Improved RGB -LSB Steganography Using Secret Key

Ankita Gangwar¹, Vishal shrivastava²

Computer science Department¹, Computer science department²
Research scholar¹, professor²

Mewar University, India¹, Rajasthan Technical University,India²

Abstract—This paper introduces a best approach for Least Significant Bit (LSB) based image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden information. It is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. In general, in LSB methods, hidden information is stored into a specific position of LSB of image. For this reason, knowing the retrieval methods, anyone can extract the hidden information. In our paper, hidden information is stored into different position of LSB of image depending on the secret key. As a result, it is difficult to extract the hidden information knowing the retrieval methods. The proposed method results in LSB based image steganography using secret key which provides good security issue than general LSB based image steganography methods.

Keywords—cover-image, secret key, Steganography, stego-image, LSB.

I. INTRODUCTION

In the past, people used hidden tattoos or invisible ink to uncover Steganographic content. Today, computer and network technologies provide easy to use communication channels for steganography. But privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. Steganography is a technique to hide information from the observer to establish an invisible communication [1]. Generally a steganographic system consists of cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a large opportunity in such a way that someone cannot know the presence of the hidden message. The goal of modern steganography is to keep its information undetectable [2]. Generally secret information is stored into the specific position of Least Significant Bit (LSB) of a cover image which is the carrier to embed messages [1, 2, 3, 4]. Anyone can ensure that the specific position of LSB contains secret information. So it is easy to recover the secret information for anyone by using retrieval method. The main intention of image steganography is to ensure security of hidden information. For security purpose, we have introduced a new approach of LSB based image steganography. Here we are adding a secret key which ensure the security of hidden information. The insertion of hidden information is totally controlled by the secret key. This secret key decides the appropriate position of hidden information. It is very difficult to retrieve the hidden information without the same secret key. So by using a secret key, we can increase the security level of the hidden information in LSB based image steganography. There are a number of researches available describing features of image steganography. Many steganographic methods have been proposed [2, 3, 4, 5, 6]. The most common of these is replacing least significant bits (LSB) of the pixels with the secret message. A well-known LSB based image steganography is presented in [3] and that proposed an adaptive method based on inter pixel relationship. This method greatly enhanced the stego image quality. It is possible to recover the secret information for anyone by applying the retrieval method. Another LSB based image steganography is presented in [2] and proposed three efficient steganographic methods that utilize the neighborhood information to estimate the amount of data to be embedded into an input pixel of cover image and that embed a fixed three bits of information in smooth areas and a variable number of bits are embedded into the edged areas. This method uses some pixels of the image to store too many bits of hidden information but other pixels remain unchanged. As a result, some pixels are distorted roughly but other pixels become unused. They also did not provide any security issue and it is possible to recover the secret information for anyone.

In this paper, we proposed an efficient LSB based steganographic method that utilizes the secret key to hide the information into an input pixel of cover image without producing perceptible distortions. Here a bit of hidden information is placed in either LSB of Green or Blue matrix of a specific pixel which is decided by the secret key. So anyone cannot exactly make a decision that the bit of hidden information is placed in either LSB of Green or Blue matrix. As a result, the security level of image steganography is attained.
II. LITERATURE REVIEW

The simplest approach to hiding data within an image is called least significant bit (LSB) insertion. For 24-bit true color image, the amount of changes will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

Now suppose we want to hide the following 9 bits of data 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed) pixels:

The following formula provides a very generic description of the pieces of the steganographic process:

\[
\text{cover image} + \text{hidden information} = \text{stego image}
\]

In this perspective, the cover image is the main image in which the hidden information will be embedded. The resultant image is the stego image (which will, of course, be the same type of image as the cover image).

A. Existing applications - LSB steganography using Secret key.

In this paper, we have taken the binary representation of the hidden information and overwrite the LSB of each byte within the cover image. Here we have introduced a secret key to protect the hidden information. The following formula, we have used in our proposed method is:

\[
\text{cover image} + \text{secret key} + \text{hidden information} = \text{stego image}
\]

B. Proposed Methods: Improved RGB-LSB image steganography using secret key.

The secret key is converted into one dimensional (1D) circular array bit stream as shown in below:

A 24-bit color scheme uses 24 bits per pixel and each byte represents the intensity of the three primary colors red, green, and blue (RGB), respectively. So, a cover image can be split into three matrices as shown in Fig. 2. The hidden information is converted from decimal to Binary. Each pixel is converted into 8 bit binary value. Then the 2D array is reshaped into a 1D array. This 1D array matrix is also called bit stream of hidden information.
The process to convert the hidden information into 1D array is shown in Fig. 3.

