SAJET

South Asian Journal of Engineering and Technology Vol.2, No.18 (2016) 102–110

ISSN No: 2454-9614

Secure Data Transmisson using Image Processing: State-of-Art - A Review

S.Thenmozhi, Dr.M.Chandrasekaran*

[a)] *Department Of Electronics and communication Engineering, Anna University Chennai, Tamilnadu, India.*

*Corresponding Author: S.Thenmozhi
E-mail: thenmozhirayan@gmail.com

Received: 10/11/2015, Revised: 12/13/2015 and Accepted: 10/03/2016

Abstract

As an important component of multimedia information security, information hiding has received wide scope in recent years. It's been difficult to maintain the intellectual properties and as well as the original contents, so the latest techniques are developed such as Image Steganography. Steganography is a technique of hiding secret data in another media such that an outsider cannot distinguish the presence of the message within it. The other media can be image, audio, video etc. The usage of Steganography is to maintain secret communication between two individuals. Steganography is a technology where embedding data, compression,, spread spectrum, and cryptography technologies like encryption and decryption to merged together to enhance security levels over the internet applications. This paper analyses the various steganographic techniques in spatial domain and transform (frequency) domain. It aims to analyze and briefly present idea on which steganographic techniques are more suitable for which applications.

Keywords: Steganography; LSB; Transform domain; Spread spectrum;

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Steganography is the technique or specialty of concealing the secret data in another media such that an outsider cannot distinguish the presence of the message. The term steganography is deduced from the Greek word "Steganos" implying covered and "Grafia" signifying writing, thus characterized as secured written work. The media in which information is covered up can be anything like text, picture, sound and so forth and is known as the cover media and the information that must be transmitted furtively is called as the secret media. The cover media, which is changed in the wake of inserting the secret information in it, is called as the stego media. The principle necessity here is that the cover media and the stego media ought to be obviously comparable such that nobody can

make out the presence of secret information in it. There are various methods that are proposed in the literature to perform steganography. Each of the method proposed has its own advantage as well as limitation. Steganography can be categorised in various domains such as spatial domain and also in transform (frequency) domain. Spatial domain techniques, involves direct modifications on the pixel values whereas the transform domain techniques work on the transform domain coefficients that are obtained.

2.Terminologies

In any steganographic system there are some key terminologies used. Some of the basic terminologies used in this system are described below:

1. Secret media: This is the information that has to be transmitted securely to the receiver. It can be anything like text, image, audio, video etc.
2. Cover media: It is a media in which the secret data will be inserted into and then transmitted. This can also be anything like text, audio, video etc.
3. Stego media: This is the media that is obtained after the secret information has been embedded into cover object. Stego media is the one, which has the secret information contained in it and has to be visibly identical to that of cover media.
4. Embedding algorithm: This is the algorithm that is used to embed the secret data into the cover object. There are various algorithms present and has to be chosen according to our requirement.
5. Retrieval algorithm: This is the algorithm used to recover the embedded data from the stego media. It is exactly opposite to that of the embedding algorithm.
6. Payload: It is the capacity of information that can be hidden and transmitted.

3.Basic Steganography

The basic process involved in steganography is embedding and retrieval of data. For embedding, cover media along with the encryption keys is provided to the embedding algorithm used and it gives the stego media, which has secret information in it. The schematic of embedding process is as depicted in Figure1 below. After the data is transmitted, at the receiver side data is retrieved by using exactly the reverse process as of embedding. The keys used during embedding should be available at the receiver side for proper retrieval. The schematic of retrieval process is as depicted in Figure2 below.

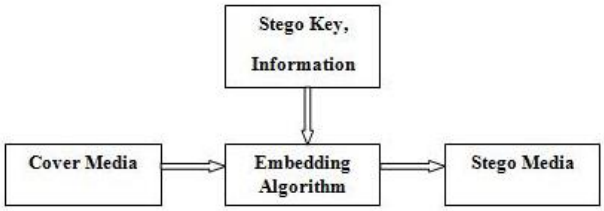

Fig 1 Embedding process

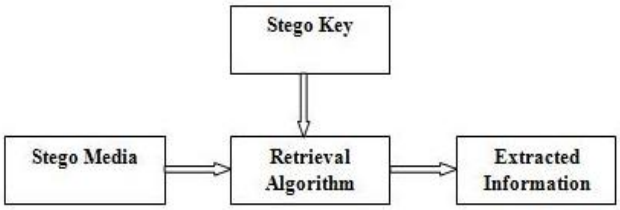

Fig 2 Retrieval process

4. Requirements of Steganographic System

A steganographic system is the one which performs the operations such as embedding and retrieving the secret information in steganography process. Any steganographic algorithm that is used should be having the following requirements:

