Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.377 – 381

RESEARCH ARTICLE

An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace

Shweta Maurya[1], Vishal Shrivastava[2]

[1]M.Tech Scholar (C.S.E)
Arya College of Engineering and I.T, Jaipur, India

[2]Professor (C.S.E)
Arya College of Engineering and I.T, Jaipur, India

Abstract- Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. The proposed work improves the imperceptibility of steganographic approach and developed new algorithm using modifying approach. A comparative analysis of the proposed algorithm with the existing techniques using the statistical hypothesis testing framework is introduced in the proposed work and also we have evaluated the performance on comprehensive set of color images.

Keywords— Cover image, LSB method, PSNR, Steganography, Stego-image

I. Introduction

A. Steganography Definition

The idea of information hiding is nothing new in the history. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. In the modern world of digital communication, there are several techniques used for hiding information in any medium. One of such technique is steganography[4] in which digital media mainly digital images are used as a medium for hiding information and the

information in the form text, digital image, video or audio file may be used as secret message. The word steganography derived from two Greek words: steganos means covered and graphos means writing and often refers to secret writing or data hiding [5]. The major goal of steganography is to increase communication security by inserting secret message into the digital image, modifying the redundancy or nonessential pixels of the image [1], and is recently become important in a number of application areas especially military and intelligence agencies which require unobtrusive communications. Digital images stored in computer systems are composed of finite number of elements in the form of array; each element has its particular location and value, mostly known as pixels. In case of 24 bit color image each pixel has three color components: Red, Green, and Blue (RGB). Each pixel is represented with three bytes to indicate the intensity of these three colors (RGB). Steganography is quite differ from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [6]. Cryptography is derived from Greek word kryptós, means hidden, and gráphein means to write and is the study of means of converting information from its normal, comprehensible format into an incomprehensible format. Its main aim is to present message in unreadable format without secret knowledge, known as the encryption. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. If the presence of hidden information is suspected or even revealed, the purpose of steganography is partly defeated [6]. Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data into an unreadable format called cipher so that an unintended recipient cannot determine its intended meaning. On the other hand steganography attempts to prevent an unintended recipient from suspecting that the data is there [7]. Nowadays, using a combination of steganography and the other methods such as cryptography, information security has improved considerably. In addition to being used in the covert exchange of information, steganography is used in many other fields such as copyright, preventing e-document forging. For the past decade, many steganographic techniques for still images have been presented. A simple and well known method is directly hiding secret data into the least-significant bit (LSB) of each pixel in an image. Then based on the LSB technique, an algorithm for 24 bit color image is developed improves the stego-image quality of color image.

II. REVIEW OF STEGANOGRAPHY

The term steganography illustrates the art and science of hidden communication. By using steganography there is a chance to send messages so that nobody can detect the existence of the message. The message is embedded by weakening some characteristics of another media, which is called cover. Final output has equal properties to cover media, and also it includes our secret information. This new object is transmitted. If somebody is able to interpret this transmitted package, the secret message can be distinguished. While this transmitted package is really similar to cover media, detection of any embedded information is very difficult. For implementation of the steganography system, two algorithms are needed to be designed: one for hiding data and the other to extract this successfully. The main subject in embedding algorithm is to hide the secret message within the cover media without attracting any attention. The extraction algorithm has a simpler process and can be achieved by inversing the steps of embedding algorithm.

The secret message usually is a text file or another image file which contains the secret information. This file is sent to the encoder unit in the first step. The encoder must be designed and implemented with high precision, to hide the secret message with a few distortion and changes in the cover image. Encoder unit usually needs a key to increase the security level of hiding method; this key is used in extraction phase too. Without using this key, the message will be available without any impediment, if someone guesses the embedding or extraction algorithm.

