DESIGN AND IMPLEMENTATION OF SELECTIVE INFORMATION RETRIEVAL FROM STEGO ENCRYPTED IMAGE

Ashwini C[1], Prof. Leelavathi G[2], Dr.Siva S Yellampalli[3]

[1,2,3] *Department of VLSI Design and Embedded Systems, VTU Extension Center, UTL Technologies, Bangalore (India)*

ABSTRACT

The work proposes a scheme of separable reversible information hiding (RIH) for encrypted images (EIs) in which hidden information can be extracted from an EI carrying information without image decryption. The proposed scheme firstly encrypts an image and simultaneously prepares room for RIH by two permutation ways. Information is, then, hidden into the EI by Passcode Based Approach for Hiding Classified Information in stego images and the EI carrying information is sent to a receiver. According to keys which the receiver has, he/she is allowed to take seven different actions, whereas the conventional scheme offers only three. This feature of the proposed scheme extends applicable scenarios. Moreover, the proposed scheme always recovers the original image, whereas the conventional scheme sometimes fails to do.

Keywords: Reversible Information Hiding, Encrypted Images, Steganography.

I. INTRODUCTION

In the information age, sharing and transfer of data has increased tremendously and usually the information exchange is done using open channels which can make it vulnerable to interception. The threat of an intruder accessing secret information has been a continuing concern for data communication experts. In this world of increasing electronic connectivity of viruses, hackers, eavesdropping and electronic fraud, electronic security is necessary for transmitting secure electronic-data across insecure networks such as the internet and wireless media. This has led to millions of sensitive data transferred from one party to another over unsecured communication channels. Most of the transferred data contains confidential messages. If these data fell into the wrong hands, they can manipulate and use the information for causing loss to others. So there is a need to provide a secure crypto system which provides high security to any sensitive data.

Cryptography is the fundamental component for securing the Internet traffic. However, cryptographic algorithms impose tremendous processing power demands that can be a bottleneck in high-speed networks. The ultimate solution for the problem would be an adaptive processor that can provide software-like flexibility with hardware-like

performance. Steganography (SG) is one of many techniques used to overcome this threat. It is a technique in which communication between two parties is done in a covert fashion using a cover object. Steganography is the art of invisible communication by concealing information inside other information. The term steganography is derived from the Greek and literally means "covered writing". A steganography system consists of three elements: cover-object (which hides the secret message), the secret message and the stego-object (which is the cover object with message embedded inside it.).

In general, the embedding operation in SG requires a digital medium to carry the data. Images and multimedia components, such as video and audio files, are widely used and exchanged through the internet. Such mediums are the best cover media to hide messages. Digital images are the most widespread cover files used for SG, due to their high embedding efficiency and the insensitivity of the human visual system (HVS). Different steganographic techniques focus on a variety of requirements such as robustness, tamper resistance, imperceptibility, security and capacity. Our embedding technique is focused on providing security while maintaining imperceptibility.

II. PROPOSED SCHEME

A separable RIH scheme in EIs shown in Figure 1 is proposed here which the scheme takes a hierarchy into account.

2.1 Sender Side

From $X \times Y$-sized original image $\mathbf{f} = \{ f(x, y)\}$ with Q-bit pixels, tonal distribution $\mathbf{h} = \{h(v)\}$ is obtained to find $v_{max} = \text{argmax}_v\, h(v)$ and $v_{min} = \text{argmin}_v\, h(v)$. A location map indicating position of pixels with v_{min} is derived, and v_{min}'s in $\mathbf{f}$ are replaced by $v$max to form modified image $\mathbf{f'} = \{f'(x, y)\}$. Histogram permutation table $\mathbf{T}_{hist} = \{t_{hist}(v)\}$ is generated by a PR number generator (PRNG) with key $K_{enc,hist}$ where $t_{hist}(v_{min}) = t_{hist}(v_{max}) - 1$, and $\mathbf{f'}$ is permuted with $\mathbf{T}_{hist}$ to get histogram permuted image $\mathbf{p} = \{p(x,y)\}$. Image $\mathbf{p}$ is permuted with spatial permutation table $\mathbf{T}_{spa} = \{\mathbf{t}_{spa}(x,y)\}$ obtained by a PRNG with key $K_{enc,spa}$ to generate encrypted image $\mathbf{c} = \{c(m,n)\}$ where $(m,n) = \mathbf{T}_{spa}(x, y)$. From $\mathbf{c}$, tonal distribution $\mathbf{d} = \{d(a)\}$ is obtained to find $a_{max} = \text{argmax}_a\, d(a)$. L-bits payload $\mathbf{w} = \{w(l)\}$ is interleaved by table $\mathbf{T}_{hide} = \{t_{hide}(l)\}$ derived by a PRNG with key K_{hide} where $t_{hide}(l) \in \{0,1, \ldots, d(a_{max}) - 1\}$ and hidden to $\mathbf{c}$ based on a RIH technique [5] where $L \leq h(v_{max}) = d(a_{max})$, and encrypted-and-stego image $\hat{\mathbf{c}} = \{\hat{c}(m,n)\}$ is obtained.

