Steganography in Images Using LSB Technique

Arun Kumar Singh
Department of Electronics and Communication Engineering
Amity University Gurgaon, HR, India

Juhi Singh
Department of Computer Science Engineering
Amity University Gurgaon, HR, India

Dr. Harsh Vikram Singh
Department of Electronics and Communication Engineering
KNIT Sultanpur UP, India

Abstract- This paper, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.
Keywords— Steganography, data-hiding

I. INTRODUCTION

The use of multimedia digital signal has become very popular in the last decade due to the spread of wireless Internet-based services such as introduction of the fourth-generation mobile communication systems, user can transfer data up to 1Gbps [1].Due to the availability of low cost editing tools, digital data can be easily copied, modified and retransmitted in the network by any user. To effectively support the growth of multimedia communications, it is essential to develop tools that protect and authenticate digital information. In this contribution, we present a novel embedding scheme based on the LSB technique. [2] If the value of the pixel of an image is changed by a value of '1' it does not affect the appearance of the image. This idea helps us to for hiding data in an image.

II. STEGANOGRAPHY TYPES

STEGANOGRAPHY comes from the Greek Words: STEGANOS – "Covered", GRAPHIE – "Writing". [3] Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. 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 data can be hidden in basic formats like: Audio, Video, Text and Images etc. The various types of steganography include:

a. *Image Steganography:* The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.
b. *Audio Steganography:* Steganography can be applied to audio files i.e., we can hide information in an audio file, it can be called Audio Steganography. The audio file should be undetectable.
c. *Video Steganography:* Steganography can be applied to video files also. If we hide information in a video file, it can be called Video Steganography. The video file should be undetectable by attacker.

d. Text files Steganography: Steganography can be applied to text files also. If we hide information in a text file, it is called Text Steganography.

III. LSB METHODS

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

IV. GRAY SCALE

The following chart displays all 256 Gray-scale colors. [4] The gray-scale color naming scheme uses a two digit hex value to define up to 256 shades of gray. In photography and computing, a grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black (also called bi-level or binary images). Grayscale images have many shades of gray in between. Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. Gray scale Shading Strengths (0=no color; 15=full color) are given below in figure 1.

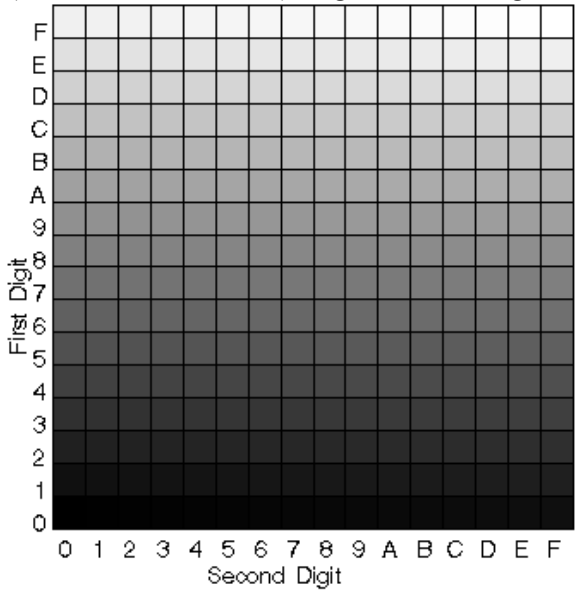

Figure 1: Gray Scale color

V. BLOCK DIAGRAM OF STEGANOGRAPHY

A message is embedded into the image by the stego system encoder via a secret key or password. [5] This password or secret key should be kept secret. The resulting stego image is transmitted over a channel to the receiver. The stego system at the decoder end, using the same key or password, will decode the stego image. Block diagram is shown in figure 2.

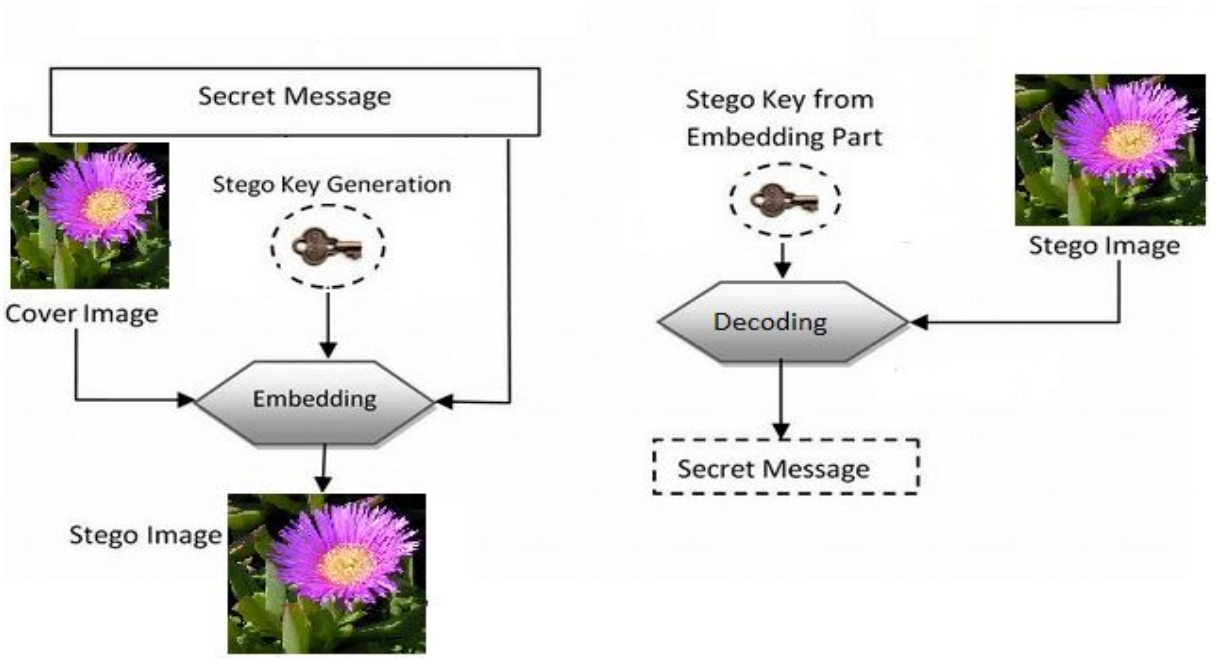

Figure 2: Block diagram of steganography[6]

