DIGITAL IMAGE STEGANOGRAPHY SURVEY AND ANALYSIS OF CURRENT METHODS

Sakshi Jindal
Dept. of ECE
Giani Zail Singh Campus College of Engineering and Technology
Bathinda, India

Navdeep Kaur (Astt.Prof)
Dept. of ECE
Giani Zail Singh Campus College of Engineering and Technolgy
Bathinda,India

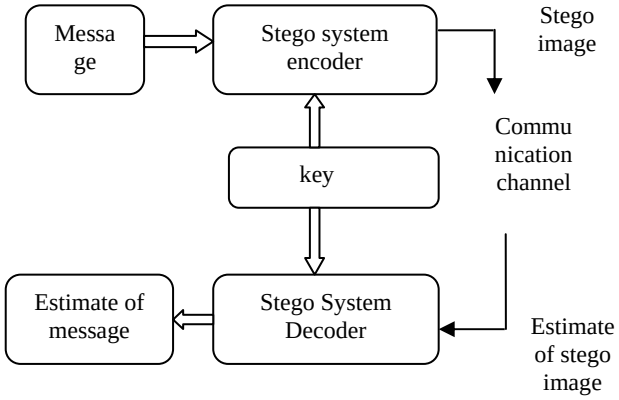
Abstract— Steganography is a technique for concealing the information such as data, file, image, text or message into another medium. The increase in number of internet users and communication through public networks has led to tremendous growth in use of Steganography. The two important ways in which information can be hidden are spatial and transform domain techniques. The latter techniques are used mainly for protection against security attacks. The proposed technique find the effective place for embedding the image with optimization of noise ratio.

***Key*words-**Image Steganography, Spatial and Frequency domains, Survey of different techniques in both domains.

I. INTRODUCTION

Steganography aims to hide information in such a way so that information may only reach its intended destination. It can be performed using any kind of carrier media such as image, text, audio, video etc.[1]The methods like cryptography and watermarking are practiced since times alongwith steganography for security purposes. Images are most widely used for steganographic purpose as it consists of more redundant information and can be easily sent through the communication channel [3] as compared to other media and the variation in luminance of coloured vectors at higher frequency ends of the visual spectrum cannot be detected by the human visual system.[5] The person who is directly not involved with the secret material will usually find it as ordinary picture, letter or data.

Steganography is not new. For example it has been in practice since 500~400BC and it is known that messages that were directly carved on tablets were coated with wax, later causing the message to be undetectable beneath the wax surface. Messages were painted on shaved head of slaves and when hair was fully grown, slaves were sent away to deliver the message.[3]Alongwith traditional media steganography is very popular in digital media. Due to the properties like large capacity, undetectability and robustness it differs from cryptography and watermarking.[11]A steganographic system mainly consists of cover medium, secret message ,algorithm for hiding and a communication channel.[3]



A STEGANOGRAPHIC SYSTEM

TABLE I: Comparision of the three techniques

Criteria	Steganography	Cryptography	Encryption
Carrier	Any media	Mostly image and audio	Mostly text
Secret data	Payload	Watermark	Text
Objective	Secret communication	Copyright	Data protection
Result	Stego file	Watermarked file	Cipher text
Attack method	Steganalysis	Data processing	Cryptanalysis
Visibility	Invisible	Mostly visible	Visible
Fail condition	Detection	Removal	Decipher

Steganography can be classified as:

- Text Steganography
- Video Steganography
- Audio Steganography
- Image Steganography

II. IMAGE STEGANOGRAPHIC DOMAINS

The two transform domains include Spatial and Frequency domains. Spatial domain embedding is based on physical location of pixels in an image. Here the LSB's if the cover medium are replaced by secret bits. It is a simple method for data embedding but cannot withstand or resist attacks like transforms or compression but their payload is high. Conversely in transform domain method, the medium is manipulated indirectly and the image is transformed into its frequency domain.
Types of spatial domain methods:

A.LSB encoding

In LSB encoding technique , the embedding is done in those bits which carry least weight so that value of the original pixel does not change. This encoding technique hides secret message into the least significant bits of the cover image without introducing any distortions which may be percepted by the human eyes.[4] Because of this various methods revolving around LSB have been developed.

B. LSB replacement

This method employs only the LSB plane of the cover image where it is overwritten with the secret bit stream according to the pseudo random number generator [1]. This introduced some asymmetry so it became easy to detect or crack steganography.