1. Embedding capacity: The algorithm that is used should be able to provide a higher data embedding capacity in the given cover object.
2. Robustness: The algorithm should be robust against different attacks from any hacker.
3. Imperceptible: The stego image should be imperceptible which means that the presence of any secret message in it should not be made out readily.

Secure: The algorithm that is used should be highly secure and protect the secret data against any attacks.

5. Image steganographic techniques

Image steganography techniques can be categorized as below

1. Spatial Domain Methods: This method involves direct manipulation on the pixel value of the cover image to store the secret data. It means few pixel values of the cover image are modified during data hiding.
   There are various Spatial domain methods few of them are as follows: i)LSB embedding method ii)Colour based steganography iii) Mapping based method
   iv) Pixel value differencing technique
   v) Edges regions data embedding

vi) Random pixel value insertion method (RPE)

vii) Collage method steganography.

2. Spread Spectrum Technique: Spread spectrum technique forms the basis for spread spectrum steganography. The secret data to be embedded is spread in the entire frequency bandwidth. The signal to noise ratio in each frequency band must be very small that it seems difficult to locate the hidden data in it. There exist small amount of information which is enough to recover the hidden data if the some amount of data is removed from the bands. So the technique finds difficulty to extract data without the cover image destruction. It is widely used in military applications has it is very robust.

3. Statistical Technique: This method involves changing the various parameter of the cover image to embedded the data such as segmenting the cover into blocks and embedding each message bit it in a blocks.

4. Transform Domain Technique: These techniques are also known as frequency domain techniques as it involves the embedding of secret data in the frequency or transform of the cover image. These techniques are bit more complex method of hiding data in an images. Various transformations and algorithms are used to hide data few are i) Integer wavelet transform ii) Curve wavelet transform iii) Discrete Fourier transformation technique (DFT) iv) Curve wavelet transform iv) Discrete cosine transformation technique (DCT) v) Discrete Wavelet transformation technique (DWT) vi) Lossless or reversible method.

5. Distortion Techniques: In this method the secret data to be stored is embedded by the signal distortion. The encoder applies the modifications to the cover image and the decoder estimates the differences in the original and distorted cover image to recover the secret image and also to find the modifications in cover applied during encoding.

6. Masking and Filtering: These techniques hide or masks the secret data to be embedded over the original data or image by modifying the luminance of area to embedded data, here message embedding takes place within significant bits of image this method are susceptible to lossy images also unlike the LSB technique.

6. Literature review

This paper analyses the various methods on the steganography based on the spatial domain and transform domain techniques.

6.1 Spatial Domain Techniques

In Pallavi Das et al's**[1]** paper proposes a new image steganography method of by using single cover image to hide the multiple secret images using LSB substitution method. Based on the described method, in a primary colour matrix one of the secret image is embedded in random manner using LSB substitution method. The 24 bit cover image is used composed of RGB 8 bits each all three components are separated to from matrix later red pixel are separated into odd and even terms and form matrix. The multiple secret images used are XORed with each other to enhance the encryption level to provide more security. Later the bits of secret image are embedded in LSB

of red pixel even matrix and LSB+1 pixel of odd matrix other secret images are stored in green and blue pixel matrix thus new matrix forms stego image to transmit reverse process is used for extraction Results reveal that the proposed method has speeder computation level compared to other techniques, low error, and satisfactory visual quality of the stego image.

In Masoud Nosrati et al's **[2]** research paper Steganography in Image Segments using Genetic Algorithm is based on the before embedding hiding techniques it helps to find accurate places in carrier image to store the data with the less changes of bits. In order to achieve it segmentation is carried out to convert message strings and LSBs to the blocks for carrying the genetic algorithm. They key file was created later after locating the exact places to embedded data, the key file is used for message extraction purpose too. The proposed method analysis determines that it offers an efficient method in the field based on least changes in sample image and histogram confirms it.

