Journal of Applied Sciences

ISSN 1812-5654

science alert

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

Journal of Applied Sciences 14 (18): 2139-2148, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.2139.2148

LCC-LSB-FPGA Stego-A Reconfigurable Security

Balakrishnan Ramalingam, Rengarajan Amirtharajan and John Bosco Balaguru Rayappan
School of Electrical and Electronics Engineering, SASTRA University,
Thanjavur, Tamil Nadu, India

Abstract: Information trouncing implants the secret info within a cover file making the former imperceptible. This study suggests an unexampled steganography construct to embed encrypted message bit in a (digital) color image taking up Linear Congruential Generator (LCC) for producing the arbitrary plot in support of pixel preference and elementary Least Significant Bit (LSB) routine for data infixing. This proposal also witnesses optimum embedding competence along with minimum computation complexness and superior image excellence. In order to prove the complexness and superiority of the proposed algorithm, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of the stego image has become calculated and results are reported. The proposed algorithm was implemented in ALTERA cyclone ii FPGA for which design and performance results are presented in the study.

Key words: Linear congruential generator, FPGA, hardware steganography

INTRODUCTION

With the advancement of internet and communication technologies, information sharing has become easier and faster. However, maintaining secrecy and confidentiality of the information being shared between two entities has turned into a specialized area requiring continuous research and development. Cryptography (Schneier, 2007; Salem *et al*., 2011) and steganography (Cheddad *et al*., 2010; Karzenbeisser and Perircolas, 2000; Amirtharajan *et al*., 2012; Provos and Honeyman, 2003; Petitcolas *et al*., 1999; Praveenkumar *et al*., 2012a, b, 2013a-j; Amirtharajan and Rayappan, 2013) are two commonly used methods employed for securing the privacy of the information transmitted between the nodes of the network.

In cryptography, the confidential information is being transmitted is scrambled so that it can be read by only by the intended recipient by unscrambling. Steganography, on the other hand offers solution by hiding the secret data in a multimedia object such as, text, image, audio and video files without being noticed by eavesdroppers. The drawback of the cryptography is that the cryptic messages draw attention of the hackers.

Steganography on the other hand does not reveal the presence of hidden secret information. If the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. In order to provide another layer of security in the steganography, the secret data is encrypted either in spatial or frequency domain, prior to hiding it in the cover object. For embedding in spatial domain several schemes such as Least Significant Bit (LSB) (Chan and Cheng, 2004; Amirtharajan and Balaguru, 2009; Amirtharajan *et al*., 2011; Amirtharajan and Rayappan, 2012a, c; Amirtharajan *et al*., 2013a), Pixel indicator method (Gutub, 2010; Amirtharajan and Rayappan, 2012b; Amirtharajan *et al*., 2013b) and Pixel Value Differencing (PVD) (Amirtharajan *et al*., 2010) have been proposed to encrypt the pixels hidden in the cover image. For frequency domain encryption, the cover image is first transformed using Discrete Cosine Transform (DCT) (Song *et al*., 2012) or discrete wavelet transform (Chen and Lin, 2006) or Integer Wavelet Transform (IWT) (Amirtharajan and Rayappan, 2012d; Thanikaiselvan *et al*., 2012a, b; Thanikaiselvan *et al*., 2013; Ramalingam *et al*., 2014) and the confidential data is hidden in the transformed coefficients of the cover.

Most encryption and data hiding algorithms have been implemented in software, due to the flexibilility. However, software implementation is vulnerable to the security breaches of the operating system in addition to the less throughput arising from the non-dedicated nature of the platform. Reconfigurable devices like FPGAs are attractive solutions for embedding cryptographic and steganography applications and offer higher throughput and security (Ramalingam *et al*., 2014; Rajagopalan *et al*., 2012a, b; Janakiraman *et al*., 2012).

Corresponding Author: Balakrishnan Ramalingam, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

The FPGA has the advantage of low investment cost and provides moderate processing speed. Knowing the review on steganography, This FPGA work is organised as follows hardware work presents reconfigurable hardware architecture for random image steganography in materials and methods with proposed method. There is no implementation hardware LCC PRNG generator enhance security of the algorithm without compromising the computation space and time in existing review. Results and discussion is presented as next section. Final section concludes the proposed method offers better security of the proposed implementation without compromising the computation space and time.

