Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Image Hiding using Least Significant Bit Algorithm Steganography

Padmini K[1] and Champakamala B S[2]
[1]Don Bosco Institute of Technology/TCE, Bangalore, India
padmini.roopesh @gmail.com
[2]Don Bosco Institute of Technology/TCE, Bangalore, India
bschampa @gmail.com

***Abstract*—Steganography is one of the techniques to conceal the existence of hidden secret data inside a cover object. Images are used as 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.**

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

I. INTRODUCTION

Steganography is a technique used for hiding information and goal of Steganography is to avoid drawing suspicion to the existence of a hidden message. The approach of hiding technique used in many application such Digital audio, video, and images are used to hide important serial number and copyright help to prevent hackers which they can access important information it can be avoided by using images are the 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.

Grenze ID: 02.ICCTEST.2017.1.111

II. Overview of Steganography

Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography is important for information security. It is the art of invisible communication by concealing information inside other information. steganography means “covered writing”. It consists of three elements: cover-image (which hides the secret message),The secret message andThe 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. 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).

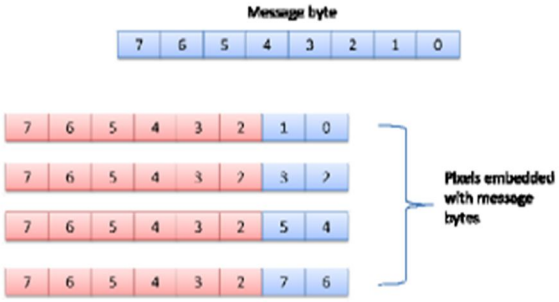

Fig 1: Proposed LSB Algorithm

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.

III. Design and Implementation

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

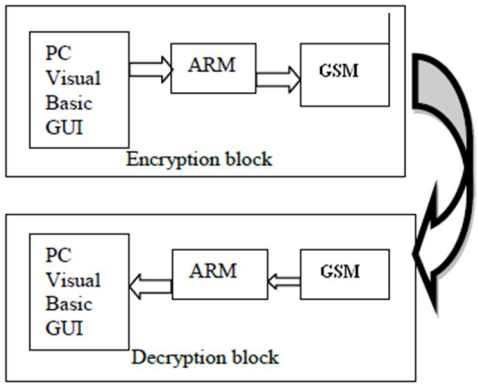

Fig 2: Experimental block diagram

The block diagram as shown in figure 2 mainly contains the following blocks.
1) Personal computer (PC)
2) ARM7TDMI
3) GSM 900

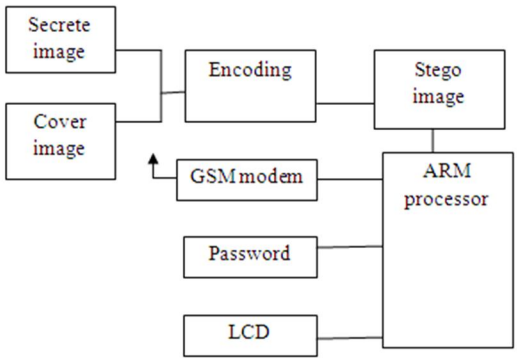

Fig 3: Block diagram of Encryption

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.

IV. Conclusion

The enhanced LSB technique described in this work 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] Neil F. Johnson and Sushil Jajodia, "Steganalysis of Image Created Using Current Steganography Software", Workshop of Information Hiding Proceedings, Portland Oregon, USA,15-17 April,1998. Lecture Notes in Computer Science, Vol.1525, Springer-Verlag (1998).
[2] Clair,Bryan,"Steganography: How to Send a Secret Message", 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganogr aphy.shtml.
[3] Bender, W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.
[4] Moller. S.A., Pitzmann, and I. Stirand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 7-21.
[5] Gruhl, D., A. Lu, and W. Bender, "Echo Hiding in Information Hiding", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996.