In Tahir Ali et al's **[3]** method usage of all pixels of the cover image can be carried but message bit is stored in LSB of one of the three colour components, RGB based on the parity of three LSBs of R, G, B components of 24-bit colour image .Here the method uses the concept of parity check for recovering and hiding secret information or data Each 24 bit colour image has RGB components od 8-bits each initially it collects LSB of three components and form a group of three bits. Later the sequence obtained of these three bits may consist of even number of 1's or odd number of 1's. If the obtained three bits has even number of 1's then it is known as even parity else it is known as odd parity. The embedding method depends on the parity bits and message bits generated by the LSB of each colour components. Result state that method can hide huge volume of data in a single RGB image with relatively small changes in input image pixel value.

In Mamta Juneja et al's **[4]** proposed a new hybrid feature detector technique to improvise an approach for Information Security in RGB Colour Images for extracting smooth and edge areas of an image by integrating Canny edge detection and Enhanced Hough transform edge linking method, and for hiding messages two Component based LSB Substitution method for hiding encrypted data in edges areas and Adaptive LSB substitution technique for hiding messages in smooth areas. Enhanced security level for hidden messages and resistance to various attacks is provided along with it by using Advanced Encryption standard (AES) and Random Pixel Embedding Technique. Various steganalysis attacks like statistical and visual attacks are sustained successfully by proposed technique.

In Nadeem Akhtar et al's **[5]** proposed a Improved Module Based Substitution Steganography Method. This paper deals with the usage of modulus and shift operations along with lossless secret data compression logic to hide data it also demonstrates some improvising to reduce difference between the cover and stego images data to be hidden are converted from decimal to 8-binary bits, these 8-bits are divided later into 4-bits to get nibble value later on the steps for modulus method are carried out. The results indicate that maximum difference between pixel values of cover and stego image is 4 (m/2, m=8) which is improved compared to previous methods and also few improvements to reduce the image pixel value difference between cover and stego is determined based on cross correlation proof i.e., is maximum value 1.0 for stego-image which proof that stego image is almost similar with the

cover image. In this method user can hide image, text, image or audio file as secret data to embed in cover image file.

In Vijaya bhandari et.al's **[6]** outlined a LSB replacement technique for 24 bit colour image A, 24 bit colour image is considered in this technique initially the cover image is split into RGB components respectively such that more data i.e., is secret image message bits are hidden in the blue plane most rather than usage of red and green components is demonstrated in the technique because according to the human visual perception intensity of blue light or object is less compared to others. This technique is demonstrated using matlab implementation, later analysis and comparison with 8 bit colour image is carried out the result obtained state that PSNR value of 24 bit colour image is more and histogram comparison show that stego image has more similarity w.r.t to original cover-image.

In Anil kumar s et al's**[7]** demonstrated a new data hiding technique Hash-LSB derived from LSB insertion on images. Hash-LSB with RSA algorithm for data hiding and providing more security to data. The developed technique uses Hash function to develop separate unique pattern for embedding the data, firstly Hash function helps to find the exact positions of least significant bit of each RGB pixel's and later these message bits are embedded into RGB pixel's individually here the cover image is fragmented into parts and values obtained by hash function are used store the secret data at particular bit here the secret message is transformed into binary bits such that pixel value are in order 3,3,2 for RGB cover image and to provide extra layer of security the data hidden is encrypted before storing it in the cover image and embedded data in cover image produces a stego image.

6.2 Transform Domain Technique

They are various methods in transform domain technique few of them are illustrated below

1. Using Wavelet transforms: Wavelet transforms such as DWT &SWT[11], curvelet transform[12],Binary images steganography[14],Integer wavelet transform[22] are used to increase capacity, PSNR values etc.,

2. Using Neural networks: By using a ANN and Levenberg Marquardt algorithm [16], and HAAR Wavelets along with neural network[17] different algorithms are proposed to reduce computation complexities and increase the quality of image are illustrated in papers below

3. Using Cryptography : By making use of cryptography along with steganography it enhances the security to very High level i.e., is by using Blowfish and AES algorithm and DCT encryption [15], DWT and optimized message dispersing Method[18],DWT and Chaos theory based on Henon Map[19] Compress encrypt Stego(CES) methods are discussed below.