C. LSB matching

LSB matching is another method which employs a minor modification to LSB replacement technique. If the secret bit does not match the LSB of the cover image, then +1 or -1 is randomly added to the corresponding pixel value[1]This could avoid the asymmetry artifacts introduced by LSB replacement.

D.LSB matching revisited

This method uses a pair of pixels as an embedding unit, in which the least significant bits of the first pixels carries one bit of secret message and the relationship of the two pixel values carries another bit of secret message [1].By this method the modification rate of pixels can decrease apparently meaning fewer changes to the cover image at the same payload compared to LSB replacement and LSBM.

E. Pixel Value Differencing Method

This method was developed to increase the embedding capacity. It divides the cover image into many non-overlapping units with the two consecutive pixels. The gray scale image is used as a cover image with long bit stream as secret data. The difference value di is calculated by subtracting the two consecutive pixels pi from pi+1. The set of all difference values may range from -255 to 255. Therefore, di ranges from 0 to 255. [9]The blocks with small difference value locates in smooth area where block with large difference values are the sharp edged area. According to the properties of human vision, eyes can tolerate more changes in sharp-edge area than smooth area. So, more data can be embedded into edge area than smooth areas.

F. Singular Value Decomposition Method

In SVD method the secret is embedded either in left singular vector, right singular vector, singular values or it may be the combination of Spatial and Transform domain. The cover image is divided into many blocks for embedding the secret message. This method provides protection against cropping attack, compression attack, Gamma correction or Impulse noise attacks.

G. Histogram Shifting Method

Histograms are used for graphical representation of image and it represents the density at a particular pixel. It plots the pixel for each part of the image. A histogram is useful in identifying pixel distribution, density of colors and tonal distribution. A Histogram shifting is the technique which is used to modify or to extract a certain group of pixels from an image. In histogram the highest value is called maxima and the lowest value is called minima. [8]There are many algorithms which support histogram functionality in order to change the image. The number of the pixels constituting the peak in the histogram of a cover image is equal to the hiding capacity of the system as a single peak in a cover image is used. Several histogram shifting techniques have been developed by dividing the cover image into blocks to generate a respective peak for each block which provides more hiding capacity into the multiple blocks.
Types of transform domain methods:

A. Discrete Fourier Transform Method

This method converts time and space frequency components into frequency domain .This method seperates components into sine and cosine values. It includes only particular set of frequencies or samples that may be sufficient to describe the original image instead of including all the frequencies.[8] The hidden message bits are inserted in real part of frequency domain excluding first pixel. After embedding IDFT is performed frequency domain converted into spatial domain The Discrete Fourier Transform of spatial value f(x,y) for an image of size M × N is defined in equation for frequency domain transformation;

$$f(u,v)=1/\sqrt{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)e^{-12v\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

B. Discrete Cosine Transform Method

It is like the Fourier Transform Technique as it converts an image from its spatial domain into frequency domain. In this technique, for every color constituent, the JPEG format of image makes use of cosine transform to convert consecutive pixel blocks of size 8 x 8 into a count of 64 cosine coefficients each.[14] It separates the image into spectral sub-bands with respect to visual quality of the image, i.e. low, middle and high frequency component. Here FL and FH is used to denote the lowest frequency components and higher frequency components respectively. FM is used as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.

A. Discrete Wavelet Transform Method

Wavelet is simply a small wave which has its energy concentrated in time to provide a tool for the analysis of transient, non-stationary or time varying phenomena. A signal can be better understood if it is expressed as a linear decomposition of sums of products of coefficient and functions. In wavelet transform, the original signal (1-D, 2-D,3-D) is transformed using predefined wavelets and the use of such transforms will mainly evolve the capacity and robustness of the information hiding system features[2].
1-D DWT segments a cover image further into two major components known as approximate component and detailed component. A 2-D DWT is used to segment a cover image into mainly four sub components: one approximate component (LL) and the other three includes the detailed components represented as (LH, HL, HH).

C. Integer Wavelet Transform Method

Integer wavelet transform maps an integer data set into another integer data set which is perfectly invertible and results in exactly the original data set. In DWT ,the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information, which may lead to the failure of the data hiding system.[6]To avoid problems of floating point precison of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which do not allow perfect reconstruction of the input image, and in this case there will no loss of information through forward and wavelet transform.[7] Due to the mentioned difference between IWT and DWT the LL sub band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL sub band is distorted.