MATERIALS AND METHODS

Functional block diagram of proposed scheme is shown in Fig. 1. Here, data is hidden by LCC random generator and LSB data hiding technique.

Cover and secret data: Here cover file and secret data is chosen, respectively as BMP gray image or color image and encrypted message.

LSB embedding process: LSB embedding technique inserts the secret data bits straight to the cover image's LSB plane in a settled order employing both color and grey images. Because of 8 bit representation, 1 or 2 bits can be buried in grey and monochrome images. 3 bits can be embedded in all the three color components if it is a 24 bit image.

Linear Congruential Generators (LCG): LCG-Linear Congruential Generator method generates pseudo random numbers up to a certain series, after which the sequence starts recurring. This is known as "seed". The level of uncertainty is determined by the values m, a and c:

$$X_{n+1} \equiv (aX_n+C)\%\ M \qquad (1)$$

$$M,\ 0<M$$

$$A,\ 0<M$$

$$C,\ 0 = C<M$$

$$X_0,\ 0\leq X_0<M$$

where, M, modulus input A, multiplier and c, constant.

According to the seed value and constraints, LCC PRNG produces two random progressions founded on Eq. 1. First sequence is to randomly choose M×N image block, second is for selecting the image pixels M×N matrix.

Algorithm for secret data embedding process:

- Input: Cover Image (C) and encrypted message (A)
- Output: Stego Cover (S)
- Step 1: Read the secret message and (Color) cover image (C)
- Step 2: Using the first arbitrary sequence, jumble the secret message
- Step 3: Change the messed up data bits into binary row matrix
- Step 4: Segment the image into 8×8×3 blocks namely B 1, B 2 . . . B n
- Step 5: By means of the random progression two, choose 8×8×3 blocks and divide the RGB plane separately
- Step 6: With random series three, arbitrarily choose the RGB pixels in 8×8 matrices to entrench the secret data
- Step 7: Perform variable bit embedding as given by the user
- Step 8: Merge the RGB planes to produce the stego cover

Hardware architecture: The reconfigurable hardware architecture of data hiding system is shown in Fig. 2. There are four modules which construct the main parts of the hardware: FSM processing unit, SRAM controller, data Embedding unit and LCC random number generator.