VI. LSB DECOMPOSITION

There are two important components, cover image and hiding data, in data hiding technique. [7] The cover image I is an 8-bit gray scale image. The size of cover image is m×n. The hiding data H embedded in I is g-bits bit stream. We use the equation below to express image C, data D and each pixel separately. [8]

$$I = \{(c_{ij} | 0 \leq i < m,\ 0 \leq j < n,\ c_{ij} \epsilon [0,255])\}$$

$$H = [(d\_i \mid 0 \leq i < g,\ g \epsilon [1,2,3,4,5])]$$

One of the simplest systems for embedding digital data into a digital cover is the Least Significant Bit method [9]. Consider an $N \times M$ image in which each pixel value is represented by a decimal number in the range determined by the number of bits used. In a gray-scale image, with 8 bit precision per pixel, each pixel assumes a value between [0, 255] and each positive number P can be represented by:

$$P = b_0 + b_1 \cdot 2^1 + b_2 \cdot 2^2 + \cdots = \sum_{i=0}^{n} b_i \cdot 2^i$$

This property allows the decomposition of an image into a collection of binary images by separating the b_i into n bit planes. In the classical LSB embedding methods, the secret message is inserted into the least-significant bit plane of the cover image either by directly replacing those bits. The amount of data to be embedded may also be fixed or variable in size depending on the number of pixels selected. The main advantage of such a technique is that the modification of the LSB plane does not affect the human perception of the overall image quality as the amplitude

variation of the pixel values is bounded by ±1. The masking properties of the Human Visual System allow significant amounts of embedded information to be unnoticed by imperceptible by the average observer under normal viewing conditions. “Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal. A detailed review of these techniques is given in. Other advantages of LSB data hiding included high embedding capacity and low computational complexity. The main disadvantages are the weaknesses with respect to robustness, tampering, geometric attacks, filtering, and compression.

VII. LSB METHOD WITH AN EXAMPLE

In LSB steganography, the least significant bits of the cover media’s digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. [10] LSB replacement steganography changes the last bit of each of the pixel values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale color value. Suppose the first eight pixels of the original image have the following gray color values:

01010010
01001010
10010111
11001100
11010101
01010111
00100110
01000011

To hide the letter Z whose binary value of ASCII [11] code is 10110101, we would replace the LSBs of these pixels to have the following new values:

01010011
01001010
10010111
11001101
11010100
01010111
00100110
01000011

Note that, on average, only half the LSBs need to change. [12] The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats for the color image are difficult to detect contrary to 8 bit format.

VIII. ADVANTAGES

Steganography has unique advantages for net-espionage agents. Even if a file is known or suspected to contain Steganographic software, it is almost impossible to extract the information until the correct password is obtained. Steganography is beneficial for securely storing sensitive data, such as hiding system passwords or keys within other files. In places where standard cryptography and encryption is outlawed, Steganography can be used for covert data transmission.

IX. APPLICATIONS

Steganography can be used in supplementary to cryptography, watermarking and fingerprinting. [13]. Steganography can be used to conceal and transfer an encrypted document containing some acquired information in military applications.

X. FUTURE SCOPE

Still efforts have to be made to increase the embedding capacity and maintain secrecy. In this method we can hide text file equal to the size of the image. Efforts can be made to hide text files having more size than image size. The secret keys have to be known to both sender and receiver. Keys are not sent in cover-images but are distributed separately. A technique can be evolved so that these keys can be generated and distributed covertly. The Transform Domain method can be utilized if more security is required. If Steganography is used with Cryptography, it will

prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques.

REFERENCES

[1] Vasco Pereira and Tiago Sousa, "Evolution of Mobile Communications: from 1G to 4G", in Proc. Of The 2nd International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks, HET-NETs'04, West Yorkshire, U.K., July 2004

[2] http://studentweb.niu.edu/9/~Z172699/Description.html

[3] M. Pavani1, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467

[4] Stuti Goel, Arun Rana, Manpreet Kaur,"A Review of Comparison Techniques of Image Steganography", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48

[5] http://dimabatenkov.info/ssis_project/methods.htm

[6] http://dhsprojects.blogspot.in/2012/08/ieee-2012-separable-reversible-data.html

[7] A. I. Kahdum, "IBN AL-HAITHAM Journal for pure & applied Science", Vol.21(1) 2008

[8] http://studentweb.niu.edu/9/~Z172699/Description.html

[9] *Diego De Luca Picione , Federica Battisti , Marco Carli ,Jaakko Astola , and Karen Egiazarian,"*A FIBONACCI LSB DATA HIDING TECNIQUE*"*,14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASIP

[10] http://imagelpcmatlab.blogspot.in/2013/12/matlab-implementation-of-steganography.html

[11] http://www.asciitable.com/

[12] http://www.viprefect.com/application-areas

[13] http://studentweb.niu.edu/9/~Z172699/Conclusion.html