Hiding Host Image using a Cover Image

Allen Tom[1], Anu V Thomas[1], Jerin Jose[1], Maria Jose[1], P. Darsana[2]
[1]UG Scholar, [2]Assistant Professor
Dept. of Electronics and Communication
Amal Jyothi College of Engineering, Kanjirappally, India

***Abstract*—This paper presents secure transmission of image by using "Steganography" technique. The host image to be hidden is firstly converted to grey scale image in order to reduce the size. Then we perform bit plane slicing of host image and place these bits at the LSB of the cover image. Thus host image is hidden in the cover image. This encoded cover image (stego image) is send to the receiver. The receiver can now decode the cover image by using secret key. Decoding is the entire reverse process of encoding. Thus we can retrieve the original host image. The proposed scheme is able to achieve security of image.**

Keywords—Decoding, Secret key, Steganography, Stego image.

I. INTRODUCTION

With the rapid development in information and communication technology the protection of digital multimedia like image, audio and video is very necessary. Transmitting data through public channels such as internet has increased. Therefore information security is playing a significant role in communication. Reliable, fast and robust security techniques are needed to store and transmit information.

To ensure this security we use Steganography technique. It is the art and science of writing hidden messages such that none but sender and recipient realize that there is a hidden message. The term Steganography is arrived from the Greek word means, 'covered writing' [1]. That is concealing information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. We make data invisible to an unauthorized user. In this way they are unable to notice the existence of secret image.

The image to be hidden is the 'host image'. The image in which host image will be embedded in is the 'cover image'. After embedding process the image is called 'stego-image'. One of the most commonly used steganography technique is LSB Steganography. Here we embed secret data by replacing K LSB bits of cover image with K secret bits directly [2][3].

Steganography can be used for wide range of applications such as, in defense organizations for safe circulation of secret data, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. In medical imaging, patient's details are embedded in image providing protection of information and reducing transmission time and cost [4], in online voting system so as to make the online election secure and robust against a variety of fundamental behaviors [5], for data hiding in countries where cryptography is prohibited, in improving mobile banking security [6], in tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications.

II. LITERATURE SURVEY

A. Features of Steganography:

Steganographic techniques have various features which characterizes their strengths and weakness. Features include:

- *Embedding Capacity:* It refers to the amount of data that can be inserted into the cover-media without deteriorating its integrity.
- *Perceptual Transparency:* It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.
- *Robustness:* It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.
- *Tamper resistance:* It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.
- *Computational complexity:* This is employed for encoding and decoding [7].

B. LSB Steganography

Least Significant Bit (LSB) Substitution [8] is the technique in which LSB's of the cover images are replaced by the bits of the secret images. We can randomize the pixel selection also. There are two types of LSB steganography: LSB replacement (LSBR) and LSB matching (LSBM). In LSBR, least significant bits of cover pixels are simply replaced by the secret message bits. In LSBM, the pixel with LSB not matching with the corresponding message bit will be randomly added or subtracted by one. So LSBM is commonly called ±1 embedding. In both methods, it is easy for the recipient to retrieve the hidden message bits by reading LSB's [9].

III. PROPOSED TECHNIQUE

This paper proposes a framework to support image steganography with a user defined password security to include as much as necessary components so as to facilitate a secure and accurate transmission of secret data. The block diagram of the proposed method is shown in Fig. 1.

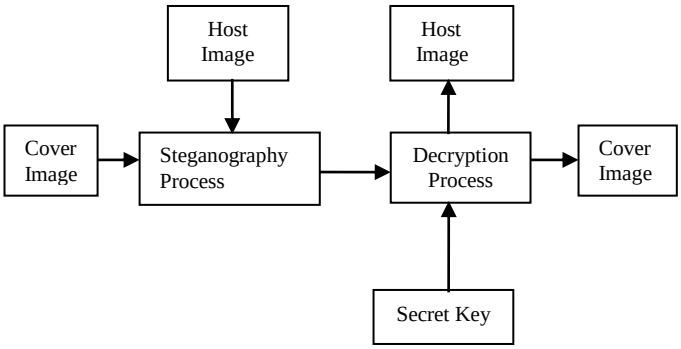


Fig. 1. Block diagram of the proposed technique

Our framework includes several modules. In the first module we will standardize the host image. Secondly we will embed the host image in the cover image by Steganography technique. In the later modules we will be using a stego key for security. The receiver will decode the secret image using this stego-key. Thus the original secret image is retrieved back. The detailed description of the proposed method is given below.

A. Standardizing the Images

At first, we are inputting or reading the required images, one is the secret image which is to be held confidentially and the other is the cover image. The size of these images should be strictly followed. Here the cover image is of size 480×360 pixels. This huge difference in the size remembers the key rule of this method, i.e., the total number of bits of the secret image should be very much less than that of the cover image so that the image should look the same as before after the embedding process. Apart from it, here there is an RGB to grey scale conversion of the secret image for the future expansion.

B. Embedding Process

Here the embedding procedure starts with Bit Plane Slicing of the secret image. At first, we split up the secret image pixels bytes into individual bits. Similarly all the secret image pixels are now converted to individual bits and composed of corresponding bit planes. Thus we have 8 bit planes with corresponding bits of each and every secret image pixels.

The proposed embedding technique is LSB Substitution Steganography. As the name suggests, the LSB of each pixel bytes of cover image is replaced with each bits of secret image. Embedding is done by the following steps:

Step 1: The bit plane slicing can be implemented by AND-ing the pixel byte with required bit position.

