International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.1, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

STEGANOGRAPHY WITH IMPROVED IMAGE QUALITY

AMITOZ SINGH RATHORE[1*], SUR SINGH RAWAT[2]
[1,2]Department of CSE, Jssaten Noida

Article Received: 18/02/2015 | Article Revised on:24/02/2015 | Article Accepted on:28/02/2015

AMITOZ SINGH RATHORE

ABSTRACT

Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). In this paper we present a technique that hides the secret message based on searching about the identical values between the secret messages and image pixels.

Keywords: Steganography, Psnr ,Text and Image

INTRODUCTION

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means "cover writing" . Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information. Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

Information-Hiding System Features

An information-hiding system is characterized be having three different aspects that contend with each other capacity, security, and robustness.

Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information . Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossibleto remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

Types of Steganography

Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of steganography.

• Fragile

Fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile steganography techniques tend to be easier to implement than robust methods.

• Robust

Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived.

There are two main types of robust marking. Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can use the fingerprint to identify which customer violated the license agreement by distributing a copy of the file.

Unlike fingerprints, watermarks identify the copyright owner of the file, not the customer. Whereas fingerprints are used to identify people who violate the license agreement watermarks help with prosecuting those who have an illegal copy. Ideally fingerprinting should be used but for mass production of CDs, DVDs, etc it is not feasible to give each disk a separate fingerprint.

Steganography Methods:

Steganography is differentiated on the basis of the media in which we hide the data. These are: text, image, audio and video.

A. Text Steganography

The Steganography method uses the text media to hide the data known as text Steganography. There are different techniques to embed the secret data in text files.

- Format Based Method
- Random and Statistical Method
- Linguistics Method

Format Based Method: This method modifies the existing text to hide the data in such a manner that it involves the insertion of spaces, resizing the text, change the style of text.

Random and Statistical Method: In this methodcharacters are hidden that appeared in random sequence. Statistical method determines the statistics such as mean, variance and chi square text which measure the amount of redundant information to be hidden within the text.

Linguistics Method: It is the combination of syntax and semantics. Syntactic steganalysis ensure the correct structure as the text is generated from grammar. In semantic method value is assigned to synonyms and data can be encoded to the actual word of text.

B. Audio Steganography

When secret data is embedded into digital sound, the technique is known as audio steganography. This method embeds the secret message in WAV, AU and MP3 sound files. There are different methods through which audio steganographyexplored:

- Low Bit Encoding
- Phase Coding
- Spread Spectrum

Low Bit Encoding: This method is used by pitch period prediction is conducted during low bit speech

encoding. Thus, maintaining synchronization between information hiding and speech encoding.

Phase Encoding: In this method, stream file splits audio into blocks and embed whole secret sequence into phase spectrum of the first block.

Spread Spectrum Encoding: One particular method of spread spectrum encoding is DSSS (Direct Sequence Spread Spectrum) which spread steganography by multiplying it by certain pseudorandom sequence.

C. Image Steganography

In this method, images are used as cover object. The image Steganography, data hiding method can be classified into different categories. These are spatial domain, frequency domain, and adaptive domain.

Spatial Domain Steganography: In spatial domain, cover image and secret data modified by using LSB and level encoding. First, the cover image is decomposed into bit planes and then LSB is of bit planes replaced with secret data fit. LSB substitution is the mostly used steganographic technique. This substitution concept includes embedding at the minimum weighting bit as it will not affect the value of original pixel. LuonChing Lin [5] proposed a scheme of data hiding in spatial domain with tolerance of distortion. This method provides better image quality. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, a secret listener can easily extract the data that we are sending.

Frequency Domain Steganography: In frequency domain, secret data is hidden in significant areas of covered image, which makes data invigorate to attacks such as compression, cropping or image processing methods than LSB approach. This provides an enhanced security level to steganography method and lead to the development of algorithms. This method transforms include DCT, DWT and DFT. A lossless and reversible scheme have been introduced that use each block of quantized DCT coefficient in JPEG image for secret data [6]. The method results in high stego image quality and achieves reversibility.DCT coefficients of an image used for embedding data bits. F5 embeds data in DCT coefficient by rounding the quantized coefficients to the nearest data bit. It also uses matrix encoding for reducing the embedded noise in the signal. F5 is one of the most popular embedding schemes in DCT domain. Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in image because wavelet separately partitions the high frequency and low frequency information pixel by pixel. This scheme mainly addresses the capacity and robustness of the data hiding system.

In recent year, DWT based algorithm for image has been proposed. These algorithms use CH band of cover image for hiding secret data.

Adaptive Steganography: This steganography method is a special case of two methods: spatial domain and transform domain. It is also known as “Statistics Aware Embedding” and Masking”. Global features of images are used before embedding secret data in coefficients of DCT or DWT. This statistics will decide where changes can be made.

