A Secure Technique for hiding data under the Fingerprint Images using Modified Haar Wavelet Based Transformation

Heena, Jagpreet Kaur

Abstract-- Steganography refers to the hiding of secret messages in communications over a public channel so that an eavesdropper (who listens to the communications) cannot even tell that a secret message is being sent. Early works has been done on single file media. Which is sometime easy to analyze and find out the secret message . In the current work we are going to propose the multiple fingerprint images to store the secret message. We are also going to choose the modified haar wavelet transformation technique to insert the data. Image sequence is connected as random manner and every image has a tag for another image In this work we are inserting the data in fingerprint image for security and reliability purpose. As in this method the message is embedded in the picture in a random manner depending on the free spaces in the picture and also the message is scrambled with image while embedding to make the retrieval of the message by an unknown user tough.

Keywords: Fingerprints, Eavesdropper, MFHWT, Embedding

I. INTRODUCTION

Steganography is a very old method of sending the messages in secret. This method of message cloaking prevails the time of the ancient Greeks. The historian Herodotus wrote about an agent that how he wrote a message of on the wood part of a wax tablet. Since messages were normally seen in the wax and not the wood, the tablet appeared blank to a common observer [6]. There is also a story of a messenger during the Persian Wars who shaved his head and had a message tattooed on his head. He waited until his hair grew back to make his journey. When he reached at his destination, he shaved his head to reveal the message. During World War II secrete agents on both sides used "invisible inks". These inks were fluids like milk, fruit juice, or urine that would darken when it heated. They also sent messages with very small punctures on a document that formed a message when combine.People often confuse steganography with cryptography, and while in many cases they solve the same purpose which is to prevent the data from unauthorized d person. Even they are similar processes which first encrypting a message then using a stego-tool for hide it which is more effective in hiding a secret message than either method by itself. According to Dictionary.com:

Manuscript received on March, 2013.

Heena is from Muktsar, She has done her BCA and Msc (IT) from Punjab Technical University, Now persuing M.Tech (CSE) from Lovely Professional Universty. Her research area is Digital Image Processing.

Jagpreet Kaur, is from Batala. She has done her B.tech (IT) and M.Tech(IT) from Lovely Professional University, Her research area is Adhoc Networking.

Steganography is "Hiding a secret message within a larger one in such a way that others can not detect the presence or contents of the hidden message". But on the other hand, Cryptography is "The process or skill of communicating, or deciphering the secret writing or ciphers." Now can be used to send the hidden messages in image, audio and even text files [4] .

A. The basics of embedding

Three basic aspects in information-hiding systems are: **security**, **capacity**, and **robustness**. Security refers to an inability of eavesdropper to detect hidden information. Capacity is the amount of information that can be hidden in the cover medium. And Robustness is the amount of modification to the stego medium can bear before an adversary can destroy hidden information. Information hiding can be relates to both watermarking and steganography. Following Figure shows a simple representation of the general embedding and decoding process of steganography. In this a secret image embedded inside a cover image which produces the Stego Image.

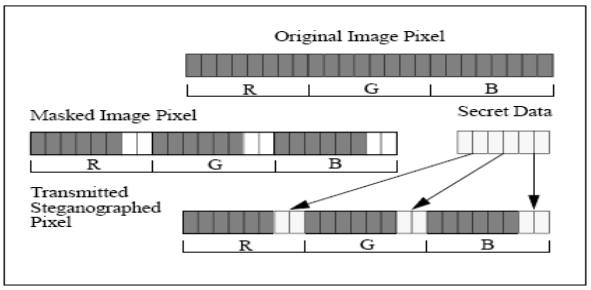

Figure 1 : Embedding Data in RGB Pixel

B. Process of Encoding and Decoding Data

The first step in encoding and decoding information is to pass both the secret Image and the cover Image into the encoder. In the encoder, one or more protocols will be used to embed the secret image into the cover image. The type of protocol will depend on information you are trying to embed and what you are embedding it in.

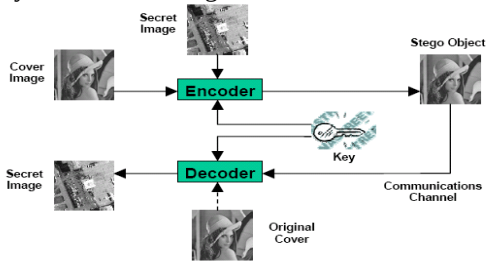

Figure 2:- General process of encoding & decoding

A key is also needed in the embedding process. This can be a public key or private key so you can encode the secret message with your private key and the recipient can decode it using your public key. Embedding the information in this way, you can reduce the chance of a third party [1].

In general the embedding process inserts a sign, S, in an object, O. A key, K, mostly produced by a random number generator is used in the embedding process and the resulting signed object, O' is generated by the mapping: O x K x S → O'.

When Object is passed through the encoder, then it will produce a stego object, that is the original cover object which contains the secret information embedded in it. This object should look almost identical to the cover object otherwise a third party attacker can detect the embedded information. After producing the stego object, then it will be sent via some communications channel, like Email, to the intended recipient for decoding. The recipient must decode the stego object in order so he can view the secret information. The decoding process is just the reverse of the encoding process.