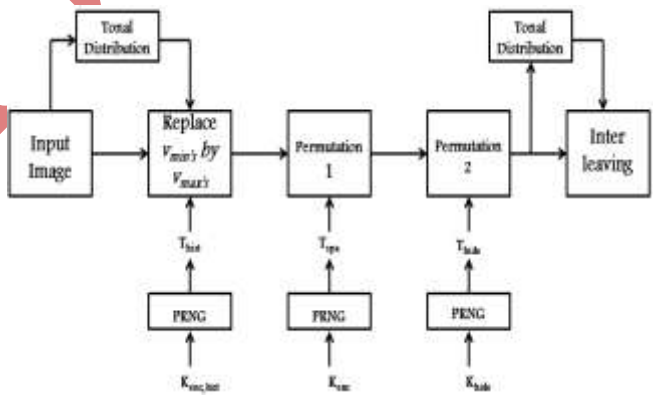


Fig 1: Proposed System

2.2 Receiver Side

A receiver who knows a_{max} and K_{hide} extracts **w** from ĉ but he/she never get either original image, a decrypted image, or a partially decrypted image. A receiver having *K*enc,spa obtains partially decrypted image $\hat{\mathbf{p}} = \{\hat{p}(x, y)\}$ where $\hat{\mathbf{p}}$ is spatially decrypted but still encrypted with histogram permutation. One who has $K_{enc,spa}$, and $\mathbf{T}_{hist}$ gets decrypted image $\hat{f}' = \{\hat{f}'(x, y)\}$ where $\hat{f}'$ is visible but is still distorted by hiding **w**. One having $K_{enc,spa}$, $\mathbf{T}_{hist}$, the location map, v_{max}, and v_{min} recovers original image **f**. A receiver knowing a_{max}, K_{hide}, $K_{enc,spa}$, $\mathbf{T}_{hist}$, the location map, v_{max}, and v_{min} gets **w** and **f**.

2.3 Features

The proposed scheme has two features; taking a hierarchy into account and always recovering the original image. The former is achieved by histogram permutation and spatial permutation. A decrypted-and-stego, a partially decrypted, a decrypted, and the original images are in the proposed scheme, i.e., four privilege levels are taken into account, whereas the conventional scheme considers only two. The latter is actualized by using a complete RIH technique , whereas the conventional scheme sometimes fails to recover the original.

