IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by
Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

IMPROVED IMAGE QUALITY WITH CRYPTOGRAPHY AND STEGANOGRAPHY FOR COLOURED IMAGE PROCESSING

G Kanishka[1]*, S Elavarasi[1], V Divyavani[1] and V Indhu[1]

Corresponding Author: **G Kanishka ✉ kanishkasabari@gmail.com*

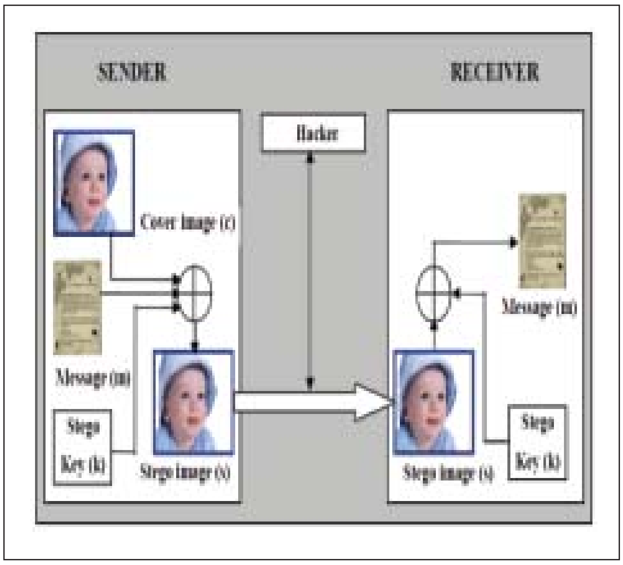
Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. 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 exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this project we proposed an image based steganography that Least Significant Bits(LSB) technique, pseudo random encoding technique and partial optimization technique on images to enhance the security of the communication.. We proposed a new method called Partial Optimization Technique, in the proposed approach all of the image pixels are classified into eight regions and then the eight distinct ordering coding are applied to each region by the developed partial optimization encoder.

INTRODUCTION

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data.A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent

[1] Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur,Tamilnadu, India.

unconventional but promising steganography mediums. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Thus, this work addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality.



STEGANOGRAPHY AND CRYPTOGRAPHY

Cryptography and steganography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message. Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents. Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists..

STEGANOGRAPHY AND WATERMARKING

Steganography aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of steganography and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of steganography is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object. This aspect or feature of watermarking is known as “robustness”.

APPLICATIONS OF STEGANOGRAPHY

Secret Communications - The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.*Copyright Protection mechanisms* that prevent data, usually digital data, from being copied. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

IMAGE DEFINITION

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. An image map is a file containing information that associates different Grayscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour are represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue.

IMAGE COMPRESSION

In images there are two types of compression: lossy compression and lossless compression. In Lossless compression, with lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file). Lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).

SPATIAL DOMAIN TECHNIQUE

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly Least Significant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques.

MASKING AND FILTERING

Masking and Filtering is a steganography technique which can be used on grayscale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

TRANSFORM DOMAIN TECHNIQUE

The Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against at tacks. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. Most of the strong steganographic systems today operate within the transform domain Trans form domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

DISTORTION TECHNIQUES

In this technique, store information by signal distortion and measure the deviation from the original cover in the decoding process. Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. In this technique, a stego-image is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels.

CHARACTERISTICS FEATURE OF DATA HIDING TECHNIQUES

Perceptibility does embedding message distort cover medium to a visually unacceptable level.*Capacity* how much information can be hidden with relative to the change in perceptibility.*Robustness to attacks* can embedded data exist manipulation of the stego medium in an effort to destroy, or change the embedded data.

Tamper Resistance Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter a message once it has been embedded in a stego-image.

IMAGE STEGANALYSIS

Steganalysis is the breaking of steganography and is the science of detecting hidden information. The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image.

EXISTING METHOD

Secure Information Hiding

An information hiding system has been developed for confidentiality. However, in this chapter, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image. The implementation of system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below.

Least-significant Bit Technique

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.The cover image is shown in Figure 4.1 and a hidden message is shown in Figure 4.2. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images as shown in Figure 4.3. The hidden image is extracted from the stego-image by applying the reverse process. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below,

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0

S(i.j) = C(i,j), if LSB(C(i,j)) = m

S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

where, LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded. S(i,j) is the stego image.

As we already know each pixel is made up of three bytes consisting of either a 1 or a 0. For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:

(11101010 11101000 11001011)

(01100110 11001010 11101000)

(11001001 00100101 11101001)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.