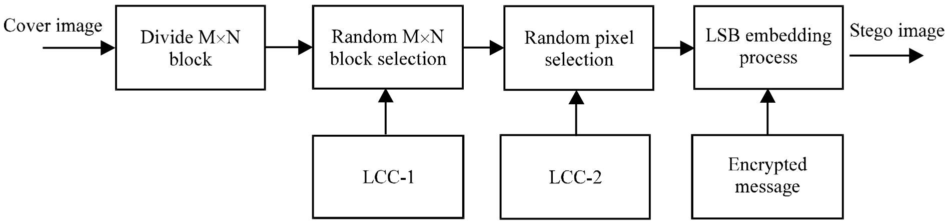


Fig. 1: Block diagram of the data hiding architecture

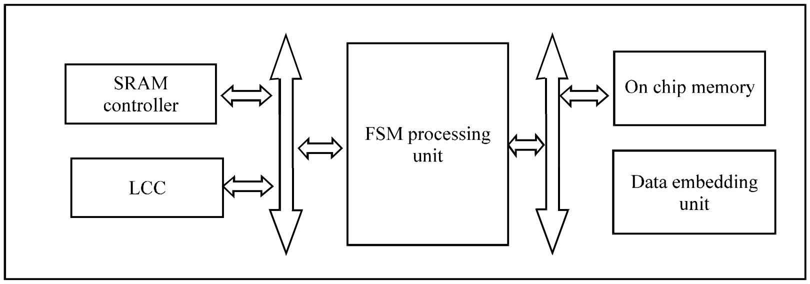


Fig. 2: Data hiding reconfigurable hardware architecture

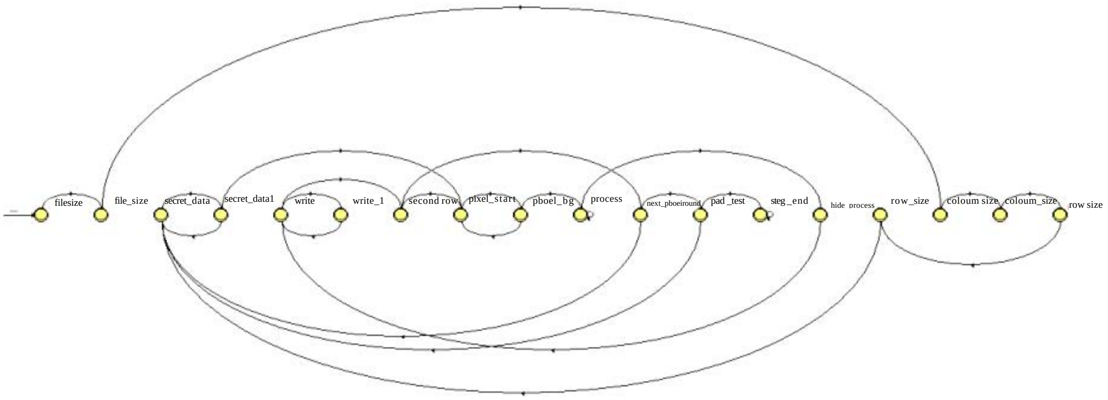


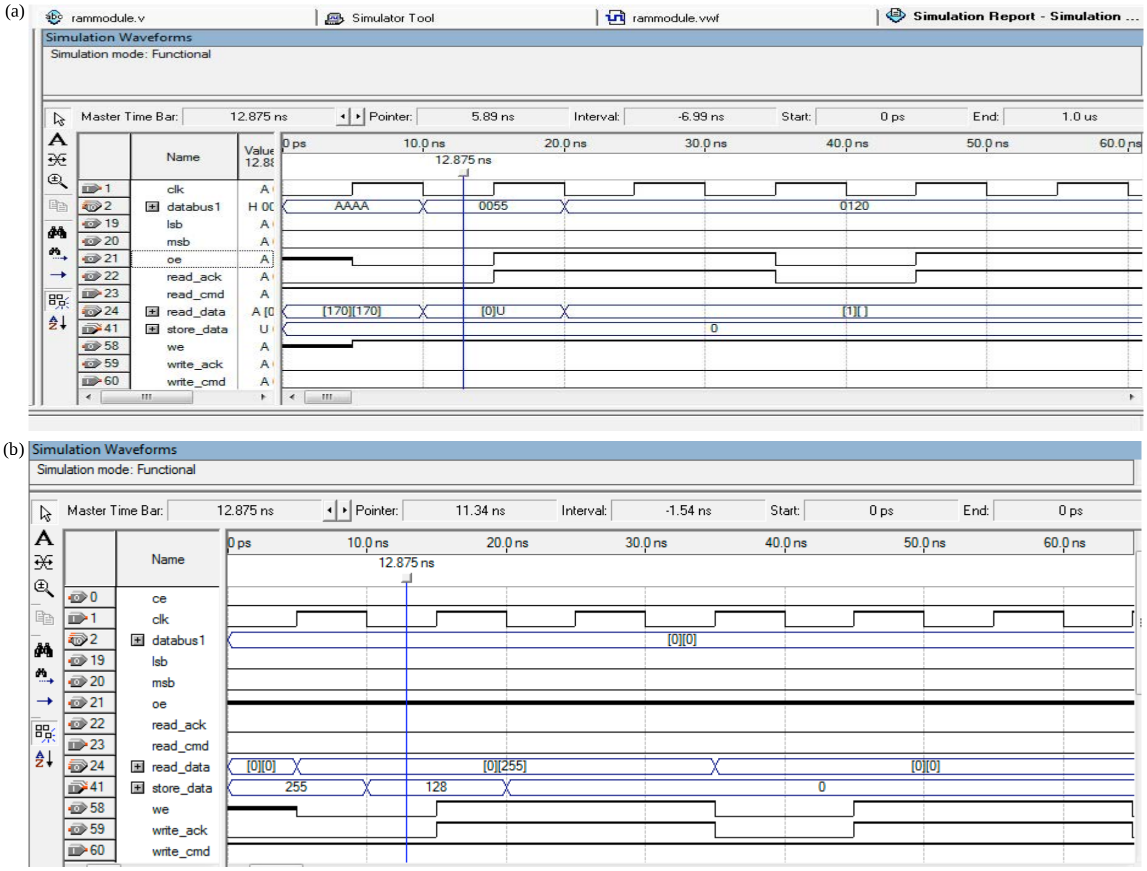
Fig. 3: State diagram of FSM processing unit

