

# Implementation of Binary Image Steganography in FPGA

A.Hazarathaiah

Professor, Department of ECE, S V College of Engineering, Tirupati, A.P, India

**ABSTRACT:** Steganography is the art of hidden inscription, used prominently to cover text, image, video and audio. The persistence of steganography is to hide the presence of a message from a third party. The intention of this paper is to achieve statistical security without degrading the stego image quality and to improve undetectability. This paper conceals the secret image behind the original image to obtain the stego image. The extraction of inversion pattern, rotation pattern and invariant local binary pattern is preceded to calculate the distortion of cover image. The obtained image is scrambled in order to distribute the pixels uniformly. To reduce the embedding impact of image and to improve the statistical security, Syndrome Trellis Code (STC) is employed which mainly uses the convolutional code with Viterbi algorithm. The steganography application is realized in STC technique by covering the binary image over the original image. The resultant stego image is obtained after proceeding with the STC technique. The proposed technique is simulated in MATLAB and implemented in Spartan 3 FPGA, interfaced with VGA controller to ensure in real time applications.

**KEYWORDS:** Steganography, Distortion, Scrambling, Binary image, STC.

## I. INTRODUCTION

Steganography is the technique used to hide a secret data behind the original data in order to obtain a covert channel that is known only to a sender and receiver. Here the original data is also called as cover media. The media need not be only text but can also be image, audio and video. By hiding a secret data behind the original data it offers a security which cannot be attacked by a steganalyzers [1]. This paper mainly focuses on a binary image which is embedded behind the original image to obtain a stego image. Steganography and Cryptography are two Network security techniques. The main difference between cryptography and steganography is that cryptography scrambles the message so that it becomes difficult to understand whereas steganography hides behind the original message.

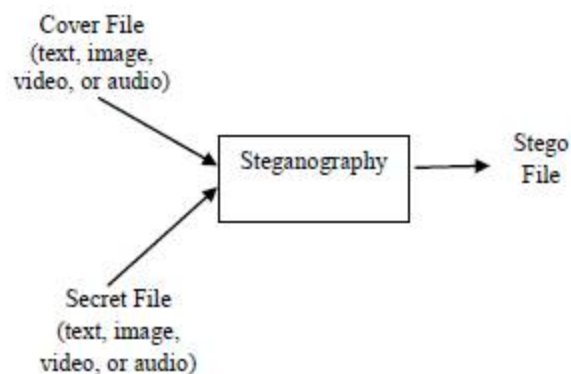


Fig. 1. Basic Block Diagram of Steganography

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

The shifts from cryptography to steganography are that it implies that the message to be transmitted is not visible to the human eye. Secret information is transmitted through unknown cover carriers in such way that the existence of the embedded messages is undetectable. Watermarking and Finger printing are two techniques allied to Steganography. Data hiding requires low distortion, but while implementing steganography technique the obtained stego image will be distorted and it's easily detected by human eye. Therefore, distortion measurement is important in steganography which can contribute towards perceptual quality. There are two ways to measure visual distortion, one is subjective measurement and the other is objective measurement [2]. Subjective measurement is very costly and its distortion measure differs for different observers. And objective measurement gives the exact distortion measure between the original and the distorted image. So, objective distortion measurement is mostly preferred. Image scrambling is a useful approach to secure the image data by scrambling the image into a chaotic format. The scrambling algorithms not only have the effect of encrypting the secret images but also increase the undetectability of secret image. In this work, distortion is calculated for cover image and based on that distortion measure, secret message is hidden behind it. Scrambling is used to make the pixels get distributed uniformly. STC is used to minimize the additive distortion and to implement the steganographic technique. The main objective of the paper is to improve Undetectability and to achieve statistical security without degrading the obtained stego image quality.

## II. PROPOSED METHOD

The proposed binary image steganography was first realized using MATLAB and it was subsequently simulated in Verilog as shown in Fig. 2.

