International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

FPGA based Data Hiding through Steganography

B. Murali Krishna, Sarat K. Kotamraju, Divya Chepuri, Nagaraju Chattu, Niharika Kamineni

Abstract*: *Nowadays, the information security has been the key factor in communications, computer systems, electronic commerce and data sharing. One of the well-known methods for procuring the security of shared information using carrier files is steganography. The carrier file can be discrete such as image, text, audio and video etc. Digital images are the most commonly used format among those due to the high capacity and availability frequency. The hidden data is stored in an indistinct carrier in image steganography, i.e the digital image is used as a cover image to mask the secret message known as stego image. Cryptography can be then adapted for increasing the security of the stego image. A zig-zag MSB-LSB slicing based steganographic algorithm is proposed in this paper for concealing a secret image in a cover image. Power report and device utilization summary of the algorithm is calculated and the output is demonstrated on the VGA screen using BASYS3 Field Programmable Gate Array (FPGA).

Keywords*: *Cryptography, Steganography, MSB-LSB Slicing, FPGA

I. INTRODUCTION

Image sharing is widely used nowadays for processes like the internet, social networking platforms and military and so on. Conserving the images from unauthorized access has become so crucial. In the emerging era of electronic commerce, there is a need for solving the problem of ensuring confidentiality and data authentication in today's rapidly open communication environment. Data hiding algorithms provide good data authentication and make it difficult for intruders to recover the original image. Requirements such as authentication, integrity, confidentiality and availability need to be considered for safe transmission of information by the usage of the stego images. Cryptography preserves the secret image that is hidden in the cover image while being transported and guarantees that only intended users can access them. Noar and Shamir[1] proposed visual cryptography in the year 1994, which has a notable characteristic of recovering the secret image without any computation. It overcomes the disadvantage of the complexity of the computations in a general cryptography method.

RSA (Ron Rivest, Adi Shamir and Leonard Adleman) is adopted for public and private key generating. The public key is distributed to all users involved in communication where only intended user knows private key. Steganography is an approach of obscuring information within another type of cover medium. The word is derived from Greek - Steganos means “being covered or concealed” and graphe means “script”. Steganography includes a wide range of secret communication methods that conceal the presence of hidden information. Modern steganographic techniques attempt to take advantage of digital media images, audio, video, etc.

In this paper, a contemporary security scheme is intended with steganography based zigzag [2] MSB-LSB slicing. This technique is interpreted using the following sections. Bit-plane slicing is explained in Section-III. Section-IV explains the RSA algorithm and the cryptography basics. Section-V details about steganography. Section-VI gives a detailed explanation of the zig-zag MSB-LSB algorithm that was proposed in this paper. Simulation results were discussed in Section-VII followed by the conclusion.

II. LITERATURE REVIEW

Yang and co-workers [3] proposed a technique with adaptive LSB replacement through which they achieved a high embedding rate and good invisibility of the stego-image. In this method, they use the edge masking characteristics to get the higher-order image by using the higher-order bits of the original image and employed is the adaptive LSB method thus a new steganographic image technique is introduced.

Jose and co-workers [4] proposed a steganographic method founded upon a 3-bit data hiding technique that depends on LSB. In the proposed method, 3-bits of message and image is taken at a time and is embedded to LSB of the cover image. By using this method the sequence mapping can be avoided and it making it difficult for the hackers to decrypt the corresponding stego image. Sharma and Kumar [5] developed a modified LSB method which is founded upon the fact that the pixels consists of the combination of RGB. In this method, the data hiding had been secured by replacing RGB components.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
***Murali Krishna**, Department of Electronics and Communications Engineering, KL Deemed to be University (KLEF), Greenfields, Vaddeswaram Guntur-522502, India. Email: muralikrishna@kluniversity.in
Sarat K. Kotamraju, Department of Electronics and Communications Engineering, KL Deemed to be University (KLEF), Greenfields, Vaddeswaram Guntur-522502, India. Email: kksarat@kluniversity.in
Divya Chepuri, Department of Electronics and Communications Engineering, KL Deemed to be University (KLEF), Greenfields, Vaddeswaram Guntur-522502, India. Email: divyachepuri1999@gmail.com
Nagaraju Chattu, Department of Electronics and Communications Engineering, KL Deemed to be University (KLEF), Greenfields, Vaddeswaram Guntur-522502, India. Email: nagarajuchattu18@gmail.com
Niharika Kamineni, Department of Electronics and Communications Engineering, KL Deemed to be University (KLEF), Greenfields, Vaddeswaram Guntur-522502, India. kamineniniharika@gmail.com

The first byte of secret information is embedded into the first-pixel red component. Then, the second byte of the secret information is embedded into the second-pixel green component.