FSM unit: The synthesized state diagram of FSM processing unit is shown in Fig. 3. FSM processing unit generates the control signal for SRAM controller, data embedding unit and LCC random number generator. FSM processing unit consists of state decoding logic circuit, timing generation unit, general purpose storage registers and functional registers. Functional registers are used to store the current state, next state and FSM state and header information of the image. General purpose registers are used to store the initial seeds of LCC and count value of embedded message bits etc. Timing and control logic is made of PLL (Phase Lock Loop) which generates the required clock signal to integrated functional hardware components.

SRAM controller: SRAM communication core is used to read or write the data from master device (such as the FPGA). It is composed of 16 bit data bus, 18 bit address bus and four control signals such us read, write and output enable and word or byte mode selection. Timing diagram of SRAM is shown in Fig. 4(a-b). The SRAM Controller supports a clock frequency of 50-200 MHZ. This study uses SRAM Controller to communicate with the 256K×16 asynchronous CMOS static RAM (SRAM) chip on Altera's DE2/DE1 Boards.

On chip embedded memory: FPGA M4K memory bits are configured as dual-port on chip embedded memory which can be used to store the M×N RGB value, encrypted secret message and M×N stego pixels and random key sequence. Schematic diagram of on chip embedded memory shown in Fig. 5. In simple dual-port mode, host can simultaneously carryout read and write operation in memory blocks because dual port memory has separate write enable and read enable signal.

Data embedding unit: Function block diagram of embedding module is shown Fig. 6. It consists of function registers A, B and cascaded AND-OR logic module each of 24 bit wide. Function registers are used to store 24 bit pixel value and secret message bits in substitution process. After hiding the data into image pixel, the pixel value is stored into on chip embedded memory.



Simulation Waveforms

Simulation mode: Functional

Master Time Bar: 12.875 ns Pointer: 5.89 ns Interval: -6.99 ns Start: 0 ps End: 1.0 us

Simulation Waveforms

Simulation mode: Functional

Master Time Bar: 12.875 ns Pointer: 11.34 ns Interval: -1.54 ns Start: 0 ps End: 0 ps

Fig. 4(a-b): SRAM (a) Read and (b) Write timing diagram

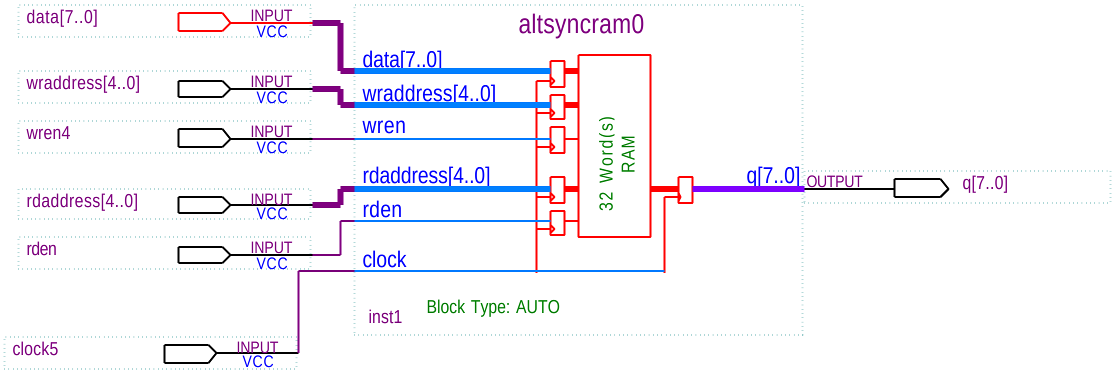


Fig. 5: On chip embedded memory

LCC random number generator: LCC random number generator consists of LFSR, XOR feedback, multiplier adder and modules function and storage buffer. A secret key can be used as an initial seed to generate the random number. RTL view of the LFSR is shown in Fig. 7.