At Fig. 4, the LSB of Red matrix of pixel 1 is 0 and the first bit of secret key is 1. The XOR value of 0 and 1 is 1. In our method, if the XOR value is 1 then the LSB of Green matrix is replaced by the first bit of hidden information. If the XOR value is 0 then the LSB of Red matrix is replaced by the first bit of hidden information and it is continued as shown in figure. The 1D array of secret key is circular. The substitution process will be continued depending on the length of hidden information's 1D array.

C. Hiding Technique of Hidden Information
To hide hidden information we have to take a cover image. This cover image is divided into three matrices (Red, Green and Blue) as shown in Fig. 2. The secret key is converted into 1D array of bit stream. For the first three Pixels of Cover Matrix following procedure is applies:

- **Secret key** and **Red matrix** are used for decision making for the pixel 0,3,6……to replace hidden information into either Green matrix or Blue matrix. Each bit of secret key is XOR with each LSB of Red matrix. The resulting XOR value decides that the 1 bit of hidden information will be placed with either LSB of **Green matrix** or **Blue matrix**.

- **Secret key** and **Green matrix** are used only for decision making for the pixel 1,4,7……to replace hidden information into either Red matrix or Blue matrix. Each bit of secret key is XOR with each LSB of Green matrix. The resulting XOR value decides that the 1 bit of hidden information will be placed with either LSB of **Red matrix** or **Blue matrix**.

- **Secret key** and **Blue matrix** are used only for decision making for the pixel 2,5,8……to replace hidden information into either **Red matrix** or **Green matrix**. Each bit of secret key is XOR with each LSB of Blue matrix. The resulting XOR value decides that the 1 bit of hidden information will be placed with either LSB of **Red matrix** or **Green matrix**.

D. Recovery Technique of Hidden Information
To recover the hidden information, we have to take a stego image. This stego image is divided into three matrices (Red, Green and Blue) as shown in Fig. 2. Then we have to know the secret key. At Fig. 6, the LSB of Red matrix of pixel 1 is 0 and the first bit of secret key is 1. The XOR value of 0 and 1 is 1. In our method, if the XOR value is 1 then the LSB of Green matrix is replaced by the first bit of hidden information. If the XOR value is 0 then the LSB of Red matrix is replaced by the first bit of hidden information and it is continued as shown in figure. The 1D array of secret key is circular. The substitution process will be continued depending on the length of hidden information's 1D array.
shown in figure. Finally the 1D array is reshaped into 2D array to form actual hidden information. We take counter as C. The process to recover hidden information from stego image is shown in Fig. 5.

The secret key is converted into 1D array bit stream. Each bit of secret key is XOR with the each LSB of Red matrix of the stego image. The resulting XOR value decides that 1 bit of hidden information is stored in either LSB of Green matrix or Blue matrix of the stego image. The length of hidden information is stored in the first row of stego image during the hiding process. The recovery process will be continued depending on the length of hidden information bit stream.

III. EXPERIMENTAL RESULT AND DISCUSSION
A. Experimental Results
Experimental results are given in this section to demonstrate the performance of our proposed method. We used some standard RGB (true color) images as the cover image. Small size image is used as the hidden information. The hidden information used in our proposed method is shown below:

Three standard RGB (true color) image, is use as cover image. The images are shown in Fig.6. The hidden information which is used to hide into cover image is shown in Fig. 7. Hidden information is inserted into cover image with secret key. The resulting image is called stego image. The procedure to get stego image from cover image is shown in Fig. 8. The stego images resulted from our proposed method is shown in Fig. 9.

IV. CONCLUSIONS
The experimental results show that the proposed method is an effective way to integrate hidden information reporting and it is very difficult for the unauthorized users to identify the changes in stego image. The use of the secret key gives a way
to secure the information from illegal user. In our proposed method, we used a secret key to hide hidden information into cover image the LSB of RGB bits. This process provides a new dimension for image steganography. It is very difficult to recover the hidden information for third party without knowing the secret key.

REFERENCES