III. BIT PLANE SLICING

Bit plane slicing [6]is well-known for transforming an image into the respective bit-planes that make up the most important as well as the least significant bits. It has been postulated that higher ordered bits carry most of the image data and that the lower ordered bits can be utilized for potent data hiding and compression phenomena. Bit plane slicing[8] works on three key goals: to obtain a binary image to a gray-level image, to reduce the image size to fewer bit values, and to increase quality by focusing. Figure 1 depicts the bit sliced values for a 3* 3 matrix. The obtained bit planes can be used for the purposes of data hiding, compressing of the image size. This methodology is quite useful for embedding the secret image in a cover image and to evaluate the relative value of each bit in the image. It also provides an option to decide the number of meaningful bits that are required for quantizing the image. This methodology is quite useful in fields such as media files compression, neural networks and estimation of video motion.

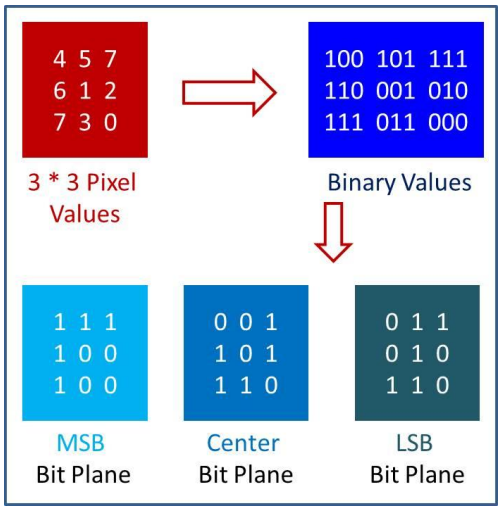

Fig. 1. Bit slicing mechanism

IV. CRYPTOGRAPHY

4.1. Cryptography:

Cryptography (take from the Greek – meaning "code writing") is the art of tuning the original message into an unreadable code that allows the confidentiality of data. Converting the information to make the information safe from an intruder is an art and science. Cryptography includes the encryption and decryption process. The five main functions involved in cryptography are: security, encryption, integrity, non-repudiation and key exchange. Three different types of cryptographic algorithms are extinct:

1) Symmetric key cryptography.
2) Asymmetric key cryptography.
3) Hash function.

4.2. RSA Algorithm

RSA was refined by Rivest, Shamir and Adleman in 1978 and is considered as the highest predominant asymmetric key cryptographic method for riskless information transportation. Public key generation is based on two random prime numbers which are put up as forth an auxiliary number. Knowledge of these prime numbers and decryption methodology is vital. The dominant steps for the RSA cryptography are: public and private key generation; encryption and decryption of images as shown in Figure 2.

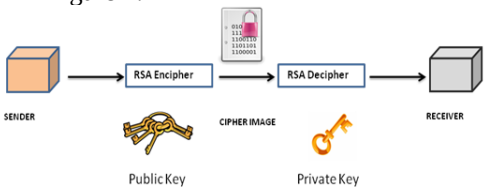

Fig. 2. RSA cryptography methodology

Exchange of key which is kept as a secret is not necessary for the process of encrypting of image. But, for revealing the decrypted image that contains the original image, there is a need to know the secret image. at the receiver end. The knowledge of the value 'A' is needed for both the sender and the receiver. Let 'P' be the public key which can be known to both the transmitter and the target receiver. Now, 'S' is considered as the private key which should be shared only to the receiver.

Key Generation

1. Choosing random large prime integers x, y
2. Find n = xy
3. Select an integer k such that $1<k<\phi(n)$, and k is a co-prime to $\phi(n)$.
4. Find z satisfying $d.k \equiv 1$

Absolute value (n,k) can be treated as a publicly shared key. The privately shared key is a composition of x, y, and its' constant z is kept as a secret.