In R. S. Kamath et al's[11] proposed a fusion algorithm first by separating RGB colour planes of cover image. Both the b plane cover image and secret image coefficients are extracted either by Discrete Wavelet Transform (DWT) or Stationary Wavelet Transform (SWT) by using wavelet based fusion technique the extracted coefficients of cover and secret image are fused together. The stego image is obtained by taking IDWT/ISWT of fused image. Many combinations of SWT and DWT can be used for embedding process (SWT-DWT, DWT-DWT,

SWT –SWT and DWT-SWT).during the extraction process also the same combination of transforms are used. Better value of RMSE and PSNR are provided by DWT and SWT among all the possible combinations. The algorithm stated performs better in terms of visual quality. To measure the quality of extracted secret image many other Statistical parameters such has EN,MD, SC,NAE, AD, MD, UIQI are used and obtained results of all parameters are in the acceptable range, Thus secret image with good quality is extracted.

In Ahmed ElSayed et al's[12] paper demonstrates a low frequency Curvelet transform method for highly secure data hiding system in a cover image. The technique uses four secret keys (Two shuffling keys, Encryption key, and key for data hiding) and provide high security also using only low frequency component of Curvelet transform. In steganography usage of low frequency component of Curvelet transform has advantages then existing other techniques they are: 1) Reduced Computation time 2) Using only small number of coefficients the Curvelet transform are designed to handle curves discontinuities thus it doesn't affect the edges as the data hiding is carried out in the low frequency components which enhances quality of stego object. Results reveal that, there are no notable changes in the Curvelet transform Case between the stego and cover image while there exist notable differences Wavelet transform Case.

In Reyadh Naoum et al's[13] paper proposes neural network method Using a Enhanced Resilient back propagation and Fibonacci Linear Feedback Shift Register (FLFSR)", in order to embed secret image within RGB cover image, system includes embedding and extraction phases. Embedding phase includes three main stage they are selection of best cover image and processing stage, selection and processing of secret image and best embedding threshold selection stage respectively. By using SOM and ERBP algorithms best cover image is processed. Processing of secret image is carried out by splitting RGB colour layers applying DWT To get more secure system modified FLFSR in turns will be used to encrypt these streams, In the proposed combination of steganography and cryptography improved the security layers in compared with existing modern steganographic systems. So it is difficult to know the original hidden image since it is encrypted before embedded.

In Krupi Patel et.al's[14]paper demonstrated usage of Binary image steganography in the wavelet domain by combination of the steganography and cryptography to increase the security level, cryptography involves scrambling of the original data hence here the cover image is normalized, Normalization involves the alterations the range of pixel values later using DWT they are pre-processed, In meanwhile the secret image bits are array padded and scrambled and then conversion of 2D secret image into a 1D binary array form by considering value of single pixel each time and forming a new 1D array. For extracting the secret image from obtained stego image, they will first normalize both, obtained stego image, as also the cover image and will find the DWT of both the normalized images. Then the embedded coefficient is selected using pseudo random generator on the basis of random key k and alpha value is extracted by differencing the stego image from the cover image in wavelet domain. It helps to provide high transparency between the cover and stego-image, it is observed that PSNR is of much higher than the expected value. Hence this method is used to hide data effectively.

In S. Thenmozhi1 et al's [16] demonstrated a secure data transmission using artificial neural network the Levenberg Marquardt algorithm and feed forward neural network method are used for image processing and neural network is used for image coding. In the methodology the secret image and cover image is converted to binary 8 bits image, initially the starting two bits of secret image are replaced by last two bits generated by ANN initial position element in starting group of cover image in similar way embedding of all other bits is carried out and thus stego image is formed and transmitted to recover the message hidden at receiver side. The proposed method is implemented using Matlab and results states that method enhances the capacity level of secret data and no distortion in the cover image.

In S. Thenmozhi et al's[19] demonstrate a new method based on DWT, In the proposed method the secret image is initially scrambled using the chaos theory (Henon map)and the embedded in high coefficients obtained from DWT of the cover image and then the encryption and decryption process is carried out during the decryption process IDWT is used for the stego image, decryption process is just reverse of the encryption . The result analysis shows that method has high capacity and satisfactory security has the secret message cannot be known without the initial values of henon map, And even the correlation coefficient r is calculated in order to determine the distinguished factors for encrypted image the obtained values state that proposed algorithm is better than previous existing algorithms.