(11101010 11101001 11001010)

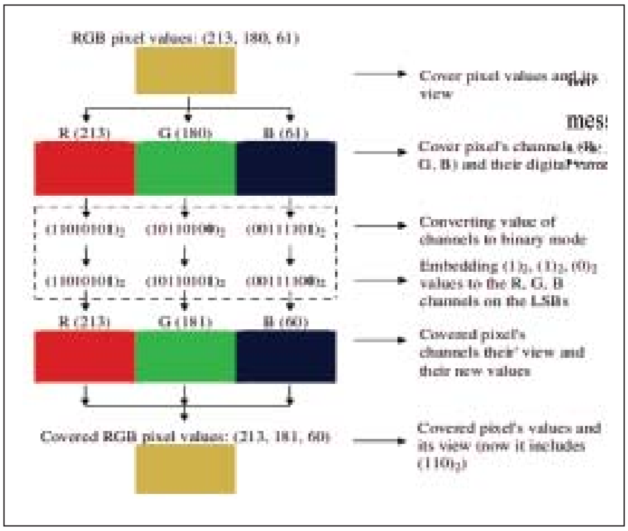
(01100110 11001011 11101000)

(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognised by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these method. LSB The

PSEUDO-RANDOM ENCODING TECHNIQUE

The simplest data hiding techniques embed the bits of the message directly into the LSB plane of the cover image in a deterministic sequence. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is too small. Other techniques process the message with a pseudorandom noise sequence before or during insertion into the cover image. The advantage of LSB embedding is its simplicity, and many techniques use these methods. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the covered image. Scaling, rotation, cropping, the addition of noise, or lossy compression to the covered image is very likely to destroy the message. Furthermore, if an attacker suspects, he/she can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified covered image. Specific LSB techniques can embed data in an image, audio, and text covers. Figure 4.6 shows a LSB application example for a red, green, and blue (RGB) pixel. In a typical full-color image that includes 24 bits/pixel, as seen in Figure 4.6, 8 bits are assigned to each of the color components. In a gray scale image, 8 bits/pixel are used. A digital image consists of a matrix of color and intensity values. Color image files can get quite large but some compression schemes have been developed to decrease the storage and communication requirements of handling image files. Bitmap and GIF files use a lossless compression algorithm.


RGB pixel values: (213, 180, 61)
Cover pixel values and its view
mes
R (213)
G (180)
B (61)
Cover pixel's channels (R, G, B) and their digital values
(11010101)$_2$
(10110100)$_2$
(00111101)$_2$
Converting value of channels to binary mode
(11010101)$_2$
(10110101)$_2$
(00111100)$_2$
Embedding (1)$_2$, (1)$_2$, (0)$_2$ values to the R, G, B channels on the LSBs
R (213)
G (181)
B (60)
Covered pixel's channels their' view and their new values
Covered RGB pixal values: (213, 181, 60)
Covered pixel's values and its view (now it includes (110)$_2$)

With the lossless compression algorithm, the decompressed image is identical to the original image (i.e. the image before compression). JPEG files use a lossy compression algorithm that approximates the image being compressed. With the lossy compression algorithm, the decompressed image is nearly the same as, but not identical to, the original image. Although data hiding can be applied on compressed images, it is more complex than data hiding on raw images.

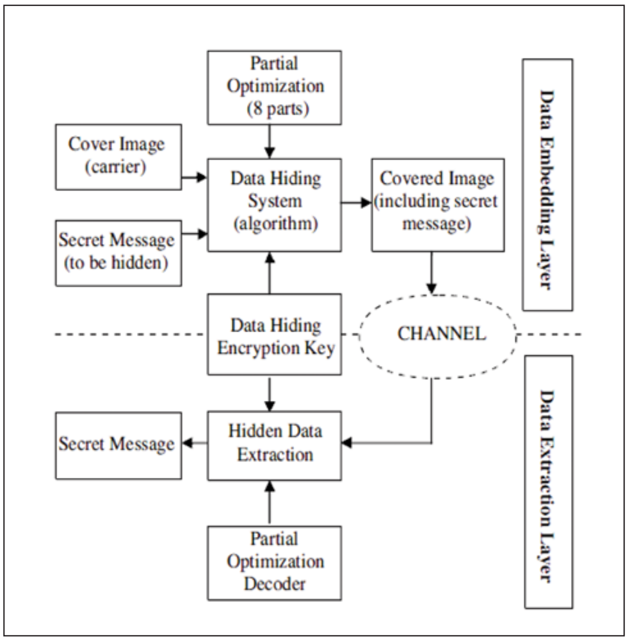
EXTRACTION OF HIDDEN MESSAGE

In this process of extraction, the process first takes the key and then random key. These keys take out the points of the LSB where the secret message is randomly distributed. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match .i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding.

