International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-8)

Research Article

August 2015

A Review of Different Approach to Reduce Distance Error between Cover and Stego Image

Navneet Choudhary, Ria Gandhi
CSE & PTU, Punjab,
India

Abstract—

In the past few years,anyone can observe the communicated data all around.So,due to the increasing need of security in an open environment like the internet, tenders for business deals etc,Steganography attempts to hide information in an image file and make communication undetectable and secure. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists.It hides data in an image file to increase robustness.Frequency domain is used to increase the robustness of steganography method.This method reduce the error difference between the cover image and the stego image and to improve PSNR(peak signal to noise ratio) i.e the quality of the image and the hiding capacity with low distortion will be improved using two algorithms i.e GA(Genetic algorithm) and IWT(integer wavelet transform). Integer wavelet transform avoids the floating point precision problems of the wavelet filter.The stegnographic methods used to hide information securely in an image file is LSB(Least Significant Bit),spatial domain embedding and transform domain embedding.

Keywords— Steganography, Least Significant Bit,Cover Object,Covert Data, Stego-Object.

I. INTRODUCTION

Steganography is the art of communication in a way which hides the existence of information of the communication.As in Cryptography, where the enemy is allowed to detect and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide information inside other secure information in a way that does not allow any unauthorized user to detect that there is a second message present".Steganography and Cryptography are both used to protect information from unauthorized users.Both Steganography and Cryptography are excellent technologies to accomplish but neither technology alone is perfect and both can be broken.For this reason the experts would suggest to add multiple layers of security to both technologies. Steganography is used in a huge amount of data formats in today's digital world. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav.Mainly these data formats are used because of the popularity of these data formats on the Internet and the use of the steganographic tools that use these data formats.All these formats are popular because it can remove the redundant or noisy data from them and replaced with a hidden information.Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is driven by the lack of strength in the cryptographic systems and the desire to have complete secrecy in an open-systems environment.Governments have created laws that either limit the strength of cryptosystems or removed them completely.This unfortunately leaves the majority of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all.Both technologies together i.e stegnography and cryptography can provide a very large amount of privacy for anyone connecting to and communicating over these systems.With the use of steganography,communication become more secure and undetectable.Many techniques are used to secure information. There are a number of steganographic techniques that can hide secret information in an image file.These schemes can be classified according to the format of the cover image or the method of hiding. There are two types of hiding methods; spatial domain embedding and transform domain embedding. The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. LSB is the most preferred technique that is used for data hiding because it is simple stegnographic technique to implement.It offers high hiding capacity, and provides a very easy way to control stego-image quality but it has low robustness to modifications made to the stego-image such as low pass filtering and compression and also low imperceptibility.

II. ALGORITHMS USING LSB IN GRAYSCALE IMAGES CAN BE FOUND IN

1.Steganography: Steganography is the art of writing hidden information in such a way thay that nobody except the sender and recipient, suspects the existence of the information.Steganography includes the concealment of information within laptop computer files.

2.Discrete wavelet transform: In numerical analysis and other useful analysis, a separate rippling rework (DWT) is an rippling rework that wavelets square measure discretely sampled.As compared with different rippling transforms, a key advantage is it's over Fourier transforms is temporal resolution.

3.Genetic algorithm: A genetic algorithm (GA) is a search heuristic that mimics the process of natural evolution. This heuristic is habitually wont to provide helpful solutions to improvements and search issues. Genetic algorithms belongs to the category of Evolutionary algorithms (EA), that generate solutions to optimization issues victimization techniques impressed by natural evolution, like inheritance, mutation, selection, and crossover.

4.Least significant bit: In computing, the least significant bit (LSB) is the bit position in an binary integer giving the units worth, which is finding whether the quantity is odd or maybe. The LSB is few times settled to as the right-most bit, attributable to the convention in positional notation of writing smaller digit more to the correct aspect. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.The other type of hiding method is the transform domain techniques which appeared to overcome the problem of robustness and imperceptibility found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT).Most researches are directed to the use of DWT since it is used in the new image compression format JPEG2000 and MPEG4.The secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients sub band unaltered.While,in an adaptive (varying) hiding capacity function is employed to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients. The advantages of transform domain techniques over spatial domain techniques secure to tolerate noises with high quality and some signal processing operations but on the other hand they are computationally complex and slower.