III. FLOWCHART FOR EMBEDDING THE DATA

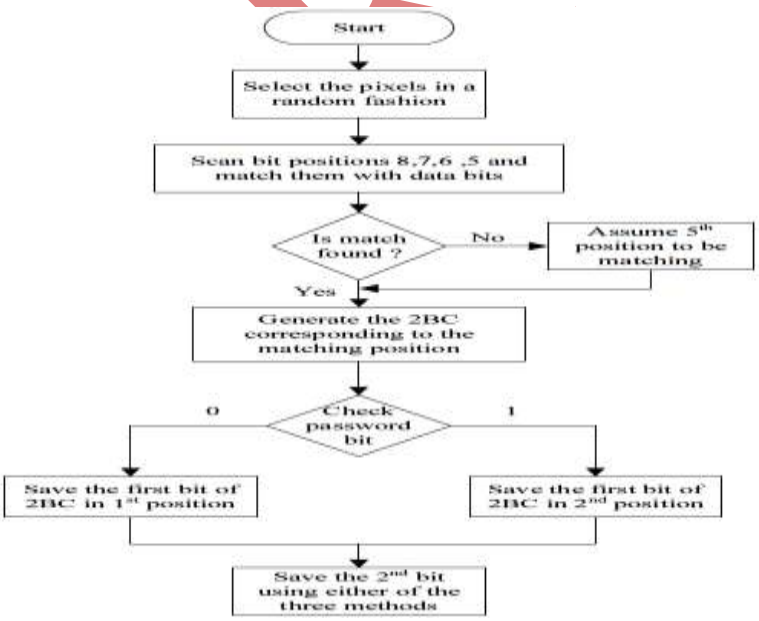


Fig 2: Flowchart for Embedding the Data.

IV. SOFTWARE IMPLEMENTATION

In this section first we will discuss the implement of the proposed system in MATLAB. There are mainly four steps involved in implementing LSB steganography as shown below.

1) Conversion of image to matrix

2) Embedding process

3) Conversion of matrix to image

4) Extraction process

4.1 Conversion of Image to Matrix

In the conversion process of image to matrix we convert the input cover image into matrix values which is stored in a text file. Firstly an image is read from computer, the original image is in the form of RGB which is converted into grey image. The grey image is resized to a particular size of 256*256. Each image has intensity values for every pixel, here these intensity values are stored into a text file. Figure 3 shows the colour cover image used. In the Figure 4 the intensity values of colour cover image, obtained during the conversion of image to matrix is represented. Figure 5 shows the colour to grey cover image used. In the Figure 6 the intensity values of colour to grey cover image, obtained during the conversion of image to matrix is represented. Though MATLAB has got inbuilt functions for steganography, we follow this method since we are trying to embed this on a FPGA and FPGA cannot read JPEG images. It reads only the intensity values of the images called pixels.