Step 2: We process the cover image. AND-ing the cover image pixels with '1' gives corresponding LSB's which we want to replace with the secret data.

Step 3: If we want to incorporate a secret data to the existing one, it should be made vacant. Similarly, in order to substitute host bit to the LSB of the cover image, those LSB's need to be vacant, means it should be zero. For that we subtract single LSB bit obtained in step 2 from the corresponding cover image pixel byte.

Step 4: Substitute the host bits to the LSB position of the cover image by simple addition of the cover image pixel obtained at step 3 with the shifted pixels from the corresponding bit planes.

Step 5: Now we have the stego image with the secret image embedded in it and is transmitted as per the user's requirement.

The algorithm for embedding the host image inside the cover image is shown below:

1. Start
2. Input: Secret image, Cover image;
3. Standardizing the image;
4. Bit plane slicing of the secret image;
5. Embedding the bit planes into the Cover image;
6. Output: Stego image;
7. End

C. Security Implementation

At the receiver, we have implemented double level security system. At the first level we need a security password. Only if the security password is acceptable, we can proceed to the second level. In this level there is a key image which is strictly banned from the outside world. On comparing, only if the key image matches, the decoding process begins. This is to avoid the possibility of retrieving the secret image by intruder's attacking trials.

D. Decoding Process

Decoding process is the exact reverse process of embedding technique. This is done in following steps:

Step 1: Collecting the LSB's of the cover image pixels to form the corresponding bit planes by re-shifting the bit position.

Step 2: Adding respective bytes of all bit planes comprise the pixels of the original secret image.

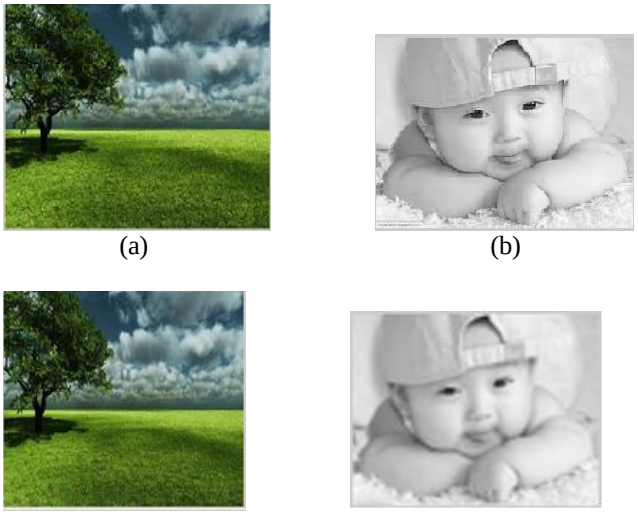
Step 3: Resizing the decoded image to its original size so that the image clarity retains.

The following shows the algorithm for the decoding process.

1. Start
2. Input: Stego image, Secret key, Key image;
3. Compare with Secret key;
4. Received the Stego image;
5. Compare with Key image;
6. Decode the Secret image;
7. Output: Secret image;
8. End

IV. EXPERIMENTAL RESULT

We carry out the proposed technique in the cover image with 480×360 pixels as shown in Fig. 2 (a). The secret image to be hidden is shown in Fig. 2 (b). The resulting stego image and the decoded secret image is shown in Fig. 2 (c) and 2 (d) respectively. From Fig. 2 (c) it is clear that the intended secret image does not attract attention to itself.



(a) (b)

(c) (d)

Fig. 2. (a) Cover image, (b) Secret image, (c) Stego image, (d) Decoded image

V. CONCLUSION

In this paper, we have proposed a method of image security by using LSB Steganography technique. Here the existence of a hidden image is unknown to unintended recipient. In order to enhance the security, we have used a secret password and a key image which is being shared with the receiver using a secret channel. With this algorithm, the stego image does not have a noticeable distortion on it. This can be used by various users who want to hide their confidential images without revealing it to other parties.

VI. REFERENCES

[1] Z. Hrytskiv, S. Voloshynovskiy & Y. Rystar "Cryptography of Video Information In Modem Communication", Electronics And Energefics, Vol. 11, PP. 115-125, 1998.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, no. 3.4, pp. 313-336, 1996.

[3] L.F. Turner, "Digital data security system," Patent IPN, WO 89/08915, 1989.

[4] Nirinjan, U.C. & Anand, D. "Watermarking medical images with patient information". In the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 1998, pp. 703-06.

[5] Katiyar, S. Meka, K.R. Barbhujya, F.A. & Nandi, S. "Online voting system powered by biometric security using steganography". In the 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India, 2011, PP. 288-291.

[6] Shirali-Shahreza, M. "Improving mobile banking security using steganography". In the 4th International Conference on Information Technology, ITNG, Las Vegas, 2007, pp. 885-887.

[7] Babloo Saha and Shuchi Sharma, "Steganography Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No.1, January 2012, pp. 11-18.

[8] Guangjie Liu, Zhan Zhang and Yuewei Dai, "Improved LSB-matching steganography for preserving second-order statistics", Journal of Multimedia, Vol.5, October 2010.

[9] P. Bateman, "Image steganography and steganalysis", Master's Thesis, Department of Computing, Faculty of Engineerring and Physical Sciences, University of Surrey, Surrey, United Kingdom, 2008.