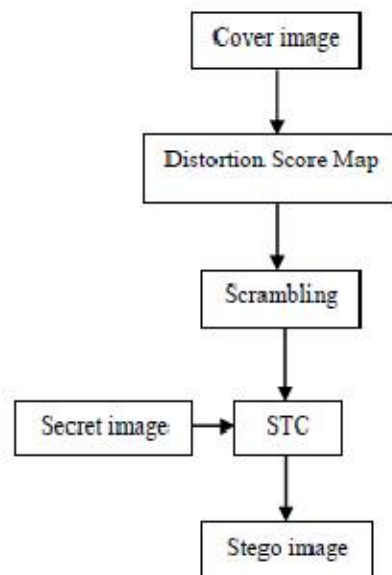


Fig. 2. Proposed Block Diagram

In this paper spatial domain-based (substitution method) binary image steganographic scheme is proposed. This method uses the pixel intensity directly to encode the message bits, therefore it results in problem of additive distortion that creeps in the binary image and affects the PSNR and the statistical properties of image.

### A. FLIPPING DISTORTION MEASUREMENT

Initially flipping distortion is measured to embed the secret image behind the cover image. Binary image processing involves complement, rotation and mirroring. In order to develop a better steganographic application in binary image, inversion pattern, rotation pattern and invariant local binary pattern or Local Texture Pattern (LTP) is extracted.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

To find the local binary pattern [3], a cover image is divided into cells. And for each pixel in a cell, the pixel is compared to each of its 8 neighbors. The pixels are arranged in a circle either in clockwise or anti-clockwise direction as shown in Fig. 3 and form a 8 digit binary number. Let the pattern  $T_{i,j}$  denote a local neighborhood of an binary image

which is centered at the location  $(i, j)$  of  $3 \times 3$  size grid is,

$$T_{i,j} = \{IC, I_0, I_1 \dots I_7\} \quad (1)$$

Where IC denotes the center pixel and  $I_K$  where  $K = 0, 1, \dots, 7$  denotes the 8 neighboring pixels.

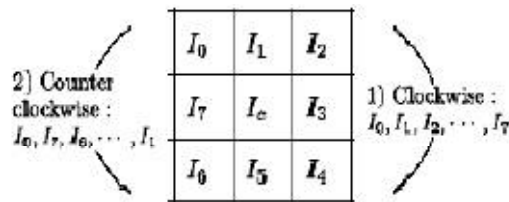


Fig. 3. Neighborhood of  $T_{i,j}$

Only 90 degree rotation invariance and all multiples of 90 degree rotated versions are considered because it has unique value. When the rotation is considered in clockwise direction the neighboring pixels are 2-bits-wise rotated in the clockwise direction by 4 times. The value corresponding to each time rotation is calculated and the minimal one is selected [4]. Mathematically, the LTP in clockwise direction is calculated as

$$LTP_{i,j}^c = \min_{b=0,1,2,3} \sum_{k=0}^7 (I_c \oplus I_{(k+2b) \bmod 8}) \times 2^k \quad (2)$$

Similarly, when the rotation is in counter clockwise direction the neighboring pixels are considered 4 times. Mathematically, the LTP in counter clockwise direction is calculated as

$$LTP_{i,j}^{cc} = \min_{b=0,1,2,3} \sum_{k=0}^7 (I_c \oplus I_{(-k-2b) \bmod 8}) \times 2^k \quad (3)$$

The final value of mirror invariant local texture pattern (crmiLTP) can be computed as

$$LTP_{i,j}^{crmi} = \min\{LTP_{i,j}^c, LTP_{i,j}^{cc}\} \quad (4)$$

The purpose of obtaining crmiLTPs is to remove the confusions on measuring both visual quality and statistical property of binary image. The proposed flipping distortion function is formed as the detectable embedding changes in the crmiLTP distribution [4]. It can be observed that the change in the number of crmiLTPs when flipping one pixel can loosely indicate the flippability of that pixel. Therefore, the change in the number of crmiLTPs can be calculated as

$$\Delta_{i,j} = \sum_{t=0}^{255} |H_t^X - H_t^{Y_{i,j}}| \quad (5)$$

Where  $H_t^X$  and  $H_t^{Y_{i,j}}$  are the histogram coefficients

which can be computed from the given equation as

$$H_t = \sum_{i=1}^{l_w-2} \sum_{j=1}^{l_h-2} \delta(LTP_{i,j}^{crmi} = t) \quad (6)$$

Where  $l_w \times l_h$  is the size of the test image.