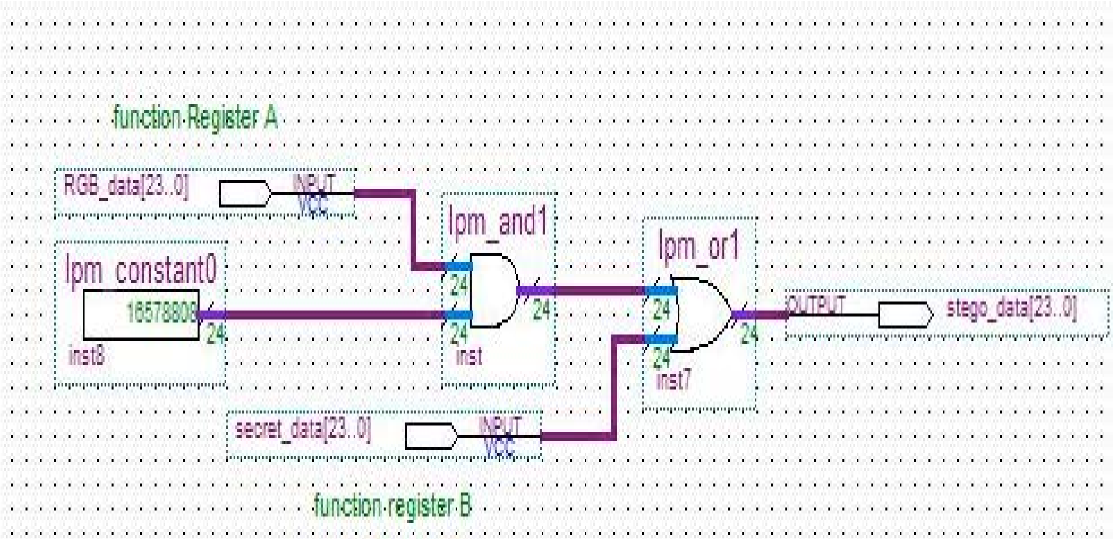


Fig. 6: Function block diagram of embedding module

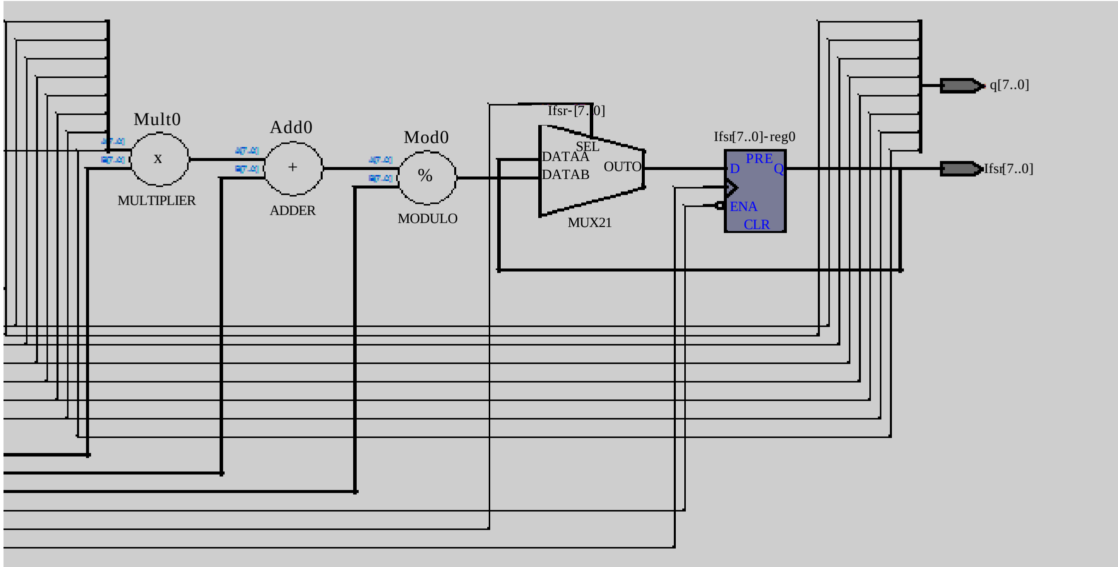


Fig. 7: RTL view LCC random number generator

HARDWARE SYNTHESIZE AND PERFORMANCE ANALYSIS RESULTS

Proposed data hiding architecture has been synthesized in ALTERA QUARTUS II Design software Version 9.0 and tested in ALTERA DE2 development board. It is made up of cyclone ii FPGA and 512 KB on board static SRAM memory. Compilation report of data hiding architecture was given in Table 1. RTL view and design floor planning output of data hiding architecture are shown in Fig. 8(a-b).