In the decoding process, the stego object is fed into the system. The public key or private key that can decode the original key that is used for the encoding process is also needed so that the secret information can be decoded. Depending on the encoding technique, sometimes the original cover object is also needed for the decoding process. Otherwise, there may or may no way of extracting the secret information from the stego object. After completion of decoding process, the secret information embedded in the stego object can be extracted and viewed. The general decoding process again requires a key, K, this time along with a signed object, O'. Also required is either the sign, S, or the original object, O, and the result will be either the retrieved sign, S from the object or indication of the likelihood of S being present in O'.

Image Steganography has attracted extensive research as well as popular usability in recent years. This is due to the fact that huge amounts of data can be hidden without perceptible impact to the carriers because of the popularity of electronic images that are widely available.so we describe steganography techniques and tools that uses image files in more details [4].

II. PROPOSED TECHNIQUE

1) Check the Capacity of Image to store the data.
2) Hiding the data in FingerPrint Image with DWT using MFHWT.

In the current algorithm we are first tagging the images. Before proceeding to tag the images we have to choose the number of images .The number of images depends on the capacity of text

Let I be the current image and it stores M characters and Size of text is N . Number of images will be K =N/M.Thus set of images will be I = $\{I_1, I_2 I_3 \ldots . I_K\}$

A. *Data Insertion*

Next step is to tag the images to do this we will choose RGB of B channel of each image. We randomize the number 2 to K and get the series as random sequence. Then choose the first image I1 that will hold the tag of next image.Perfom the same step for next tagged image and repeat same till Kth images are tagged. Now applying DWT with MFHWT for each image and insert the data inside.

B. *Data Extraction*

Choose I_1 image and applying DWT with modified Haar wavelet transformation extract Data. Find the reference of next image from the Blue channel component. Repeat the process till Kth image Process in Modified Fast Haar Wavelet Transform[5]. In MFHWT, first average subsignal (a' =a1,a2, a3… $a_{n/2}$), at one level for a signal of length N i.e. f =(f1, f2,f3,f4…fn) is

$$a_m = \frac{f_{4m-3} + f_{4m-2} + f_{4m-1} + f_{4m}}{4}, \; m = 1,2,3,\ldots,N/4,$$

and first detail sub-signal(d'= $d_1,d_2,d_3 \ldots d_n$), at the same level is given as :

$$d_m = \begin{cases} \dfrac{(f_{4m-3} + f_{4m-2}) - (f_{4m-1} + f_{4m})}{4}, & m = 1,2,3,\ldots,N/4, \\ 0, & m = N/2,\ldots,N. \end{cases}$$

C. *Algorithm Steps*

(I) Input the Image I.
(II) Input the text that we want to insert in the Image.
(III) Compute the volume of text data and estimates a ratio of data that makes Segment that is able to insert into a single FingerPrint Image.
(IV) Makes the number of copies of Image that is equals to the number of Segments of text data.
(V) Before Inserting, Place cross sectional link in first pixel of Blue Channel.
(VI) Once cross sectional link has been established go for Steganography Technique.
(VII) Applied Modified Harr Wavelat Based Transposition for Steganography on each Segment of text data in different Cross-sectional tagged Image.

D. *Measuring Image quality*

In objective measures of image quality metrics, some statistical data are calculated to indicate the reconstructed quality of image. The image quality metrics provide some measure of closeness between two digital images by exploiting the differences in the statistical distribution of pixel values. The most commonly used error metrics for comparing compression are Mean Square Error (MSE) and Peak to Signal Noise Ratio (PSNR)

REFERENCES

[1] Mahmoud Hanan,Al-Dawood Aljoharah [2010] "Novel Technique for Steganography in fingerprints Image : Design and Implementation" Sixth International conference on Information Assurance and Security .
[2] Marvel L.M [1999] "Spread Spectrum Image Steganography",IEEE TRANSACTION ON IMAGE PROCESSING,vol. 8 ,Pp- 1075-1083
[3] Almohammad Adel, Ghine Gheorghita [2010] "Image Steganography and Chrominance Components" 10th IEEE International Conference on Computer and Information Technology, Pp – 996– 1001.
[4] Mathkour Hassan,Al-Sadoon Batool,Touir Ameur[2008]" A New Image Steganography Technique", IEEE,Pp-1-4
[5] Bhardwaj Anuj and Ali Rashid [2009]," Image Compression Using Modified Fast Haar Wavelet Transform", World Applied Sciences Journal 7, Pp- 647-653
[6] Herodotus, The Hisories, and chap. 5 - The fifth book entitled Terpsichore, 7 - The seventh book entitled Polymnia, J. M. Dent & Sons, Ltd, 1992

AUTHOR PROFILE

Heena is from Muktsar, She has done her BCA and Msc (IT) from Punjab Technical University, Now persuing M.Tech (CSE) from Lovely Professional Universty. Her research area is Digital Image Processing.

Jagpreet Kaur, is from Batala. She has done her B.tech (IT) and M.Tech(IT) from Lovely Professional University, Her research area is Adhoc Networking.