Image Block-based Steganography using Varying Size Approach

Vikas Verma
Dept. of CSE
RIET
Phagwara, Punjab

Rishma Chawla
Dept. of CSE
RIET
Phagwara, India

ABSTRACT

The field of data hiding in digital image processing becomes important as the use of public networks such as the Internet becomes popular and activities of spam increases. Various methods have been proposed and implemented in data hiding. Steganography is one such way to increase the security of messages over the internet. The least significant is one of the methods used in steganography. While most methods work bit by bit value or pixel by pixel value to hide the data. The one disadvantage of such methods is that there is low percentage of data that can be hidden. In this paper, a new algorithm has been proposed that works on blocks of images that are found same or similar in other image. As in today era, the size of digital images are quite large as compared to images used in early years of digital processing and the images contain randomized pixel having blocks of different sizes and variations in colors. This leads to similarity of block of one image with part of other image of same domain and the same approach is used to hide an image inside another image. In this regard, blocks of hiding image are matched up to maximum size m*n with parts of cover image.

Keywords

Image hiding, least significant bit (LSB), block based, steganography, varying size

1. INTRODUCTION

Steganography is art and science for invisible communication and play vital role on the network security. It is known as technique of hiding information within other information in such a way that it is hard or even impossible to tell that it is present in covering information. Hiding messages or information techniques are growing at considerable rate [1]. This is largely due to the fear of encryption services getting outlawed and the owners who want unauthorized access to information [2].

The word steganography in Greek means “covered writing” (Greek words “stegos” meaning “cover” and “grafia” meaning “writing”) [3]. Depending on the requirement of different applications, different steganography techniques are used. For example, some applications require that large information to be hidden while other applications may require that information to be completely invisible.

Generally, all types of digital file formats can be used for steganography but the file which contains redundant information can be better used as the redundant data can be modified to get new meaning and later on it can be again set to original one. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding [4].

Steganography and cryptography are two related fields. Cryptography scrambles a message so it cannot be understood, and unless the secret key is known, the original message cannot be recovered. Steganography hides the message so it cannot be seen or detected [5]. Two levels of protection can be done if the message is encrypted before hiding it, so it must be decrypted before reading it. Steganography differs from cryptography in the sense that where Cryptography focuses on concealing the contents of a message, steganography focuses on concealing the existence of a message [6]. Two other technologies that are closely related to steganography are watermarking and finger printing [7].

There are many carriers for steganography however the most popular is digital images. Typically, the message is embedded within another image known as a cover image using its properties. The resultant is an image known as a stego-image that looks similar as cover image but it also contains the hidden message. It is this stego-image that is sent between the sender and the receiver [8].

With the rapid development of information technology, security is the main concern for all. The information needs to be kept confidential and this has become challenging issue today. Steganography techniques have been developed in order to achieve the security. The stego media is similar to the cover media hence it is difficult for the hackers to detect the existence of secret message on the cover media. The hidden secret information can be extracted by retrieving algorithm.

Image steganography has become an essential and potential field in information hiding for protecting the confidential information [8]. The three important requirements need to be considered for steganographic model are [9] :

(i) Level of hiding: means to preserve the details of the cover image when the secret information is being embedded.

(ii) Amount of hiding: means the maximum number of bits that can be hidden with an acceptable resultant stego image quality.

(iii) Robustness: is the ability of stego image to retain its contents from attacks.

Fig. 1 shows the different ways of steganography.

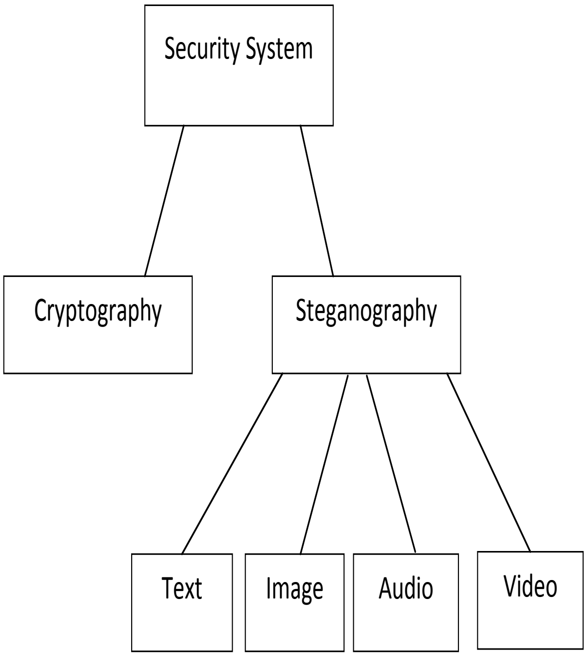

Fig. 1: Ways to achieve Steganography [10]

2. STEGANOGRAPHY METHODS

There are broadly two categories, namely Spatial Domain and Transform Domain under which embedding techniques fall. These techniques work on difference approaches on cover image with different constraints but with the same objective of securing and maximizing hidden data [11].