Timing analysis: Throughput of data hiding architecture is calculated through ZERO plus logic analyzer modules.

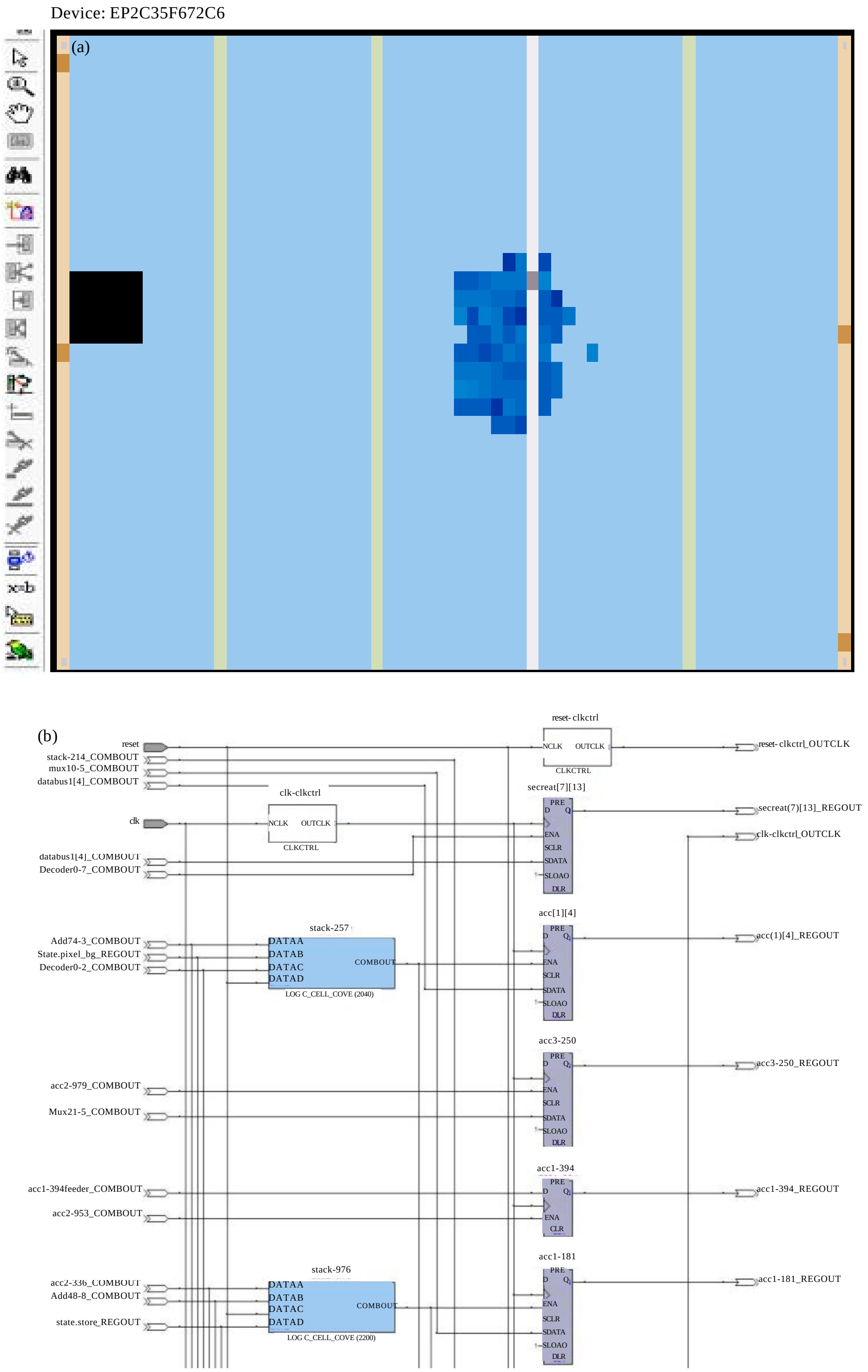
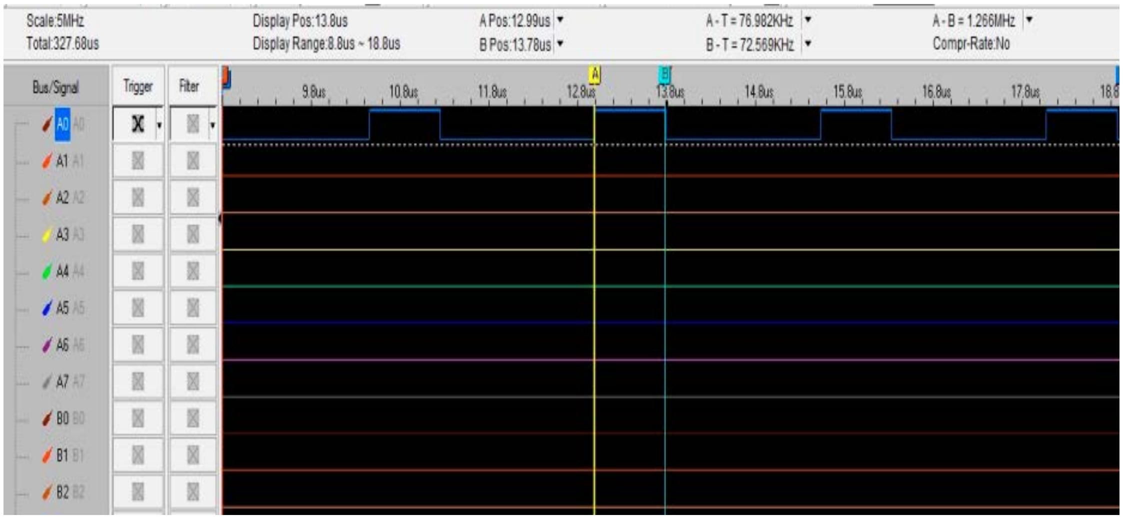