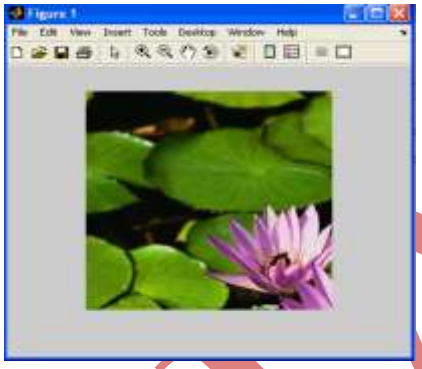


Fig 3: Cover Image

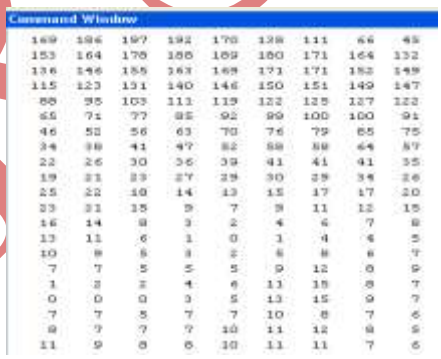


Fig 4: Intensity Values Of Cover Image

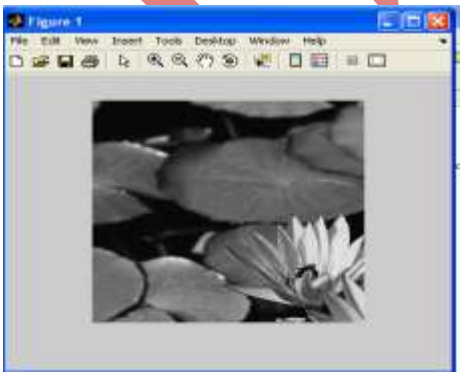


Fig 5: Colour to Grey Image

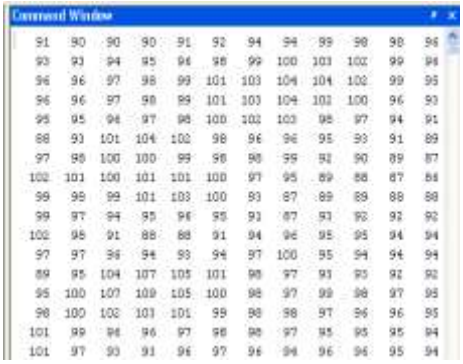


Fig 6: Intensity Values of Colour to Grey Image

4.2 Embedding Process

After completion of image to matrix the next step is to embed a message into an image. In this project we embed a message bit into the least significant value pixel value of an image by only bit wise. The image obtained during this process is called as stegano-embed image. The message is embedded into the intensity values of image obtained during image to matrix conversion. The flowchart of embedding a message into an image is shown in Figure 7. The message is embedded into all 256*256 pixels of image. Figure 8 shows the stegano image.

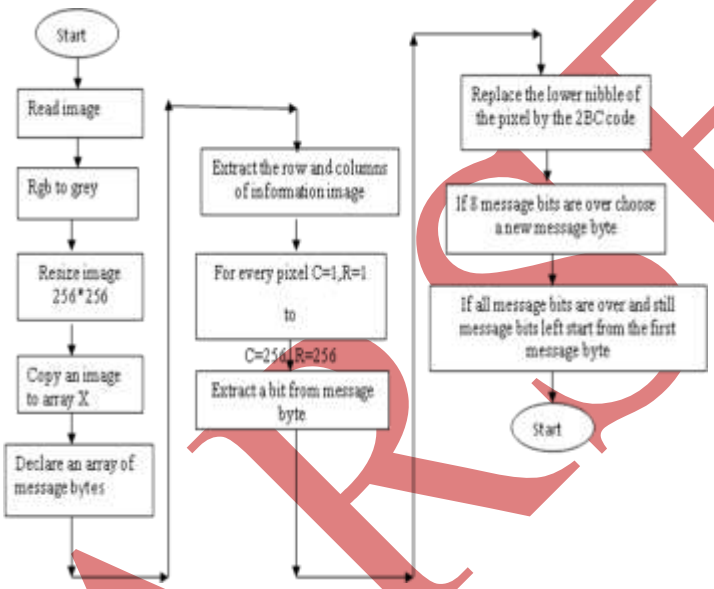


Fig 7: Flowchart for Embedding

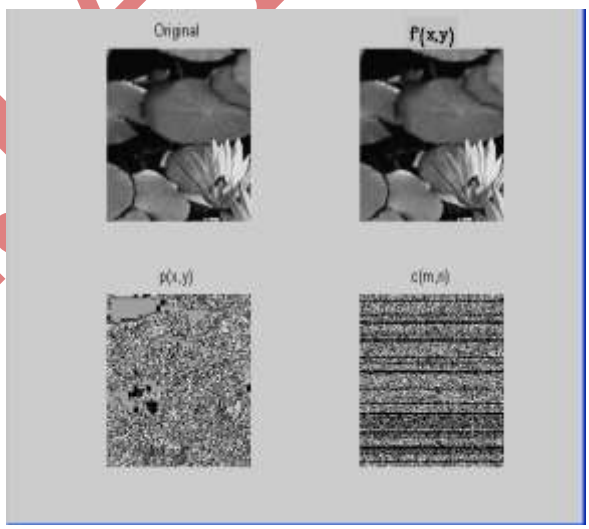


Fig 8: Stegano Image a. original image *f*(*x*,*y*), b. *f*‘ (*x*, *y*) *permutation 1 image* ,*c*. *p*(*x*,*y*) *permutation 2 image* , d. encrypted image *c*(*m*,*n*)

4.3 Conversion of Matrix to Image

In this stage intensity values are converted back to image. The image obtained has message embedded into it. The cover image and the image obtained here has to be identical. Hence the objective of steganography is satisfied.

4.4 Extraction Process

In this process we extract the message which was embedded during embedding process. At first declare a message byte, here the size of the message is 8 bits. Read a pixel from the array starting from address=0.Extract the LSB and replace the ith bit in the message byte where i =1 to 8 Address=address=1. When i =8, a byte is extracted. Repeat for extracting next byte. The flow chart for extraction is shown in the Figure 9.

