FPGA Implementation of Data Hiding In Images
Mr.R.V.Rathod*1, Prof.L.K.Chouthmol*2,
*1 (E & Tc Department, Savitribai Phule Pune University, India)
*2 (E & Tc Department, Savitribai Phule Pune University, India)
rathod.raja7@gmail.com*1, lata_51105@rediffmail.com

Abstract: It is the process of embedding data within the domain of another data, this data can be text, image, audio, or video contents. The embedded watermark can be visible or invisible (hidden in such a way that it cannot be retrieved without knowing the extraction algorithm) to the human eye, specified secret keys are taken into consideration in order to enhance the security of the hidden data. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed. The results showed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks. However, the limitation of capacity has led us to think about an improved approach which can be achieved through hardware implementation systems with the help of a programmable gate array (FPGA) board. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

Keywords–Cryptography, Encryption, LSB (Least significant bits), Steganography.

I. INTRODUCTION

Cryptography is the practice of 'scrambling' messages so that even if detected, they are very difficult to decipher. The purpose of Steganography is to conceal the message such that the very existence of the hidden is 'camouflaged'. However, the two techniques are not mutually exclusive. Steganography and Cryptography are in fact complementary techniques. No matter how strong algorithm, if an encrypted message is discovered, it will be subject to cryptanalysis. Likewise, no matter how well concealed a message is, it is always possible that it will be discovered. By combining Steganography with Cryptography we can conceal the existence of an encrypted message. In doing this, we make it far less likely that an encrypted message will be found. Also, if a message concealed through Steganography is discovered, the discoverer is still faced with the formidable task of deciphering it. The historical examples given earlier show that the use of Steganography is not limited to a new medium. It should therefore come as no surprise that techniques have been developed to work with digital media. It is now possible to hide any sort of digital media inside any other type of digital media. For example, it is possible to hide a text message, encrypted or plain text, inside of a digital picture or sound file. It is also possible to conceal one type of digital media inside of the same type of digital media. For example an image of a famous painting could be used to conceal a photograph of schematics of some type. Steganography has been in the news recently as it was members of the al-Qaeda terrorists were communicating by embedding Arabic messages inside digital files, such as JPEGs and MP3s, and distributed over the internet. Steganography is the art of concealing the presence of information within an innocuous container.

II. PROPOSED SCHEME

![Fig.1 Encryption process](Image)

Fig.1 shows encryption process of plain text in test image using LSB stenography which will give encrypted stego image as output data is embedded within that image for secret communication and will be retrieved at receiver side.
Fig. 2: Decryption system

Fig. 2 shows block diagram of decryption system using LSB decryption which will give original image and plain text after decryption. So this provides secure commutation of data by embedding into image compare to sending data only which may hack then we are going to implement this algorithm in FPGA Spartan kit for VLSI implementation.

2.1 Existing Method

Watermarking techniques may be applied without fear of image destruction due to lossy compression because they are more integrated into the image. Most of the work in this category has been concentrated on making use of redundancies in the DCT (discrete cosine transform) domain, which is used in JPEG compression. But there have been other algorithms which make use of other transform domains such as the frequency domain. The major problem with many of these watermarking schemas is that they are not very robust against different types of image manipulations or attacks. Moreover, some of these techniques are quite complicated to implement in real-time.

2.2 Steganography

Steganography is the art of embedding information in such a way that prevents the detection of hidden messages. It means hiding secret messages in graphics, pictures, movie, or sound. Steganography comes from the Greek word steganos, which means ‘covered’, and graphy, which means ‘writing’. Covered writing has been manifested way back during the ancient Greek times around 440 B.C. Some of old stenography examples are shaving the heads of slaves and tattoo messages on them. Once the hair had grown back, the message was effectively hidden until the receiver shaved the heads once again. Another technique was to conceal messages within a wax tablet, by removing the wax and placing the message on the wood underneath. The most popular and frequently method of Steganography is the Least Significant Bit embedding (LSB). The level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. If we are using the least significant bits of the pixels’ color data to store the hidden message, the image itself is seemed unaltered, and changing the LSB’s value will have no effect on the pixel’s appearance to human eye. This art of covert communication is very ancient. Till date, multitudes of methods and variations have been developed, for hiding information. Hiding the secret message under a wax coating of a wax coated tablets is one of the oldest methods. The message can be camouflaged in text message.