Fig. 8(a-b): (a) Chip planner and (b) RTL view

Figure 9 shows Logic analyzer timing output. The data hiding architecture consumes 0.8 is for RGB separation, random number generation and embedding process in one 8×8 block.



Scale:5MHz
Total:327.68us
Display Pos:13.8us
Display Range:8.8us ~ 18.8us
A Pos:12.99us
B Pos:13.78us
A - T = 76.982KHz
B - T = 72.569KHz
A - B = 1.266MHz
Compr-Rate:No

Fig. 9: Logic analyzer timing output

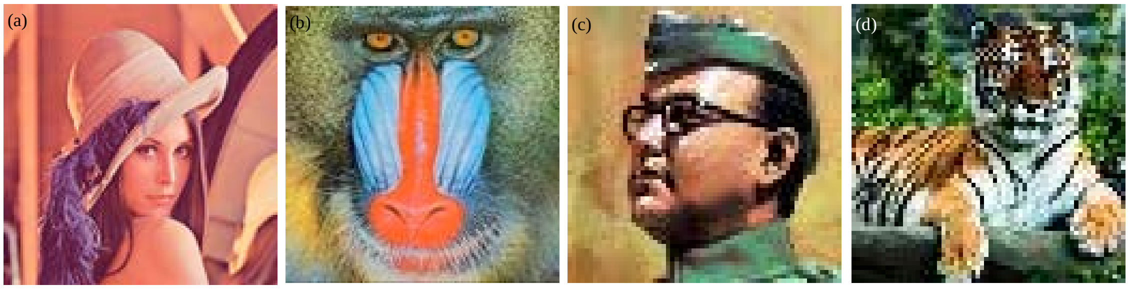


Fig. 10(a-d): Cover images of (a) Lena, (b) Baboon, (c) Netaji and (d) Tiger

Table 1: Compilation report of data hiding architecture

Family	Cyclone II
Device	EP2C35F672C6
Total logic elements	960/33216(3%)
Total combinational function	723/33216(2%)
Dedicated logic register	610/33216 (2%)
Total pins	44/475
Embedded multiplier 9 bit elements	2/70 (3%)

Quality analysis of embedded stego image: In this present implementation, color digital images Lena and baboon of dimension 128×128 have been taken as cover images, which is shown in Fig. 10(a-d). The stego process has been studied by calculating MSE and PSNR for variable k bit embedding and its results are given in Table 2. Figure 11(a-d) shows the stego image for k = (3, 3, 2) scheme.