The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels.This function "hides" a message within an image that theuser provides. The final output is an image file that contains the message protected by encryption and encoding. This function will eventually be expanded to randomly "hide" the message across the "canvas" message or the cover image.

Algorithm (1) **The Proposed encoding Algorithm.**

Inputs: Cover Image, Image file or text file, key

Output: Stego image.

Begin

Determining Message Type and Normalize

If message is text convert from ascii to integer values

If message is image convert to integer value representation

Ensure sufficient hiding space

Ask for the key value to be used for xor encryption

Scan the image row by row and encode it in binary.

Check the size of the image and the size of the secret message.

Start sub-iteration 1:

Choose one pixel of the image randomlydivide the image into three parts (Red, Green and Blue parts) hide two by two bits of the secret message in each part of the pixelby searching about the identical.

If the identical is satisfied then set the image with the new values.otherwise hide in the two least significant bits and set theimage with the new valuessave the location of the hiding bits in binary table.

End sub-iteration 1.

Set the image with image values and save it

End

The Proposed decoding algorithm:-This algorithm "reveals" hidden messages by reversing the processing steps completed by the Encoding algorithm.

Algorithm(2): **The Proposed decoding algorithm**

Inputs: Image that contains a hidden message that needs to be decoded,key.

Output: This output file will either be an image or a hidden textmessage that was encodedInto the original image.

Begin:

Obtain the stego file with the hidden data to processand break down to pixels and obtain pixel values

S: Stego file

S1 to n =pixel values

Recover Header Set to determine type of message

If the Header starts with 't' it is a text file.

If the Header does not start with 't'then the message is an image.

Now using the header value we know the type ofmessage and the bits that are to be obtained.

O: Obtained bits

Now perform the XOR operation on the bitsobtained using the Stego key.

K: key

P= O ⊕ K

Thus the obtained data is used to reconstruct thedata which is hidden message.

I=F-1{S, K}

F-1 is inverse function

3.Analysis:

The algorithm is tested using PSNR (Peak Signal to Noise Ratio). PSNR is used to test the quality of the stegoimages. The higher the value of PSNR the better is theStego image quality .

PSNR is obtained as following:

Cover file:C of size M×M

Stego file: S of size N×N

Cover and stego images with pixel values (p, q) from 0 to
M-1 and 0 to N-1.

Calculate the MSE (Mean Square Error) between cover
file and the stego file.

$$MSE = 1/MN \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} (C(p,q) - S(p,q))^2$$

$PSNR$ = 10. log10$MAX2/MSE$

MAX is the maximum pixel value of the images

If the stego image obtained from the process has largePSNR value then the image has higher quality. Here weconsider the PSNR value of stego image with hidden textand hidden image withinthe cover image. The values are as shown in table

Cover data	Size of cover	Message Hidden	Size of message Hidden	SNR	PSNR
Animal.jpg	800Kb	Text	8kb	80.41	92.14
		Image	10kb	46.71	91.15
Animal.bmp	50Kb	Text	8kb	81.47	90.02

		Image	10kb	48.15	95.83
Animal.jpg (grayscale)	41kb	Text	8kb	82.60	95.14
		Image	10kb	40.83	92.51

The figures represent the cover images and the stegoimages with the hidden data i.e., image and text.

Cover Image without Hidden Message

Image to be hidden in the cover Image

Stego Image with hidden data

The figure represents stego data with hidden image in it.There is no difference in between the images.

Cover Image without data

Cover Image with Hidden data (text)

Conclusion

The results show that the algorithm proposed hereis effective to bring an improvement in PSNR value.Altering the weight of cover data and message data seem toimprove the PSNR value. The proposed approach is testedon various data and provided better quality insteganography data.The proposed algorithm is also tested with text file and Image file as the hidden data and proved toprovide betterresults .The algorithm can be used on different types of the cover data.

REFERENCES

[1]. Hemalatha S1, U Dinesh Acharya2, Renuka A3, Priya R. Kamath"A secure and high capacity image steganography technique"Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013

[2]. Atallah M. Al-Shatnawi"A New Method in Image Steganography withImproved

ImageQuality" Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 - 3915

[3]. Ge Huayonga,b, Huang Mingshenga, Wang Qiana "Steganography and Steganalysis Based on Digital Image2011" 4th International Congress on Image and Signal Processing

[4]. Weiqi Luo, *Member, IEEE*, Fangjun Huang, *Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE* "Edge Adaptive Image Steganography Based on LSBMatching Revisited"IEEE transaction on information forensics and security, Vol. 5, No. 2, June 2010

[5]. Da-Chun Wu a, Wen-Hsiang Tsai b "Asteganographic method for imagesby pixel-value differencing"Pattern Recognition Letters 24 (2003) 1613–1626