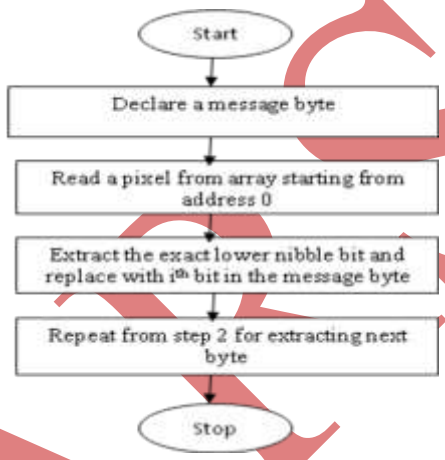


Fig 9: Flowchart for Extraction

The results obtained in MATALB are satisfactory, and then the code is translated in to VERILOG. The development of the algorithm in VERILOG is different in some aspects. The main difference is VERILOG don't support the built in functions of MATALB. The VERILOG code is complied and simulated in XILINX ISE simulator interfaced to Spartan 3 board. The simulation results are presented in the Figure11 and 12 below.

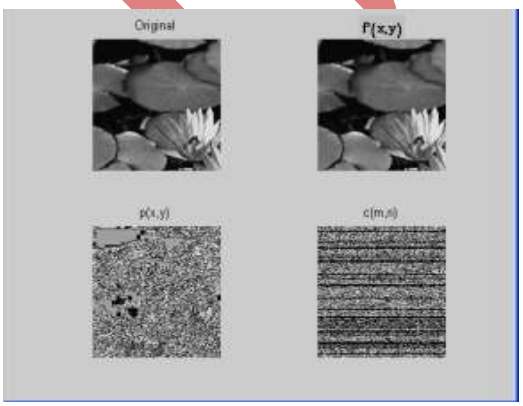
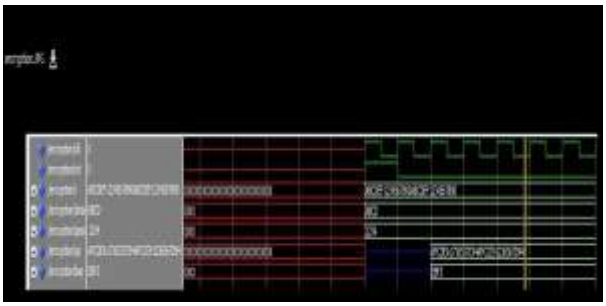


Fig 10

Fig 11

Fig 10: Stegano Image a. original image *f*(*x,y*), b. *f'* (*x, y*) *permutation 1 image* ,*c. p*(*x,y*) *permutation 2 image* , d. encrypted image *c*(*m,n*)

Fig 11: Experimental Setup for Hardware Testing with FPGA board setup



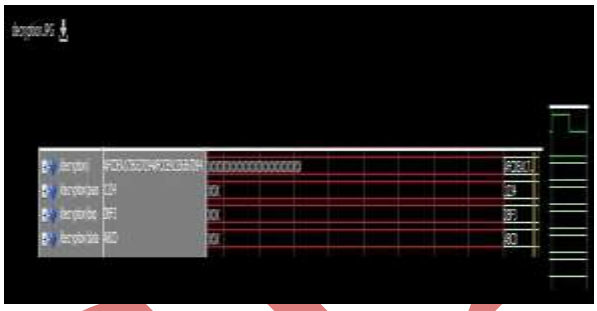
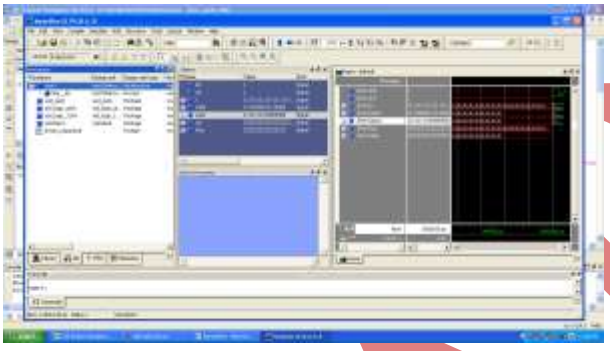