Finally, the flipping distortion assigned with the weighted sum of crmiLTP changes can be computed as

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

$$D_{i,j} = \left( \sum_{t=0}^{255} W_t |H_t^X - H_t^{Y_{i,j}}| \right)^m + \beta \quad (7)$$

Where  $W_t$  denotes the weight corresponding to the crmi LTP whose value is  $t$ , and tuned to control the sensitivity of distortion score map and their values are experimentally set as  $= 1/2$  and  $= 1/2$ . While calculating the distortion score map, only the weights of 20 best crmiLTP is assigned to nonzero, because of the binary image and rest of the weights are set to zero. A steganographic scheme should only change the pixels with the lowest distortion scores [1].

## B. SCRAMBLING

The objective of image scrambling is to generate a meaningless image which prevents human visual system or computer vision system from understanding the original content.

### i. Key Based Scrambling

In image scrambling, it is significant to have simple algorithm to shuffle the pixel values fast and reorder it to reveal the original. Key based scrambling proposes a solution which provides both simplicity and maximum security using a user defined sequence to preserve the information. In key based approach a pseudorandom sequence is built which uses long positive integer value sequence. Since these values are used for image pixel row and column shuffling. In order to produce the longer sequence the user provided sequence is occasionally inserted. To shuffle the image well, each value of the shorter sequence is incremented whenever it is repeated in the longer sequence.

After shuffling the produced order sequence which is the key in this process, all rows are switched according to the key sequence, columns are switched using the same sequence. Then the process is followed by circular shifting and the result obtained after this process is visually acceptable. Using this scrambling technique makes flippable pixels get distributed more uniformly in the cover image. One issue is that the large uniform region contained in an image significantly decreases the density of flippable pixels.

### ii. Scrambling Using LFSR

A scrambler is a device that manipulates a data stream before transmitting the input data which is implemented using Linear Feedback Shift Register (LFSR) as shown in Fig. 4. The manipulations are reversed by a descrambler at the receiving side. Due to long sequences of consecutive digits from incoming data streams, the clock signals become low and lead to delay in clock signal, and decreases the data transfer rate in the system. Hence complexity increases in the system and leads to over consumption of logic resources. Hence there is a need for clock recovery at the receiver, which in turn requires a sure minimum number of transitions in the incoming serial data stream. And this uses Pseudo Random Bit Sequence (PRBS) circuit to perform scrambling.

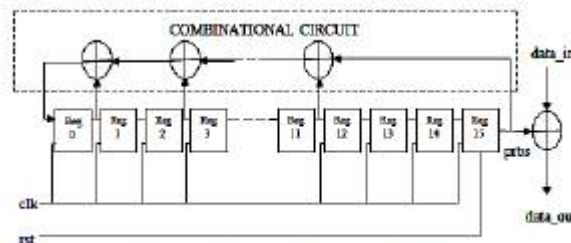


Fig. 4. Scrambler using LFSR

## C. SYNDROME TRELIS CODE

The STC is employed to minimize the designed embedding distortion and to implement the steganographic scheme. Minimizing the embedding impact on cover media and improving the embedding efficiency is an important for enhancing the security of steganographic methods which is achieved by STC. The STC uses the convolutional code with a Viterbi algorithm-based encoder [5] to minimize the additive distortion function.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

## III. RESULTS AND DISCUSSIONS

Initially the binary image steganography system is simulated in MATLAB 2014 simulation tool. The input cover image and secret image are shown in Fig. 5.

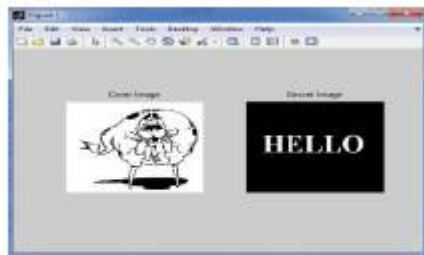


Fig. 5. Cover and Secret Image

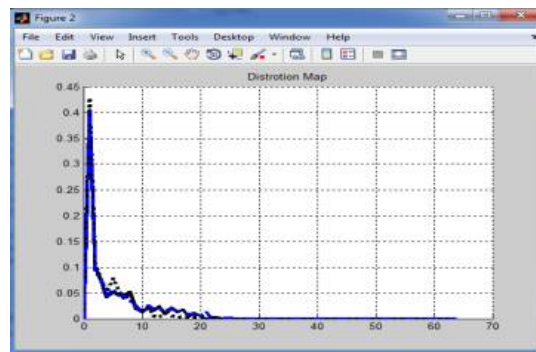


Fig. 6. Distortion Score Map

Fig. 6. shows the flipping distortion measurement of cover image with respect to secret image.