V. STEGANOGRAPHY

Different efforts are made in olden days to conceal the hidden message through a secure network to transmit through the enemy territories. The Germans invented the Microdot technique during World War II. Data was reduced in size, especially photos, until it was the size of a dot which is of micrometer dimension. After making sure that the message is extremely difficult to spot, the message is then transmitted through the reliable medium with the details of the secret suppressed on one of the pages. An occultist, called Trithemius, coined the term steganography for the first time. Steganography[9] is an approach of obscuring information within another type of cover medium. The word is derived from Greek words, Steganos means "being covered or concealed", and graphe means "script". It includes a wide range of secret communication methods that conceal the presence of hidden information.

Modern steganographic techniques attempt to take advantage of digital media images, audio, video, etc. [7]

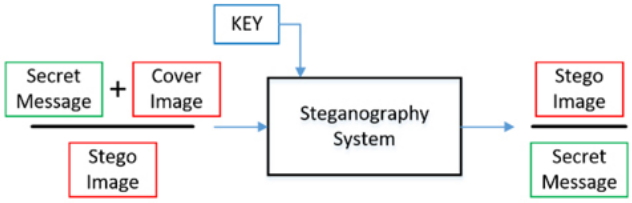

Fig. 3. A steganography system

VI. PROPOSED METHOD

Zig-zag MSB-LSB algorithm is an established method for visual secret sharing where an image is divided into n slices. The knowledge of all n slices might decrypt the image, but n-1 slices will expose no data regarding the secret image. If all the n slices are assembled, then the only secret image will be obtained, otherwise, it will not be projected. Steganography of pictures is an established procedure to cover-up data inside an image. Images are categorized into various categories such as primary color (RGB) based images and greyscale intensity images. In cage of the RGB based images, the Red, Green, and Blue are the three major constituents with an intensity range of [0 255]. Mainly, steganography of pictures has been employed to cover-up data inside an image [7]. The contended methodology acknowledges an RGB image and extracts the respective planes to store the secret data which is in the form of an image in the LSB bits of the R, G planes of the image which could be emphasized from the subsequent steps as follows.

Step 1: A RGB image that needs to be reflected as a cover image is taken and isolated into its respective R, G, B planes using MATLAB tool.

Step 2: The secret image is encrypted using an asymmetric technique in cryptography, i.e., the RSA algorithm mentioned as follows.

(a) Enumerate mod(n) for private, public key
n=x*y=4*5=20
(b) $\phi(n)=(x-1)*(y-1)=3*4=12$
(c) Select an integer k such that $1<k<\phi(n)$
and k is a co-prime to $\phi(n)$; 'k'=5
(d) Find privately shared key 'z', satisfying $d.k\equiv1$
i.e k*d=a* $\phi(n)$+1 where a is any integer
For a=27 the z=65

Step 3: Secret image that is encrypted is now embedded in the LSB bits of the red and green planes of the cover image. All the planes are combined again and the so obtained image is acclaimed as the stego image.

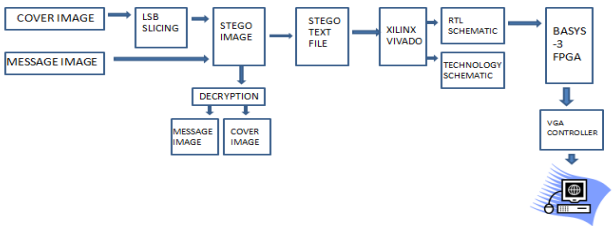

Fig.4. Flow chart of the proposed algorithm

VII. RESULTS AND ANALYSIS

Analysis of the hardware results as well as software simulations was briefed in this section. Taking two different images, the respective stego image corresponding to the cover and secret images generated using MATLAB tool which are provided in Figures 5a and 5b.