In Spatial Domain methods, approach is used on the principle of tuning the parameters of the cover-image so that the difference between cover-image and the stego-image is little and imperceptible to the human eye. One of the reasons of acceptability of these kinds of approaches is simple algorithmic nature and ease of mathematical analysis [12]. The most widely known image based on modifying the least significant bit (LSB technique). As the resolution and depth of color increase in an image, the impact of manipulating the LSB becomes less noticeable. Hence high resolution images are preferred for use as cover-images.

On the other hand, there are number of transform embedding approaches which includes Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [12]. Irrespective to the domain, transform coefficients are selected to mix with the secret data so that information is not visible to human eye.

Now a days, steganography methods use text, image, audio or video media. One media is being used to hide other type of information, say, a text file can be used to hide audio information or image file can be used to store video information.

This section attempts to provide the most common methods employed under steganography techniques in digital world. As discussed, the preferred media for steganography are text, image, audio and video. Since text files have very small amount of redundant data, text steganography is not very useful. As per scenarios, images are the most useful and popular cover media to hide objects – may be text, image, audio or video objects.

Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use three primary colors – RED, GREEN and BLUE. This RGB model of colors is also known as true color [13]. Each primary color is represented by 8 bits [14]. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors [13].

Following is the brief of commonly known steganography methods.

2.1 Least Significant Bit:

In this method, the least significant bit or bits of each pixel in an image may be used to hide the information. As change of least significant bit of a pixel result in a minor change of color that is invisible to the human eye. Due to the large size of bmp images, they are capable of hiding large data as compared to jpeg images. Some variations of Least Significant Bit methods are also proposed. These variations make the algorithms strong as compared to earlier version of LSB techniques. As an example, from an image, a set of pixels based on mid-point circle algorithm are selected that are used to embed information about secret text [15].

2.2 DCT-based steganography:

It gained its importance by being associated to the famous format of JPEG. The technique consists of dividing the cover image into blocks and then applying the DCT. Afterwards, the coefficients are compared and manipulated so that object information to hide is inserted in these coefficients [16]. The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each [17, 18].

3. PROPOSED WORK

This algorithm proposes a novel method of embedding and extraction of data in black and white as well as color images. This method uses the approach of variation of gray scale or colors in image of large dimensions. More the number of pixels are there in an image, greater is the probability of matching of its part with part of another image of same domain. If we have a database of images of different domain and an image to hide, we can search for a cover image from database based on the matching criteria of the image with image to be hidden. In this approach, we start with block of image to hide of dimension m*n with prior minimum condition on m and n pixel values. This block is being searched for match with block within cover image. If any block is being found we can increment the size gradually from both the cover image and secret image to find the block of maximum size of p*q pixels that matches with the block of image to hide. The same process is repeated from one left to right and top to bottom to cover all parts of hiding image.

Major steps of the algorithm are described below:

- Start with top left corner of image to hide, pick up a block of m*n size with minimum values as set depending on the application.
- Starting with top left corner of cover image and moving left to right and top to bottom, search for the block in the cover image. When the match is found, increase the column width of block being searched and repeat the process till the match is found in block cover image.

- Now the maximum width for one block has been found, moving downward increasing the height of block to search in cover image. In this way maximum block size is found.
- Note down the top left and bottom right co-ordinate positions in the cover image where the block matched.
- Pick up the next block from image to hide and repeat the same process till we cover all parts of image to hide.
- For now, the blocks positions have been found and stored in an array.
- Use a string to store the information within two dimensional arrays as message of bits.
- Compress the message to reduce the storage amount required.
- Encrypt the message using a private key.
- Store the encrypted message in the cover image using Least Significant Bit image steganography technique.

Fig. 2 demonstrates the finding of secret image block inside the cover image.

4. CONCLUSION AND FUTURE WORK

As compared with the traditional Least Significant Bit algorithm and other block based image steganography techniques, the data hiding steganographic method presented in this paper was found to be of increased imperceptibility to steganalysis attacks on the cover image. Moreover, this method has the capability to embed large information that matches with the cover image parts. Larger the block matching found, greater is the hiding capability. Therefore, this method is best suited for the purposes of communication applications.