III. IMAGE STEGANOGRAPHIC TECHNIQUES

SPATIAL DOMAIN EMBEDDING

Spatial Domain:These techniques use the pixel gray levels and their color values directly for encoding the message bits.These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images.The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) replacement technique in which the least significant bit of the binary representation of the pixel gray levels is used to represent the message bit. This kind of embedding leads to an addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel.To overcome this problem, the decision of changing the least significant bit is randomized i.e. if the message bit does not match the pixel bit, then pixel bit is either increased or decreased by 1. This technique is called as LSB Matching. It can be observed that this kind of embedding adds a noise of 0:5p on average. To reduce the noise,use of a binary function of two cover pixels to embed the data bits. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information.Embedding reduces the noise shown in the cover signal. In a multiple base number system has been employed for embedding data bits.The variance value for a block of pixels is used to compute the number base to be used for embedding. A similar kind of algorithm based on human vision sensitivity has been proposed by the name of Pixel Value Differencing. This approach is based on adding more amounts of data bits in the high variance regions of the image for example near “the edges” by considering the difference values of two neighboring pixels. This approach has been improved by clubbing it with least significant bit embedding in it.The steganographic algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which makes more changes or adds higher additive noise.LSB replacement technique has been extended to multiple bit planes.It has been proved that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image.A new algorithm which uses a combination of Single Digit Sum Function and Matrix Encoding has been proposed.

Types of Spatial Domain Stegnography

There are many versions of spatial steganography,directly all can change some bits in the image pixel values in hiding data.Least significant bit (LSB)-based steganography is one of the easiest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions.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.

1. Transform Domain Embedding

These technique encode message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is used for robust watermarking. Similar techniques can also provide large capacity embedding for steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). By embeding in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing.

2. Discrete fourier transform

The discrete Fourier transform (DFT) converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids, ordered by their frequencies, that has those same sample values.To convert the sampled function from its original domain (often time or position along a line) to the frequency domain.

3. Discrete wavelet transform

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled.

5.Discrete cosine transformation technique (DCT)

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important in science and engineering,from lossycompression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations.