Mean Square Error (MSE):

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{m=1}\sum_{j=1}^{n=1}(Xij-Yij)^{2} \qquad (2)$$

where, M and N represent the total number of pixels in the Rowand column of the image. Xi, j represents the pixels in the cover image and Yi, j, represents the pixels of the stego-image. Lesser MSE value means higher image quality.

Peak Signal to Noise Ratio (PSNR):

$$\text{PSNR} = 10\log_{10}\left\{\frac{I^{2}_{max}}{MSE}\right\}\text{dB} \qquad (3)$$

where, I max is the peak intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the value of PSNR superior the image quality cover image.

From the Table 2, it is vivid that proposed algorithm provides high PSNR and low MSE for variable bit embedding.

Fig. 11(a-d): Stego images of (a) Lena, (b) Baboon, (c) Netaji and (d) Tiger

Table 2: MSE and PSNR metrics for 128×128 images

Cover image		MSE and PSNR K[R,G,B][3,3,2]		MSE and PSNR K[R,G,B][2,2,2]		MSE and PSNR K[R,G,B][1,1,1]	
Lena	R	5.4930	40.7327	2.5833	44.0091	0.0417	61.9329
	G	5.5112	40.7183	2.5755	44.0221	0.0521	60.9638
	B	2.5905	43.9969	2.5791	44.0161	0.0313	63.1823
Baboon	R	5.3985	40.8081	2.5375	44.0868	0.3945	52.1703
	G	5.5192	40.7120	2.5846	44.0068	0.2143	54.8207
	B	2.5743	44.0240	2.5644	44.0408	0.3424	52.7854
Netaji	R	5.2182	40.9556	2.5778	44.0181	0.2541	54.0806
	G	5.4019	40.8053	2.5510	44.0635	0.2527	54.1043
	B	2.5413	44.0801	2.5401	44.0822	0.4841	51.2815
Tiger	R	5.5135	40.7165	2.5413	44.0801	0.2524	54.0954
	G	5.4752	40.7468	2.5829	44.0097	0.2139	54.8285
	B	2.5644	44.0408	2.5469	44.0705	0.1664	55.9197

CONCLUSION

Proposed data hiding architecture enables the new gateway for hardware based color image steganography for audio data hiding. The speed of the hardware has been sufficient for real time application. It achieves higher throughput for various size color images. LCC PRNG provides the good secure way of hiding the audio in image pixel based on the LSB substitution method. As 30 dB is fixed as the threshold PSNR value for human visual system, the present results possess excellent imperceptibility without noticeable degradation and the same is well supported by the estimated PSNR value for the stego covers.

REFERENCES

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India, pp: 1-6.

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

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.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Chen, P.Y. and H.J. Lin, 2006. A DWT based approach for image steganography. Int. J. Applied Sci. Eng., 4: 275-290.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 56-64.

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

Karzenbeisser, S. and F.A.P. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

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., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013a. Secret link through Simulink: A stego on OFDM channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013c. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013d. Purposeful error on OFDM: A secret channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013e. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013f. Spread and hide: A stego transceiver. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J.

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

Praveenkumar, P., K. Thenmozhi, S. Vivekhanandan, J.B.B. Rayappan and R. Amirtharajan, 2013i. Intersect embedding on OFDM channel-a stego perspective. Proceedings of the IEEE Conference on Information and Communication Technologies, April 11-12, 2013, JeJu Island, pp: 1211-1214.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013j. 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.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

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.

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

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.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., John Wiley and Sons, New Delhi, India.

Song, X., S. Wang and X. Niu, 2012. An integer DCT and affine transformation based image steganography method. Proceedings of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, July 18-20, 2012, Piraeus, pp: 102-105.

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. In: Global Trends in Information Systems and Software Applications, Krishna, P.V., M.R. Babu and E. Ariwa (Eds.). Springer, USA., ISBN: 978-3-642-29215-6, pp: 212-221.

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