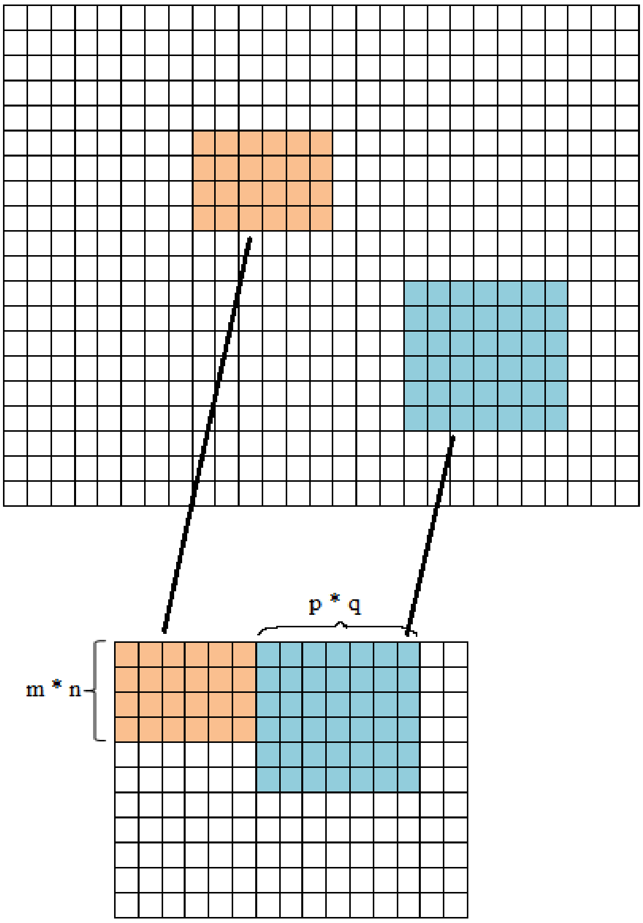

Fig. 2: Cover Image and image to hide.

The recommended mode of transmission of stego images is through email attachments or web postings. Unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression [2]. For example, converting a GIF or a BMP image, which reconstructs the original message exactly (lossless compression), to a JPEG format, which does not (lossy compression), and then converting back, can destroy the data in the LSBs [14].

In relation to present research, future work would centre on working on selection of image from pool of database that would act as cover image as per its feature extraction properties. Also the technique would be extended for more generalization as far as the sizes of blocks are concerned. This will facilitate the use of steganography in more sensitive application areas like in electronic commerce, online trading and digital forensics.

5. REFERENCES

[1] Ghazanfari, K., Ghaemmaghami, S., Khosravi, S. R., “LSB++: An improvement to LSB+ Steganography,” TENCON 2011 -2011 IEEE Region 10 Conference, Bali, 2011, pp. 364-368.

[2] Katzenbeisser, S., Sadeghi, A. Information Hiding, 11th International Workshop (2009) Darmstadt, Germany, June 8-10, 2009, Lecture Notes in Computer Science 5806, Springer.

[3] Moerland, T. (2009) Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[4] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

[5] B. Pfitzmann, Information Hiding Termonology, Proc. First Int’l Workshop Information Hiding. Lecture Notes in Computer Science No. 1,174, Springer- Verlag, Berline, 1996, pp. 347-356.

[6] Wang, H and Wang, S, (2004) Cyber warfare: Steganography vs. Steganalysis, Communications of the ACM, 47:10, October 2004.

[7] Jamil, T., (1999) Steganography: The art of hiding information is plain sight, IEEE Potentials, 18:01, 1999.

[8] H. B. Kekre, Sudeep D. Thepade, Ratnesh N. Chaturvedi, Block Based Information Hiding using Cosine, Hartley, Walsh and Haar Wavelets, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-1 Issue-9 March-2013.

[9] Dr. H. B. Kekre, Archana B. Patankar and Dipali Koshti “Performance Comparison of Simple Orthogo-Nal Transforms and Wavelet Transforms for Image Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 44– No.6, April 2012.

[10] Abbas Cheddad, Joan Condell ,Kevin Curran, Paul McKevitt School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulsterat Magee, London derry, BT487JL, Northern Ireland, UK Contents lists available at Science Direct journal homepage: www.elsevier.com/locate/sigpro Signal Processing.

[11] Yambin Jina Chanu, Themrichon Tuithung, Kh Manglem singh, "A Short Survey on Image Steganography and Steganalysis Technique," IEEE Trans., 2012.

[12] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image," IEEE Trans. International Congress on Image and Signal Processing, 2011, pp. 252-255.

[13] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[14] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.

[15] Vikas Verma, Poonam, Rishma Chawla, " An Enhanced Least Significant Bit Steganography Method Using Midpoint Circle Approach," IEEE International Conference on Communication and Signal Processing, 2014, pp. 692-695.

[16] Wen-Yuan Chen and Chin-Hsing Chen, "Public-key image steganography using discrete cosine transform and quadtree partition vector quantization coding", Optical Engineering 42, 2886-2892, 2003.

[17] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf.

[18] Chang, C.-C., Chen, T.-S., and Chung, L.-Z. (2002) A steganographic method based upon JPEG and quantization table modification, Information Sciences, vol. 141, 2002, pp. 123-138.