III. ANALYSIS OF STEGANOGRAPHIC TECHNIQUES

S.NO	TITLE	YEAR	ADVANTAGE
1.	Edge Adaptive Image Steganography	2010	Enhanced security and improved image quality
2.	Modified high capacity steganography using wavelet transform	2010	Security and imperceptibility
3.	Wavelet based Non LSB Steganography	2011	High PSNR
4.	Steganography using LSB hiding method	2012	Efficient,robust to attacks,improved image quality
5.	Fast Matrix Embedding by Matrix Extending	2012	Higher embedding efficiency,faster embedding speed
6.	Blind Detection Resistant Steganography using texture complexity and PVD	2012	Resistant to attack method
7.	High Security Image Steganography with Modified Arnold's Cat Map	2012	Highly secure and high hiding capacity
8.	Hiding text messages in image by replacing only some particular bits	2013	Robust and useful in real world applications
9.	Steganography in spatial domain by embedding three bits in a pixel	2013	Large capacity and high PSNR
10.	Non embedding Steganography using average technique in transform domain	2013	High capacity and PSNR
11.	Secure digital image steganography using matrix rotation	2013	Good perceptual invisibility and highly secured
12.	IWT Steganography using OPA algorithm	2013	Preserved visual quality
13.	Arnold Transform based Stegangraphy	2013	Highly secured with good perceptual invisibility
14.	Adaptive Edge image steganography	2014	Resistant to steganalytic attacks,enhanced capacity

15.	Adaptive hiding capacity function using OPA	2014	High hiding rates and imperceptibility
16.	Adaptive Image Steganography based on denoising methods in IWT	2015	Improved capacity,high PSNR, certain robustness

IV CONCLUSION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which 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.

REFERENCES

[1]Weiqi Luo, Fangjun Huang, Jiwu Huang, (2010), "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security,vol.5,No.2,pp.201-214.

[2] Ali Al-Ataby, Fawzi Al-Naima,(2010), "A Modified High Capacity Image Steganography Technique based on Wavelet Transform", The International Arab Journal of Information Technology,vol.7,No.4,pp.358-364.

[3]Atallah M. Al-Shatnawi,(2012), "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences,vol.6,No.79,pp.3907-3915.

[4]Chao Wang, Weiming Zhang, Jiufen Liu, Nenghai Yu,(2012), "Fast Matrix Embedding by Matrix Extending", IEEE Transactions of Information Forensics and Security,vol.7,No.1,pp.346-350.

[5] N Sathisha ,Amarshree,K Suresh Babu, KB Raja KR Venugopal, LM Patnaik,(2013), "Non Embedding Stegaonography using Average Technique in Transform Domain",IEEE 9th International Colloquium on Signal Processing and its Applications ,vol.8,No.10.pp.1-6.

[6]S.Jayasudha,(2013), "Integer Wavelet Transform Based Steganographic Method Using OPA Algorithm",International Journal Of Engineering and Science,vol.2,No.4,pp.31-35.

[7]A.Antony Judice, Dhivya Shamini.P, Divya Sree.D.J, Lekshmi Sree.H.A.,(2014), "An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform", International Journal of Computer Science and Network Security,vol.14,No.7,pp.125-132.

[8]Amritpal Singh, Satinder Jeet Singh,(2014), "An Overview of Image Steganography Techniques", International Journal of Engineering and Computer Science,vol3,No.7,pp.7341-7345.

[9]Latika, Yogita Gulati,(2015), "A Review of Steganographic Research and Develpopment", Intenational Journal of Advanced Research in Computer Science and Software Engineering, vol.5,No.4,pp.871-874.

[10]Zaid AL-Omari, Ahmad T. Al-Taani,(2015), " A Survey On Digital Image Steganography",International Conference on Information Technology,pp.109-115

[11]G.Prabakaran, R.Bhavani, M.Kiruthika,(2015), "Adaptive Image Steganography based on Denoising Methods in IWT", Intenational Journal of Advanced Research in Computer Science and Software Engineering, vol.5.No.1,pp.567-574.

[12]Steganography, Wikipedia
http://en.wikipedia.org/wiki/Steganography

[13] Abbas Cheddad, Joan Condell, Kevin Curran,Paul MC Kevitt,(2010), "Digital Image Steganography:Survey and Analysis of Current Methods", Signal Processing,Elsevier, vol.90.No.4,pp.727-752.

[14] Amandeep Kaur,Rupinder Kaur, Navdeep Kumar,(2015), "A Review on Image Steganography Techniques", International Journal of Computer Applications, vol.123,No.4.pp.20-24