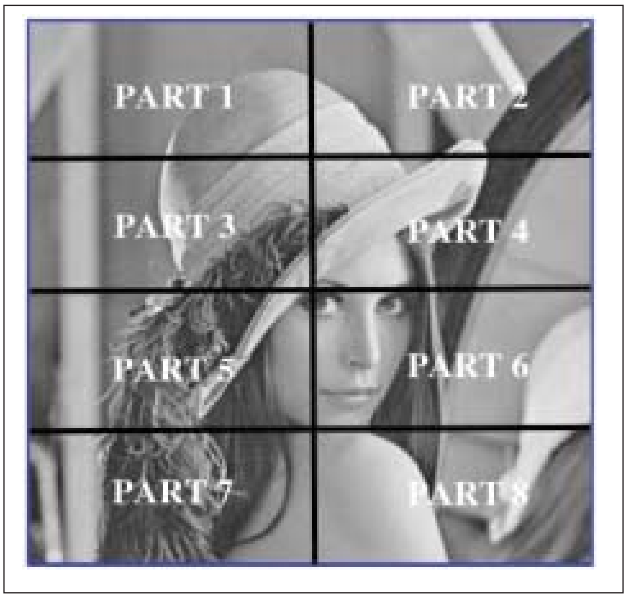
PROPOSED METHOD

PARTIAL OPTIMIZATION METHOD

There are five components needed to understand partial optimization-based data hiding processes. There is a carrier, technically called 'cover' and denoted by the letter 'c'. The letter 'm' denotes the secret message that needs to be hidden. Partial optimization is denoted by the letter 'p', where the cover image is separated into eight distinct parts in this stage. Next is the output called the covered image, denoted by the letter 's', into which the message m needs to be embedded. Finally, the data hiding encryption key is denoted by 'k'.


Partial Optimization (8 parts)
Cover Image (carrier)
Data Hiding System (algorithm)
Covered Image (including secret message)
Secret Message (to be hidden)
Data Embedding Layer
Data Hiding Encryption Key
CHANNEL
Secret Message
Hidden Data Extraction
Partial Optimization Decoder
Data Extraction Layer

The output s is obtained using ‘c + m + k + p’ in the data embedding encoder or technique. The data extraction/decoder process is to be constituted by three components. The key that is used in the coding process is necessitated in the decoding procedure.



These variations are applied to 8 parts of the image. It can be easily seen that Optimization 1 is the classical LSB data hiding methods bit array. The most effective outcome obtained from each region means that the number of altered bits is minimum. Hence, the minimal values that have been attained from the 8 regions compose an extraction that has lower bit error rate. Finally, the most suitable optimization method is determined for each image part and the LSB data hiding method is applied to the cover image.

Optimization 1	D_7	D_6	D_5	D_4	D_3	D_2	D_1	D_0
Optimization 2	D_0	D_1	D_2	D_3	D_4	D_5	D_6	D_7
Optimization 3	D_7	D_6	D_5	D_4	D_0	D_1	D_2	D_3
Optimization 4	D_0	D_1	D_2	D_3	D_7	D_6	D_5	D_4
Optimization 5	D_7	D_5	D_3	D_1	D_6	D_4	D_2	D_0
Optimization 6	D_0	D_2	D_4	D_6	D_1	D_3	D_5	D_7
Optimization 7	D_1	D_3	D_5	D_7	D_0	D_2	D_4	D_6
Optimization 8	D_6	D_4	D_2	D_0	D_7	D_5	D_3	D_1

MEASURE THE IMAGE QUALITY

In order to measure the image quality, the mean square error (MSE) and peak signal to noise ratio (PSNR) have usually been used in the literature. The MSE should be computed first, as given in Equation 1, and then the PSNR can be derived, as in Equation 2. Here, ‘O’ and ‘C’ are the original image and the covered image pixelvalues (binary) respectively, to be compared and the image size is ‘m x n’.

$$MSE = \frac{1}{m\ x\ n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||\,O(i,j)-C(i,j)||^2$$

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

The PSNR quality metric is used for comparing the classical LSB data hiding method and the proposed method.

CONCLUSION AND FUTURE WORK

Steganography is an effective way to hide sensitive information. The ultimate objectives of the Steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. In this project we proposed an image based steganography that Least Significant Bits technique, Pseudo Random Encoding technique and Partial Optimization technique on images to enhance the security of the communication. In future we are going to improve the quality of hidden image which is used for our analysis. And also the performance of above techniques are analysed through the MATLAB simulation on colour images.

REFERENCES

1. Hong W, Chen T S (2012), "A novel data embedding method using adaptive pixel pair matching," *IEEE Transactions on Information Forensics and Security,* Vol. 7, pp. 176-184.

2. Yalman Y, Akar F, Erturk I (2010), "An image interpolation based reversible data hiding method using r-weighted coding," *13th IEEE International Conf. on Computational Science and Engineering,* pp. 346-350.

3. Yalman Y, Erturk I (2009), "A new histogram modification based robust image data hidintechnique," 24th IEEE International Symposium on Computer and Information Sciences, pp. 39-43, 2009.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991