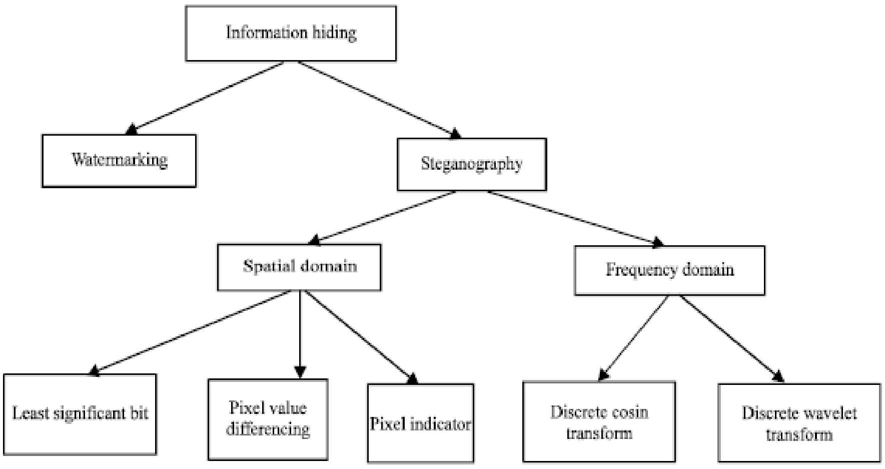

Fig 1. Stegnoghraphy Techniques

IV. LITERATURE REVIEW

Various paper are discussed in this section.An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images in which the work presents a replacement Steganography technique is to produce security to pictures that contain crucial knowledge or information.This approach depends on LSB technique.Image Steganography for Message Hiding Using Genetic Algorithm considers the need for higher security in Secrete Message transmission.It introduce Image Steganography for Message Hiding Using Genetic Algorithm.To make it more powerful and secure than, Genetic Algorithm is used.A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain. Steganographic algorithms can be characterized by a number of defining properties like Transparency, Capacity, and Robustness. High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform presents the application of wavelet transform and genetic algorithm (GA) in a steganography scheme.A GA based mapping function to embed data in discrete wavelet transform coefficients in 4 ×4 blocks on the cover image. The optimal pixel adjustment process (OPAP) is applied after embedding the message. We utilize the frequency domain to improve the robustness of steganography and implement GA and OPAP to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT presents image steganography technique that combines the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT). It embeds secret image in frequency domain of cover image with high matching quality. Also,it embed the secret image in different coefficients of cover image bands such as horizontal detail, vertical detail and diagonal detail and observe the effect of embedding on the performance of stego image in terms of Peak Signal to Noise Ratio (PSNR), Mean Structural Similarity Index Measure (SSIM), Histogram Error (HE).Stego image and extracted secret image could have high visual quality and they are perceptually similar to their original versions.This method shows high robustness against six different attacks and examined with wavelet based steganalysis algorithm.

V. CONCLUSION

This paper presented a novel ideas to increase the capacity and the imperceptibility of the image after embedding. GA is used in various techniques to obtain an optimal mapping function to reduce the error difference between the cover and the stego image and use the block mapping method to preserve local image properties and to reduce the algorithm complexity, and then applied the Optimal Pixel Adjustment Process to increase the hiding capacity of the algorithm in comparison to other systems. Future scope appears endless.

REFERENCES

[1] S Iftikhar, Z Anwar, M Kamran (2014),"A novel and robust fingerprinting technique for digital data based on Genetic Algorithm",IEEE,pp 173–177.

[2] P Chaturvedi, RK Bairwa (2014), "An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images",In:Int. J Recent Research and Review, Vol. VII, Issue 1,ISSN 2277 – 8322.

[3] Stuti Goel, Arun Rana,Manpreet Kaur (2013), " A Review of Comparison Techniques of Image Steganography",Global J Computer Science and Technology,Vol 13.

[4] S Atawneh, A Almomani, P Sumari (2013)," Steganography in digital images: Common approaches and tools",IETE ,Vol 30,pp 344-358.

[5] Hemalatha,S,Acharya,U.D,Renuka, A.Kamath,P.R (2012)," A secure image steganography technique using Integer Wavelet Transform",MIT (IEEE), pp 755 – 758.

[6] Raftari, N,Qazvin Azad Univ,Qazvin, Iran,Moghadam (2012)," Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT",A.M.E Dept. of Electr., Comput. & IT Eng.

[7] Saeed Masaebi,Amir Masoud Eftekhary Moghaddam (2012),"A New Approach For Image Hiding Based On Contourlet Transform",Int j electrical and computer engineering,Vol 2.

[8] Shiva Kumar,K.B,Khasim,T.Raja,K.B (2011),"Transform Technique for Robust Steganography", Computational Intelligence and Communication Networks (CICN),pp:310 – 314.

[9] Elham Ghasemi,Jamshid Shanbehzadeh,Nima Fassihi (2011),"High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform",Int multiconference engineers and computer scientist,vol-1.

[10] El Safy,R.O,Zayed,H.H (2009),"An adaptive steganographic technique based on integer wavelet transform",IEEE,pp:111 – 117.

[11] Nan-I Wu,Chung-Ming Wang ,Min-Shiang Hwang (2007)," Data Hiding: Current Status and Key Issues",Institute of Computer Science and National Chung Hsing University.

[12] Chi-Kwong Chan,L.M. Cheng (2004)," Hiding data in images by simple LSB substitution", Computer Engineering and Information Technolog,City University of Hong Kong, Vol 37,pp 469–474.