International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

Least Significant Bit algorithm for image steganography

Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Institute of Technology,Bangalore, India

Abstract

Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopted. Embedding secret information inside images requires intensive computations, and therefore, designing Steganography in hardware speeds up Steganography. This is implemented using ARM7TDMI processor and GSM 900.

There are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. In this work, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.

Keywords— Steganography, embedded, Cover image, Data hiding, LSB method, MSB, ARM7 TDMI, GSM 900.

Introduction

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is to use steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

The goal of Steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become popular in a number of application areas. Digital audio, video, and images are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Nowadays images are the most popular cover object used for steganography where an altered image with slight variations in its colors will be indistinguishable from the original image by a human being, and thus the importance of Image Steganography. In this work images are used as a cover object to hide the secret information.

Some of the techniques used in steganography are domain tools or simple system such as least significant bit (LSB) insertion and noise manipulation, and transform domain that involve manipulation algorithms and image transformation such as discrete cosine transformation and wavelet transformation. However there are techniques that share the characteristic of both of the image and domain tools such as patchwork, pattern block encoding, spread spectrum methods and masking. This work is carried out using ARM7TDMI processor and GSM 900to achieve secured data encryption and decryption.

Overview of Steganography

Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means “covered writing”. A Steganography system consists of three elements: cover-image (which hides the secret message),the secret message and the stegano-image(which is the cover object with message embedded inside it).

A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

ISSN:2319-7900

The LSB is the lowest significant bit in the byte value of the image pixel.

The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).

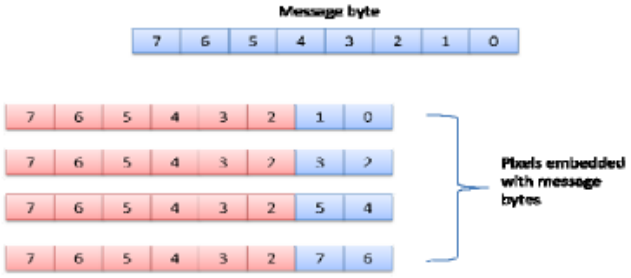

Figure 1: Proposed LSB Algorithm

The concept of LSB Embedding is simple. It exploits the fact that 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. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

Design and Implementation

For security, only encryption may not be enough, hence proposed project includes Steganography wherein encrypted data is hid into the image and then image is transmitted in the network.

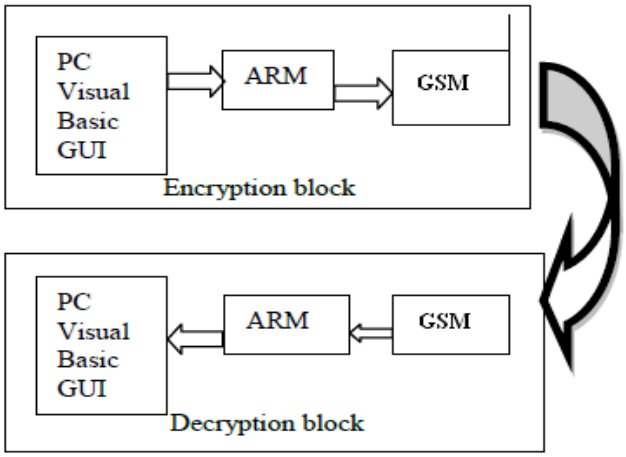

Figure 2: Experimental block diagram

The block diagram as shown in figure 2 mainly contains the following blocks.

1) Personal computer (PC)
2) ARM7TDMI
3) GSM 900

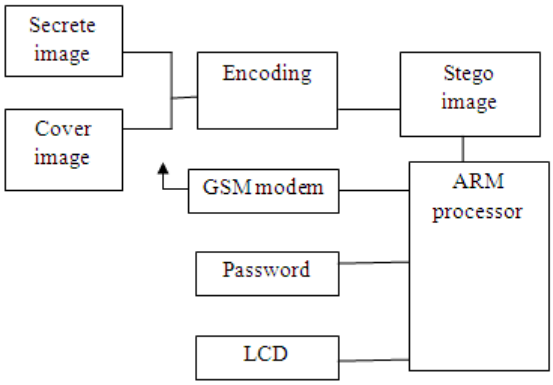

Figure 3: Block diagram of Encryption

Encryption process: Read the secret and cover image and convert them into gray scale images, then check the size of the secret image with that of the cover image such that size of the secret image should be less than cover image. Encode the secret image into binary using bit gate command and divide it into RGB parts then substitute MSB bits of secret image into LSB bits of cover image. Hide the password with Stego image and send using GSM modem.

Decryption process: The reverse process takes place at the receiving end, Stego image can be decrypted using password.

Simulation and Results

1. MATLAB Simulation

MATLAB is a high-performance language for technical computing. 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. In this work, Matlab is implemented for processing LSB steganography technique with different frame size 256*256, 128*128, 64*64 and simulation results are shown.

There are mainly four steps involved in implementing LSB steganography as shown below.

a. 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

ISSN:2319-7900

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 4 shows the cover image used.

In the figure 5, the intensity values of cover image obtained during the conversion of image to matrix is represented.