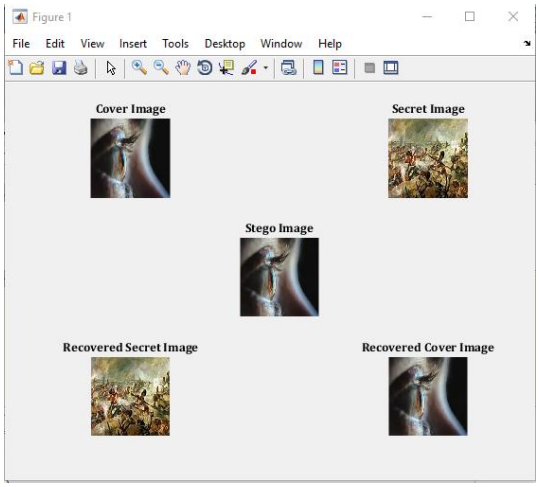

Fig. 5a. Software implementation of Image-1

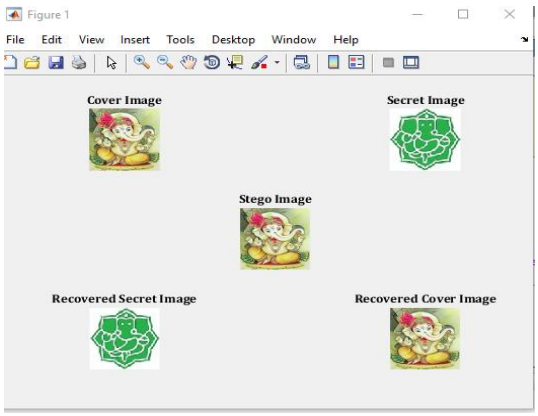

Fig. 5b. Software implementation of Image-2

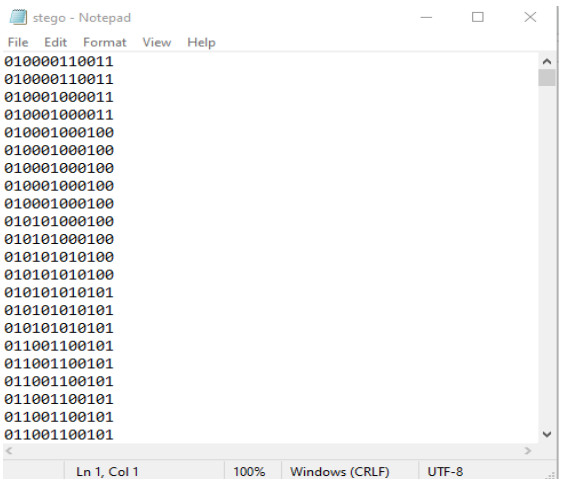

Fig.6. Binary text file of stego image

Figure 6 shows the binary file generated analogously to the obtained stego image which contains the secret image embedded in zig-zag MSB-LSB positions. This binary file is used to figure out the RTL and technology schematics of the stego image as shown in Figure 7 and 8. RTL schematic is utilized for exhibiting the design in terms of generic basic gates like AND, OR, adders, and so on. The technology schematic is used to represent the design at a higher level by replacing the basic elements with LUT's, buffers, and other technological peripherals.

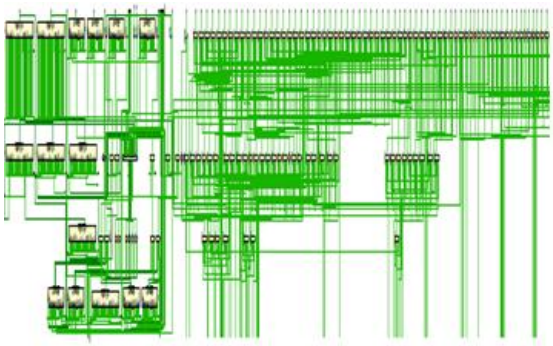

Fig. 7. RTL schematic of the proposed system

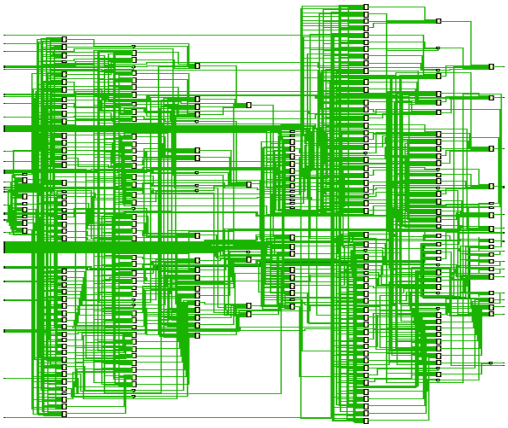

Fig. 8. Technology Schematic of the proposed system

Basys 3 FPGA (Artix-7) architecture is used for hardware implementation for displaying on VGA monitor shown in Figure 9 and the efficiency of the design is given by Static and Dynamic power utilization in a detailed power report as in Figure 10 using Xilinx Power Analyzer.