Fig 12: Encryption Timing Diagram

Fig 13: Decryption Timing Diagram



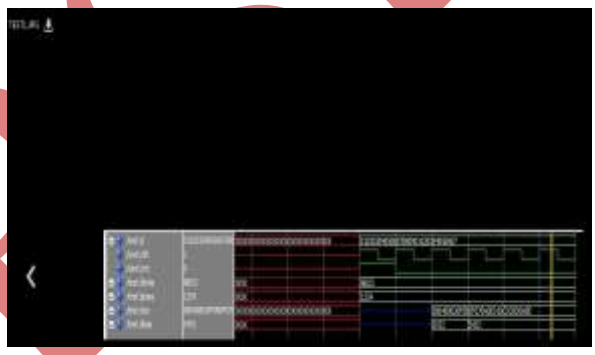


Fig 14: Data When rst=1 Timing Diagram

Fig 15: Data when rst=0 timing diagram

V CONCLUSION

The proposed approach in this project uses a new steganographic approach called image steganography. The main intention of the project is to develop a steganographic application that provides good security. This project proposes a new scheme of separable RIH in EIs to take a hierarchy into account. In addition, this scheme always recovers the original image, whereas the conventional scheme sometimes fails to do. In this work, Passcode Based Approach for Hiding Classified Information in stego images implementation seems to strike the best to get the improvement of embedding capacity of data by 25% as image size is increased.

Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively. It acts as blueprint for FPGA implementation. Adopting FPGA technique, it has fulfilled timing simulation with the advantage of low design cost and high speed. In this work, a new steganography method for hiding classified data based on matching of bit values has been presented. The most important feature of this method is the difficulty to which a third party would encounter in trying to intercept the hidden data. This difficulty arises from the two random algorithms used to select the matching and embedding pixels, the fact that the data bits are not hidden directly, and the use of password and there is an

improvement in the image embedding data capacity. Moreover, implementation is a pure HDL implementation which can be used as an IP in any ASIC product or implementable on any FPGA and any type of images can be used as the cover image such as jpeg, bmp, Png images. In this technique processing image is realtime and there is no need of any external memory and processor support.

REFERENCES

[1] Atallah M. Al-Shatnawi, "A New Method in Image steganography with improved image quality", Applied mathematical science, Vol. 6, no79, 2012.

[2] Zoran Duric, Michael Jacobs, and Sushil Jajodia. "Information Hiding: Steganography and Steganalysis".Review Article Handbook of Statistics, Vol. 24, pp. 171-187,2005.

[3] S. Bhavana and K. L. Sudha .Text Steganography Using LSB Insertion Method Along with Chaos Theory.International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, pp. 145-149, April 2012.

[4] T. Morkel, J. H. P. Eloff, and M. S. Olivier. An Overview of Image Steganography. Proceedings of the 5th Annual Information Security South Africa Conference (ISSA2005) (Eds.: H. S. Venter, J. H. P. Eloff, L. Labuschagne, and M. M. Eloff), Sandton, South Africa, 2005.

[5] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi. Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 3, pp. 168-187, 2012.

[6] E Lin, E Delp."A Review of Data Hiding in Digital Images", CERIAS Tech Report 2001-139, West Lafayette, IN 47907-2086

[7] Fujiyoshi, Masaaki and Hitoshi Kiya. "Reversible Information Hiding and Its Application to Image Authentication." Multimedia Information Hiding Technologies and Methodologies for Controlling Data. IGI Global, 2013. 238-257. Web. 6 Nov. 2013. doi:10.4018/978-1-4666-2217-3.ch011

[8] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE Transactions on Information Forensics and security, vol. 7, Issue 2, 826-832, April 2012.

[9] Barni, M., "What is the future for watermarking?," IEEE Signal Processing Magazine, vol 20, Issue 6, pp. 53-59, Nov. 2003

[10] S. M. Masud Karim M. S. Rahman, and M. I. Hossain." A New Approach for LSB Based Image Steganography using Secret Key". Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp. 286 – 291, 2011.