A More Secure Steganography Method in Spatial Domain

ABSTRACT:

This paper presents a new approach for hiding message in digital image in spatial domain. In this method two bits of message is embedded in a pixel in a way that not only the least significant bit of pixel is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, But the point is in each embedding process only one alternation in one bit plane is allowed to happen. As it is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.

EXISTING SYSTEM:

- In special domain, the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods; hide data in another domain such as wavelet domain.

- Least significant bit (LSB) is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.
- LSB method has intense affects on the statistical information of image like histogram. Attackers could be aware of a hidden communication by just checking the Histogram of an image. A good solution to eliminate this defect was LSB matching. LSB-Matching was a great step forward in Steganography methods and many others get ideas from it

PROPOSED SYSTEM:

- In this paper it is planned to introduce a method that embed 2 bits information in a pixel and alter one bit from one bit plane but the message does not necessarily place in the least significant bit of pixel and second less significant bit plane and fourth less significant bit plane can also host the massage.

- Since in our method for embedding two bits message we alter just one bit plane, fewer pixels would be manipulated during embedding message in an image and it is expected for the steganalysis algorithm to have more difficulty detecting the covert communication. It is clear that in return complexity of the system would increase.

- In our method there are only three ways that a pixel is allowed to be changed:

    - Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
    - The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
    - The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)

ADVANTAGES

- User cannot find the original data.
- It is not easily cracked.
- To increase the Security .
- To increase the size of stored data.
- We can hide more than one bit.

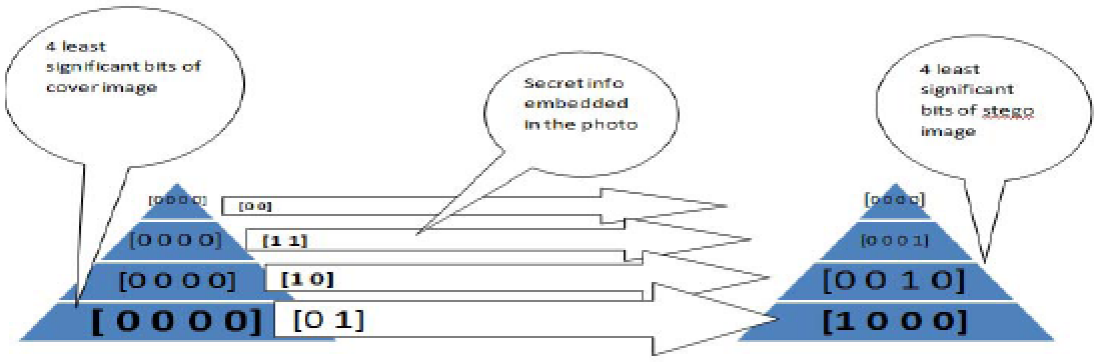

Fig. 2 How cover pixel with four less significant bits of [0 0 0 0] change according to different messages

HARDWARE REQUIREMENTS

Processor	: Any Processor above 500 MHz.
Ram	: 128Mb.
Hard Disk	: 10 GB.
Compact Disk	: 650 Mb.
Input device	: Standard Keyboard and Mouse.
Output device	: VGA and High Resolution Monitor

SOFTWARE REQUIREMENTS

Operating System	: Windows XP.
Coding Language	: Visual C# .Net
Simulation	: MATLAB (for checking Histogram of Original & Stegno image)

MODULE:

This project consists of developing Two main modules. The one is encryption module and the decryption module. These two modules are the main core for the application.

- **ENCRYPTION MODULE**

- In Encryption module, its consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image file through another open file dialog box which is opened when the image button is clicked. Where the user can select the bmp file and then the Hide button is clicked so that the secret data or message is hidden in Picture through LSB matching revisited technique.

- **DECRYPTION MODULE**
  - This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted image and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

REFERENCE:

Ali Daneshkhah, Hassan Aghaeinia, Seyed Hamed Seyedi, "A More Secure Steganography Method in Spatial Domain", In **IEEE 2011** Second International Conference on Intelligent Systems, Modelling and Simulation.