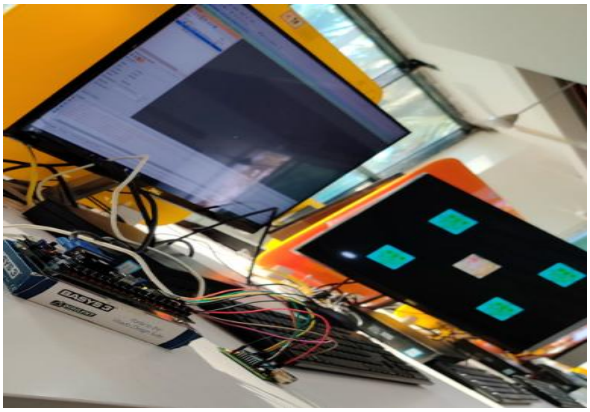

Fig. 9. Hardware implementation of the system

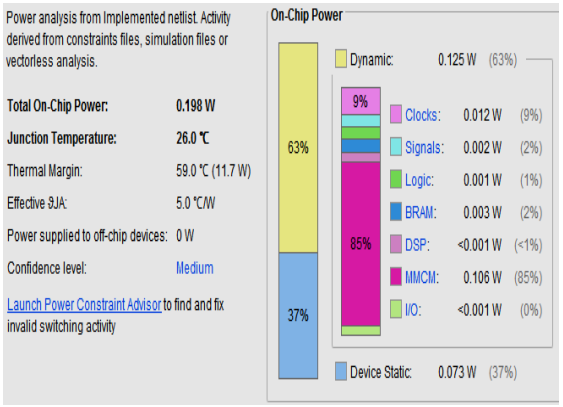

Fig. 10. Power report of the proposed system

VIII. CONCLUSION

To intensify the data authentication, the zig-zag MSB-LSB algorithm is established for secret image sharing. This method can be used to distract hackers from sharing the original confidential information. The admixture of cryptographic and steganographic methods has benefited shielding the secret image from the intruders while sharing in open access media. The succession of the cryptographic system and stenographic system may decrease the liability to breach the data authenticity. Addition of dynamic partial reconfiguration to the algorithm is highly secure against vulnerability attacks in channel.

ACKNOWLEDGMENT

We acknowledge KL University for a generous funding.

REFERENCES

1. H.-M. Sun, M.-E. Wu, W.-C. Ting, M. Hinek, "Dual RSA and its security analysis. Information Theory" *IEEE Transactions*, 2007, vol. 53, pp. 2922–2933.
2. K. B. Padeppagol, M. H. Sandhya Rani, "Design and implementation of lifting based wavelet and adaptive LSB steganography to secret data sharing through image on FPGA" *International Journal of Engineering and Management Research (IJEMR)*, 2018, vol. 8, pp. 112–119.
3. C.-C. Cang, H.-W. Tseng, "Data Hiding in Images by Hybrid LSB Substitution" 2009 Third International Conference on Multimedia and Ubiquitous Engineering, *IEEE*, pp. 360–363.
4. M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", *IJSR*, 2014, vol. 3, pp. 2281–2284.
5. V. Sharma, S. Kumar, "A new approach to hide text in images using steganography", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, 2013, vol. 3, pp. 701–708.
6. Z.-A. Jamal, Ahmadabadi, M. S. Ebrahim, A. Latif, "An Adaptive Secret Image Sharing with a New Bitwise Steganographic Property" *Information Sciences*, 2016, vol. 369, pp. 467–480.
7. X. Wu, C.-N. Yang,. (). Invertible secret image sharing with steganography and authentication for AMBTC compressed images. Signal Processing: Image Communication. 2019, vol. 78. pp. 437–447.
8. "A block based data hiding method in images using pixel value differencing and LSB substitution method", Tasnuva Mahjabin, Syed Monowar Hossain, Md.Shariful Haque, 15th International Conference on Computers and Information Technology,pp.168-172
9. "An adaptive secret image sharing with a new bitwise steganographic property" Jamal Zarepour-Ahmadabadi ,MohammadEbrahim Shiri Ahmadabadi, AliMohammad Latif- ELSEVIER volume:369.