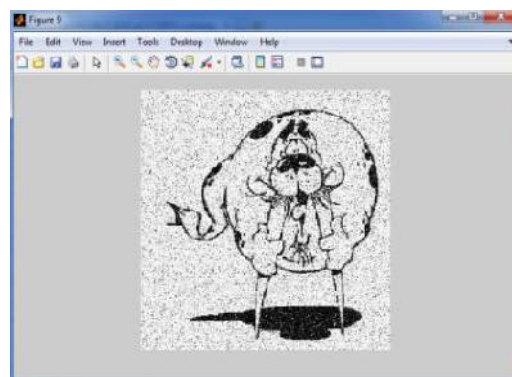


Fig. 7. Distorted Stego Image

Fig. 7. shows the distorted stego image and the distortion is due to the pixel difference in both cover image and secret image which is easily attacked by steganalyzers due to pixel variance.

# International Journal of Innovative Research in Computer and Communication Engineering


(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015



Fig. 8. Distortion-less Stego Image

Fig. 8. shows the restored image (i.e.) stego image without distortion, in order to achieve the statistical security without degrading the obtained stego image and to minimize the embedding distortion.



	1	2	3
1	45.5255		
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

Fig. 9. PSNR value

Fig. 9. shows the PSNR value, if it is high then the quality of image is good otherwise it will be bad. PSNR can be calculated using Mean Square Error (MSE) as shown in equation (8).

$$PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right) \quad (8)$$



Fig. 10. Image Displayed in VGA monitor

Fig. 10. shows the design of VGA Controller using Verilog HDL and implement it on FPGA. First and foremost, RGB data or binary data are abstracted from an image file in image format (i.e., jpeg, bmp) using MATLAB and converted to oe file (i.e. Xilinx supported format). Then arranged data are then stored n a Coe file created in MATLAB is stored in



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

the internal Memory of FPGA. After that, a VGA Controller program [6] is written in Verilog HDL using ISE Design Suite, which will compile, run and simulate the written program. Once the simulation is succeeded, the program will be burnt into Spartan-3 Board, which will process the VGA Controller program and display the image on CRT monitor screen [7].

## IV. CONCLUSION

A secure binary image steganographic system has been implemented. A secret image of size  $100 \times 100$  has been hidden into a cover image of size  $256 \times 256$ . The flipping distortion for cover image is measured and then scrambling is applied to distribute the pixels uniformly. Then STC is applied to implement the steganographic application. The proposed technique is simulated in MATLAB and implemented in Spartan 3 FPGA interfaced with VGA controller. It can be seen that the proposed method performs well on both image quality and security. Therefore, in future the work that has already been implemented in MATLAB and simulated in Xilinx can be extended to realize a real time implementation in FPGA. On comparing both the MATLAB and verilog obligation the coding formulation in MATLAB will be apparent as compared to the verilog. But while considering in terms of implementation in real time environment verilog will be in manifest.

## REFERENCES

- [1] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," Proc. SPIE, Vol. 4314, pp. 369–375, Aug. 2001.
- [2] J. Cheng and A. C. Kot, "Objective distortion measure for binary text image based on edge line segment similarity," IEEE Trans. Image Process., Vol. 16, No. 6, pp. 1691–1695, Jun. 2007.
- [3] D. Huang, C. Shan, M. Ardabilian, Y. Wang, and L. Chen, "Local binary patterns and its application to facial image analysis: A survey," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., Vol. 41, No. 6, pp. 765–781, Nov. 2011.
- [4] Bingwen Feng, Wei Lu, and Wei Sun, "Secure binary image steganography based on minimizing the distortion on the texture," IEEE Trans. Inf. Forensics Security, Vol. 10, No. 2, pp. 243–255, Feb. 2015.
- [5] T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Trans. Inf. Forensics Security, Vol. 6, No. 3, pp. 920–935, Sep. 2011.