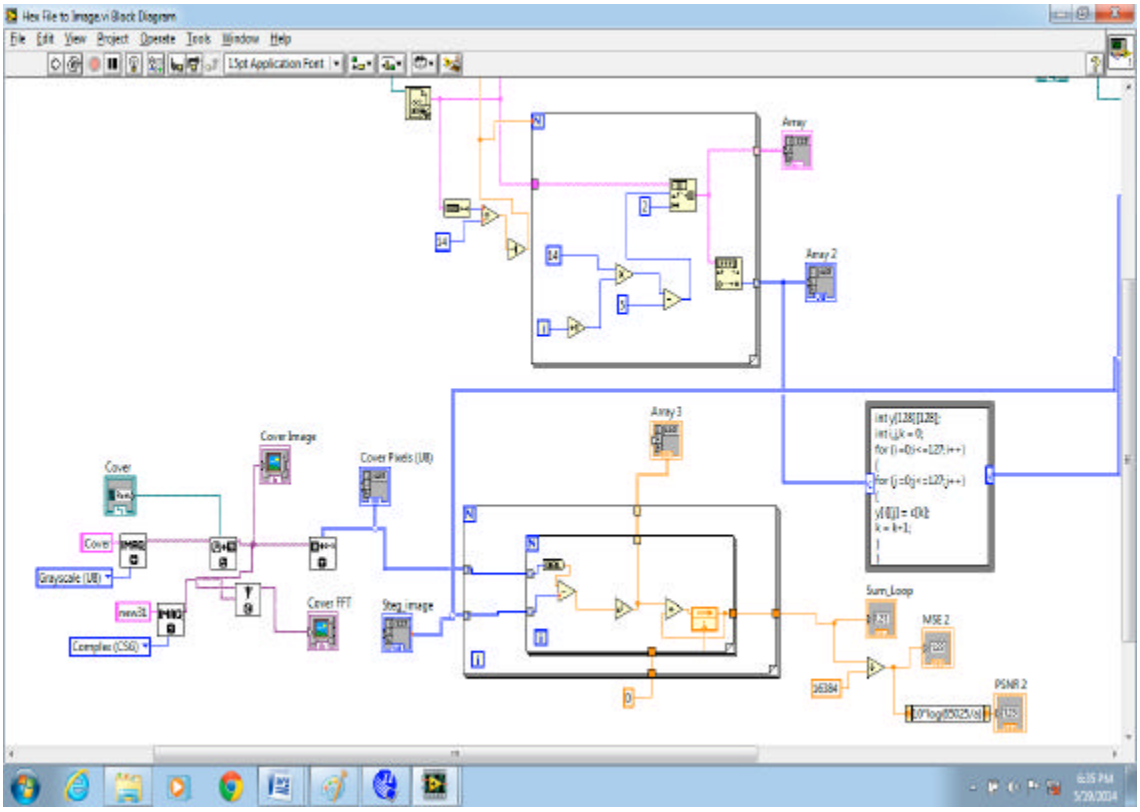

Fig. 8: Section of LabVIEW block diagram for performing analysis and error metrics calculation

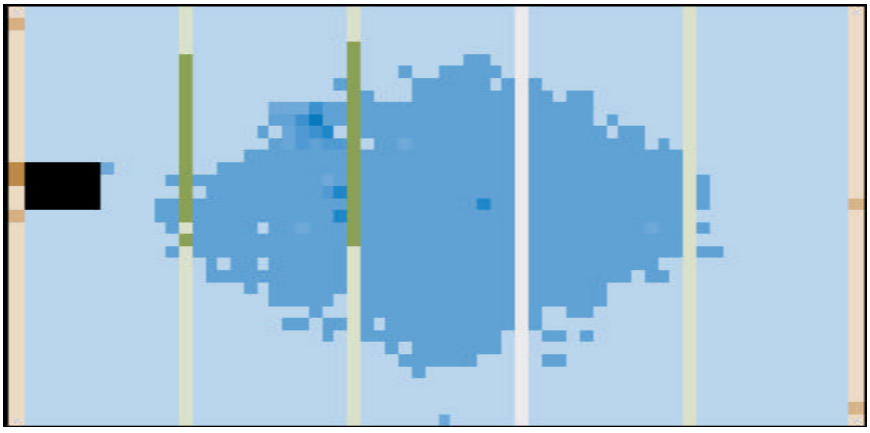

Fig. 9: Chip planner view of the encryption of 128×128 tyre image

carried out on both the images. Due to the presence of various grayscale levels between 25 and 237, the number of four-input functions were 11,180 in Rice image. These combinational functions were mainly required to perform the XOR operation between the grayscale value and 14-bit CA value during every clock cycle of execution. But for Circles image which has 6913 pixels in 0 gray level

and 2532 pixels in 255 grayscale levels, the logic elements have been optimally used where only 4527 four-input functions were taken by the algorithm during the synthesis and compilation process. Similarly the other 13 images consumed different logic elements based on the grayscale dominance and distribution throughout the pixels of the images.

ACKNOWLEDGMENT

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

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. 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, 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.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014k. Coded crypted converted hiding (C^3H)-a stego channel. J. Applied Sci., 14: 1786-1797.

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

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.

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.