2.3 Least Significant Bit (LSB) Algorithm

First we will investigate least significant bit insertion, where you literally put the information in the least significant bits of an image. This is a simple technique but the down side is that the message is very susceptible to information loss when using lossy compression techniques. We will now go over an example that involves inserting an A into 3 pixels of a 24 bit image. Here is the original raster data:

```
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
```

The binary value of A is 10000011 and encoding A into the last bits of this 3 pixel sequence will change the above sequence to:
(00100111 11101000 11001000) (00100110 11001000 11101001). Notice that only the underlined bits had to be changed in order to create the A. On the average only half of the bits would have to be changed in an LSB (Least Significant Bit) encoding scheme. With such a small variation in the colors it would be very difficult for the human eye to discern the difference. Next we will do least bit insertion with an 8 bit value. Since 8 bit values can only have a maximum of 256 colors the image must be chosen much more carefully. Consider a palette with four colors: white, red, blue, and green which have the palette position entries of 0(00), 1(01), 2(10) and 3(11) respectively. The values of four adjacent pixels with colored white, white, blue, blue (00 00 10 10). We will try and hide the decimal number 10 represented in binary as 1010. The resulting raster is: 01 00 11 10, which corresponds to red, white, and green, blue. These large changes in the image are very noticeable in a color image although an 8 bit grey scale image will produce relatively good results. There are multiple tools that implement LSB. One tool, Stego can change around the palate to lessen the frequency of adjacent colors with too strong of a contrast. Stools tries to approximate the cover image by changing around the palette to make the difference between bits only one and sometimes causes very noticeable shifts in the palette.

2.3 Parameter of Steganography

Capacity of Cover Object: The maximum length of message that can be embedded into a cover without affecting perceptual quality or signal strength is referred as capacity of the particular object. Level of embedding: The actual amount of embedding as percent of capacity of cover object is level of embedding. So it can be anywhere between 0% to 100%. The State of Art of Digital Image Steganography is a digital Images. To store an image on computer, it is divided into small parts called pixels. The value of intensity of these pixels is stored for three basic colors as an image on computer. ‘.bmp’, ‘.pnw’ is some file formats to store such images, which are uncompressed file formats for images. These images have a lot of redundancy. Also the loss of small information in pixel intensity is not captured by the human eye. So there exist compression techniques like jpeg for images. The compression techniques will try to decorrelate the redundancy and may also introduce some loss of information.

III. APPLICATIONS

1. Modern Printers: Steganography is used by leading manufacturers in digital & laser printers, including HP and Xerox. Here, tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2. Digital Watermarking: Steganography is used for digital watermarking, where a message is hidden in an image so that its source can be tracked or verified.

3. E-mail Spam: e-mail messages is encrypted steganographically. Coupled with the "chaffing and winnowing" technique, a sender gets messages out and cover their tracks all at once.

IV. RESULTS

As shown in fig.3, which shows the how header file is created and Fig.4 which is the header file in which data is going to embed is first of all processed like color image is converted into gray scale image and then gray scale image is resized so that every image will become of equal size after that image is denoised to get proper result. Then secrete data is stored in same folder of matlab current directory to embed in image. Data may be logo, plain text or any which we are going to embed using
with Xilinx 10.1 version is configured. LSB stenography until now FPGA processor Spartan 3 XCS300

Fig.3: Header file created

Fig.4: Header file

IV. CONCLUSIONS

In this paper, we presented a new approach for data transmission in image by using coding with simple LSB coding protecting method. We initially motivated our study of raw video by examining the intended applications. Here we propose a data hiding and extraction procedure for high resolution images. Although embedding data in image using VLSI implementation takes more size but it can be transmitted from source to target over network after processing the source image using these Data Hiding and Extraction procedure securely. There are two different procedures, which are used here at the sender’s end and receiver’s end respectively. The procedures are used here as the key of Data Hiding and Extraction. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed.

REFERENCES