Figure 4: Cover Image

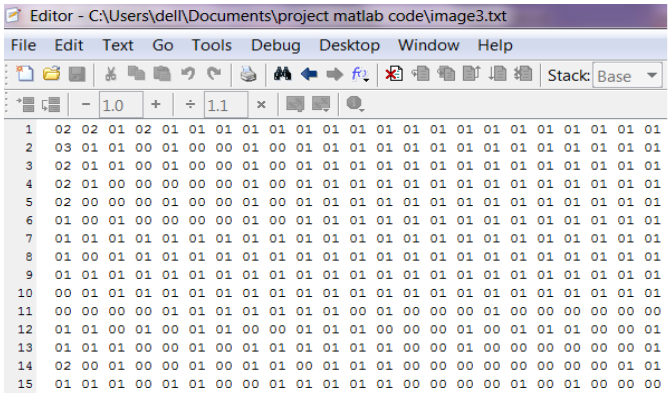

Figure 5: Intensity values of Cover image

b. Embedding process

After completion of image to matrix the next step is to embed a message into an image. 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 intensity values of the embedded image are as shown in the figure 7 and stegano image in figure 8.

Figure 6: Secret Image

c. 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 have to be identical. Hence the objective of Steganography is satisfied.

d. 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 i th 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.

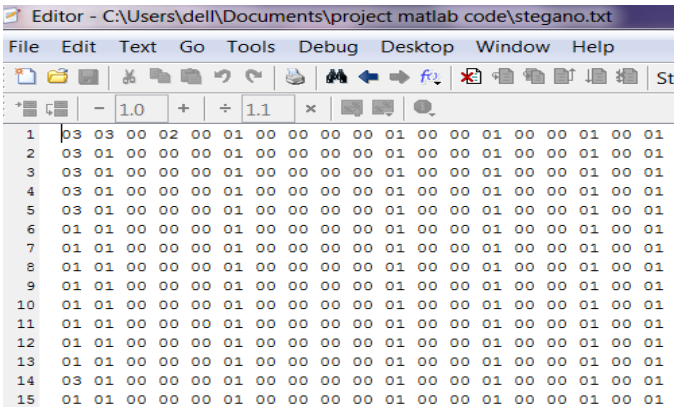

Figure 7: Intensity values of Stegano-image

Figure 8: Stegano Image

ISSN:2319-7900

2. Hardware simulation

Figure 9: Receiving status of data from PC to ARM

As in figure 10, this Kit includes ARM7TDMI Controller. LCD having 16*2 character interfaced to controller. UART0 and UART1 used for serial communication. Here we use UART0 for PC Communication and UART1 for GSM interfacing. We send secret image + cover Image=stego image from PC to Controller. When Controller receives all data sent by PC, it starts sending to receiver through GSM Modem similarly decoding process take place at receiver side. Stego image received by GSM, then it send to controller, then controller decode original image (secret image) from cover image and transmit to PC.

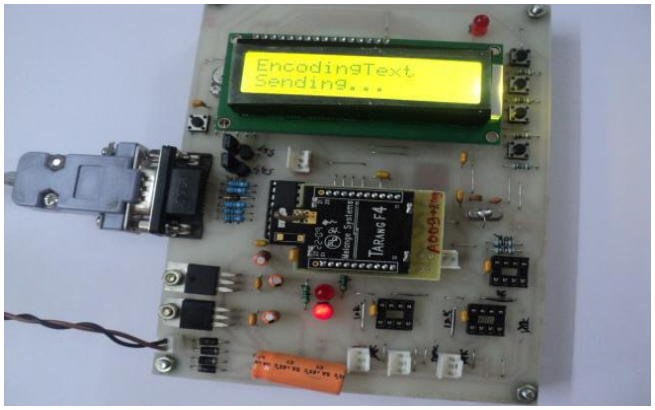

Figure 10: Encoded data is sent through GSM

Conclusion

The enhanced LSB technique described in this project helps to successfully hide the secret data into the cover object without any distortion. 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. Since LSB doesn't contain any information there is no loss of information and secret image recovering back become undistorted.

References:

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012.

[2] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Computer Engineering Department Hashemite University, Zarqa, Jordan Sahel Alouneh,Computer Engineering Department, German-Jordan University, Amman, Jordan, "FPGA Hardware of the LSB Steganography Method" IEEE 2012.

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

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M, "Image Steganography Techniques: An Overview", International Journal of computer science and security, vol (6), Issue (3), 2012.

[5] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, " A Survey on Image Steganography and Steganalysis",Journal of Information Hiding and Multimedia Signal Processing c ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011.

[6] Vijay kumar sharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimize technique", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.

[7] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon,, Image Steganography and: Concepts and Practice", Department of Electrical and Computer Engineering Department of Computer and Information Science Polytechnic University,Brooklyn, NY 11201, USA.

[8] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu "A Comparative Analysis of Image Steganography",International Journal of computer Applications,Vol2-No3, May 2010.

[9] Saeed Mahmoudpour, Sattar Mirzakuchaki,"Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers", International Journal of Computer Applications (0975 – 8887) Volume 37– No.7, January 2012.

ISSN:2319-7900

Biographies

Champakamala .B.S, received the B.E. degree in Electronics and Communication Engineering from Visvesvaraya Technological University, Belgaum in 2005 & M.Tech degree in VLSI & Embedded System design from Visvesvaraya Technological University, Belgaum in 2012.Currently, she is an Assistant Professor of Telecommunication Engineering in Don Bosco Institute of Technology Bangalore.

Padmini.K, received the B.E. degree in Telecommunication Engineering from Visvesvaraya Technological University, Belgaum in 2004 & M.Tech degree in VLSI & Embedded System design from Visvesvaraya Technological University, Belgaum in 2013.Currently, she is an Assistant Professor of Telecommunication Engineering in Don Bosco Institute of Technology Bangalore.

Radhika .D.K, received the B.E. degree in Telecommunication Engineering from Visvesvaraya Technological University, Belgaum in 2004 & M.Tech degree in Digital Communication Engineering from Visvesvaraya Technological University, Belgaum in 2010.Currently, she is an Assistant Professor of Telecommunication Engineering in Don Bosco Institute of Technology Bangalore.