In V.Senthooran et al's[20] This paper presents a new method of data hiding based on the modified quantization table values and DCT coefficients. Based on the mathematical formula the Embedding strength of each coefficient are determined by comparing the appropriate quantization table value and DCT coefficients in order. Later by using LSB method the secrete bits are stored in frequency components of the quantized DCT coefficients. The proposed embedding method has three segments. Initially the segment divides the cover-image into non overlapping 8 x 8 pixels blocks. In second segment the DCT coefficient value in every block is compared with suitable quantization table entries. During the last segment message embedded based on the mathematical formula, occurs in quantized coefficients in every block this proposed method produces higher embedding capacity and acceptable image quality by applying changes in standard quantization table in middle part. By doubling quantization table with interpolation technique it can be further extend to 32x 32 or 16x 16 pixel blocks in future and stego image size is analysed in each case.

7. Conclusion and future work

In this review paper the various steganographic techniques in both spatial and transform domains are studied and critically analysed. The different proposed technique are based on the factors like increase in the stego image quality, low MSE, Higher PSNR rates and embedding capacity, and also various technique to provide the Robust Image to avoid various attacks and High secure image analysis method are illustrated.

Steganography has applications in various fields such as confidential transmission, video surveillance, military communication and medical applications, internet banking, mobile communication the insight into the steganographic methods will definitely help us to find new areas and to improve its applications in the already existing application areas also.

8. Acknowledgment

We would like to thank the authors who previously implemented various steganography algorithms which helped me to gain knowledge regarding the transform domain and contributed to the make a review survey on steganography techniques described in this paper.

References

[1] Pallavi Das, Satish Chandra Kushwaha, Madhupama Chakraborty" Data Hiding Using Randomization and Multiple Encrypted Secret Images" the IEEE ICCSP 2015 conference.

[2] Masoud Nosrati ,Ali Hanani,Ronak Karimi "Steganography in Image Segments using Genetic Algorithm" IEEE2015 Fifth International Conference on Advanced Computing & Communication Technologies.

[3] Tahir Ali Amit Doegar **"**A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015

[4] Mamta Juneja and Parvinder Singh Sandhu (2014) "Improved LSB based Steganography Techniques for Colour Images in Spatial Domain" International Journal of Network Security, Vol.16, No.6, PP.452-462, Nov. 2014

[5] Nadeem Akhtar, Ambreen Bano, Faraz Islam "An Improved Module Based Substitution Steganography Method" IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies

[6] Deepesh Rawat, Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Colour Image", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013

[7] Anil Kumar , Rohini Sharma " A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013

[11] Aarti Dalvi, R. S. Kamathe "Color Image Steganography by Using Dual Wavelet Transform (DWT, SWT)"International Journal of Scientific Engineering and Research (IJSER) Volume 3 Issue 7, July 2015

[12] Ahmed ElSayed, Abdelrahman Elleithy, Prasanthi Thunga1 and Zhengping Wu "Highly Secure Image Steganography Algorithm using Curvelet Transform and DCT Encryption" Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island

[13] Reyadh Naoum, Ahmed Shihab, Sadeq AlHamouz " Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation" IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015

[14] Krupi Patel,Dr. Leena Ragha" Binary Image Steganography in Wavelet Domain"IEEE2015 International Conference on Industrial Instrumentation and Control (ICIC)College of Engineering Pune, India. May 28-30, 2015

[15] Janki Gajjar. "Image Steganography Based on Transform Domain, Blowfish and AES for second level security" An international journal of advanced computer technology, 4 (6), June-2015 (Volume-IV, Issue-VI)

[16] S. Thenmozhi1, Dr.M.Chandrasekaran "Secure Transmission Of Data Using ANN Based Steganography" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.20 (2015)

[19] S. Thenmozhi,M. Chandrasekaran "A Novel Technique for Image Steganography Using Nonlinear Chaotic Map" IEEE Intelligent Systems and Control (ISCO), 2013 7th International Conference on 4-5 Jan. 2013

[20] V.Senthooran,L.Ranathunga" DCT Coefficient Dependent Quantization Table Modification Steganographic Algorithm" IEEE network soft-computing(ICNSC) 2014 international conference 19-20 Aug. 2014