Output of the encoder unit is called steganograme which should be close enough, to cover media. Then this image and the key, which is used in embedding phase, are transmitted via a communication channel. In the next step this package are applied to decoder unit. Output of the decoder unit is delivered in the receiver side. The output of extraction unit is just an estimate of secret message, because during transmission through the communication channel, the steganograme is exposed to different types of noises, which can change the values of some bits. The application of steganographic technique can be broadly classified as operating in two different domains, such as spatial domain and frequency domain. In spatial domain, the embedding and hiding process are mostly carried out by bitwise manipulation. For example, manipulating the LSB in one of the color components in an image. While, the frequency domain includes those which involve manipulation of transformed image such as Discrete Cosine

Transformation (DCT) and wavelet transformation. Such manipulation includes changing the value of the quantized DCT coefficients.

III. Proposed Approach

The process of embedding data in this proposed algorithm is to RGB color cover image is taken up and its individual color channel are separated. Then change the colorspace to YCbCr. Select the Cr Channel and divide it into 8*8 size block. The text message to be embedded into cover image is encoded to form a bit sequence.
For each bit of the sequence are following method is apply.

(a)Take each block of Cr channel and then each block is transformed to the discrete cosine transformation domain.

(b)Select appropriate coefficient using the randomly generated secret key known only to rightful owner.

(c)Insert each bit into these coefficient.

After placing the modified block into their corresponding position to form modified Cr channel, change back the colorspace from YCbCr to RGB. Then stego image is formed. Therefore the perceptibility of image can be increased after changing the DCT values.

Perceptibility of this change is calculated with the Peak Signal-to-Noise Ratio (PSNR), which is used in the noisy communication channels to evaluate the ratio between the signal and the noise. The phrase PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is most easily defined via the mean squared error (MSE).

$$MSE=(1/MN)\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij}-X'_{ij})^2 \qquad \text{eq(1)}$$

$$PSNR=10.\log_{10} I\text{^}2/MS \qquad \text{eq(2)}$$

where:
Xij is the *ith* row and the *jth* column pixel in the original (cover) image,
Xij is the *ith* row and the *jth* column pixel in the reconstructed (stego) image

Here, I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. Usually the images with PSNR value less than 40, will be extremely ruined and cannot be compared with the original image. For decoding the message in the receiver side, these parameters will be used to extract the secret message successfully. These parameters work as a key. Without any information about this key nobody can access the message correctly. There for the security level in this algorithm is higher than the JSteg algorithm which does not use any keys for communication.

IV. RESULTS OF ALGORITHMS

Our colorization method produces believable colorized output images. We have colorized images in various color spaces and our method produced best results in YCbCr color space, we have presented a comparison between results obtained by our proposed method to 24 bit color image (improved LSB) [2][3] in Table (1-2). The results are compared with the original target image based on various parameters like Mean SquareError (MSE), Peak Signal to Noise Ratio (PSNR). As is apparent from this comparison proposed method produces much better results. Images of various dimensions ranging from 256X256 to 1024x1024 were tested and the method proved Successful.

Table I. The PSNR(db) of Stego Images-Our First Steganography Method

Method/image	Lena	peppers	Babbon	Airplane
Our Proposed method	50.99	50.06	50.98	50.05

Table II: Comparison of PSNR (in dB) of the stego image in different method

Technique	Psnr
[2] 24 Bit Color Image (Improved LSB) Method	42.69
[3] A Stegnograpy Implementation Based On DCT Method	40.67
Our Proposed method	50.99

V. Conclusion

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. The image quality remains much conserved and robustness to the stego-attacks is also better in our proposed steganography technique based on colorspaces. This was the main concern of this research. The method presented has very good performance in imperceptibility.

References

[1] Feng, J.B., Lin, I.C., Tsai, C.S., Chu, Y.P., 2006. Reversible watermarking: current status and key issues. International Journal of Network Security 2 (May), 161–170. .

[2] Deepesh Rawat and Vijaya Bhandari ‘A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image’, International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013

[3] Gurmeet Kaur and Aarti Kochhar ‘A Steganography Implementation based on LSB & DCT’ International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends” 4(1): 35-41 (2012)

[4]. M. M Amin, M. Salleh, *S.* Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin "Information Hiding using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia. 2003 IEEE.

[5] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

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

[7] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science,Springer, 1998. pp. 32-47.

