IOSR Journal of Computer Engineering (IOSR-JCE)
ISSN: 2278-0661, ISBN: 2278-8727, PP: 01-04
www.iosrjournals.org

A Review on Novel Image Steganography Techniques

Prof.S.V.Kamble[1] ,Prof. B.G.Warvante[2]

[1] *(Assistant Professor DKTE'S Textile & Engg.Institute,Ichalkaranji)*
[2] *(Assistant Professor TKIET Warananagar)*

Abstract *: Steganography is an important area of research in recent years involving a number of application. it is the science of embedding information into the cover images viz. text,video, and images. this article reviews stegnography based on digital image. Concept and priniciple of steganography are illustrated. Different embedding techniques that are LSB, Spatial domain ,DCT, Huffman encoding,DWT embedding method are generalized . then the performance specification of image steganography is disscussed . An image based steganography that combines LSB, DCT, and compression techniques on raw image to enhance the security of the payload.*

Keywords*-Least significant bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT)*

I. INTRODUCTION

Image steganography is the art of information hidden into cover image,. Is the process of hiding secret message within another message.The word steganography in greek means "Covered Writing". The information hiding process in a steganography with different techniques includes identifying a cover mediums redundants bits. The embedding process creates a stego medium by replacing the redundant bits with data from the hidden message.

During the process of hiding the information three factor must be considered that are ***capacity*** it includes amount of information that can be hidden in the cover medium. ***Security*** implayes to detect hidden information and ***Robustness*** to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [5]. Using steganography a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. Secrets can be hidden inside all sorts of cover information that is text,image,audio,video,etc. Most steganographic utilities hide information inside image, as it is relatively easy to implement images are mostly used in the process or of steganoraphy because it is hard to break [11]

In cryptography techniques scrambles a message so it can not be understood. Where as in steganography hides the message so it can not be seen. Watermarking and finger printing that seem hold promise for copyright protection. It becomes problematics when this technology is misused. Steganalysis is a techniques are used for detecting secret information hidden in a given image using steganographic tool. The art of steganalysis plays a major role in the selection of features or characteristics to test for hidden message[11].

This paper describes differnet technique used in image steganography,performance,analysis & comparision on each techniques.

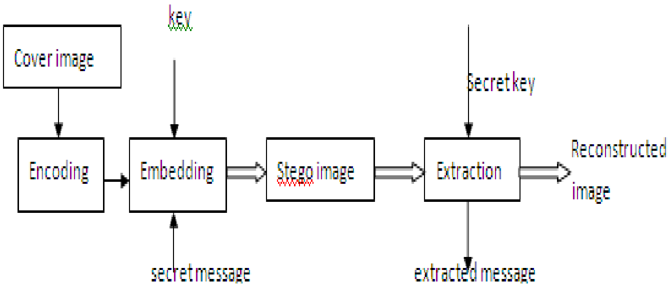

Figure 1.General block diagram for stegnography

II. Related Work

Neil F. Johnson,Sushil jajodia et. Al[1] , They discuss diffenet techniues of steganography and file compression, masking & filtering techniques.

Mamta janesa, parvinder sing sandhu et al[3] ,They discuss the design of a roboust image stegano graphy technique based on LSB insertion & RSA encryption technique.

Piyush marwaha, paresh marwaha[4], They propose the concept of multiple cryptography where the data will be encrypted into a cipher & the cipher will be hidden into a multimedia image file in encrypted formal,visual steganography algorithm will be used to hide the encrypted data.

Feng Pan, Jun Li et al[7] ,They present an image steganography method which utilize horizontal pixel & verticle pixel difference,in the horizontal direction they use high quality model function method for two pair of pixel embed message they use PVD method.

Pfitzmann & westfield[8],They proposed a particle algorithm for embedding JPEG image that would provide high steganographic capacity without sacrificing security.

Ming.chen,z.Ru.et al[9] , They have explain manystegnography tools which are capable of hiding data with an image. These tools can be classified into five category on their algoritham i.e are spatial domain based tools, transform domain based tools, document based tools,file structure based tools, video compress encoding and spread spectrum techniques.

Hassan mathkour, Btool Ai.sadoon et.[10] , They discussed several steganography techniques with an emphasis on image steganography they list a set of criteria to look into the strength & weaknesses of presented techniques.they also discussed & compared various steganography tools. Implemented a tool exemplifying its process.

Ge Huayong,Huang Mingsheng et. Al[11], They illustrate concept and priniciple of steganography and steganalysis, spatial domain and transform domain embedding method are generalized. Then the performance specification of image steganography is discussed.

Sueed sarreshtedari & shahrokh Ghaemmaghami[12], They proposed steganography algorithm works on the wavelet transform coefficients of the original image to embed the secret data.

III. MODELS

In these section describes some parameter and performance issues for different embedding techniques.

3.1 Least Significant Bit (LSB) Embedding

Steganography application that hide data in image generally use a variation of least significant bit (LSB) embedding. In this technique the data is hidden in the least significant bit of each byte in the image,the size of each pixel depends on the format of the image and normally ranges from 1 bytes to 3 bytes. An 8 bit pixel is capable of displaying 256 different colors.given two identicle images, if the least significant bits of pixels in one image are changed the two images still looks identical to the human eye [3].

24-Bit Image

To hide an image in the LSBs of each byte of a 24-bit image, we can store 3 bits in each pixel. A 1,024 * 768 image has the potential to hide a total of 2,359,296 bit(294,912) bytes of information. E.g the letter A can be hidden in three pixel. The original raster data for 3 pixel (9 bytes) may be

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

The binary value for A is 10000011. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

On average ,LSB requires that only half the bits in an image be changed.

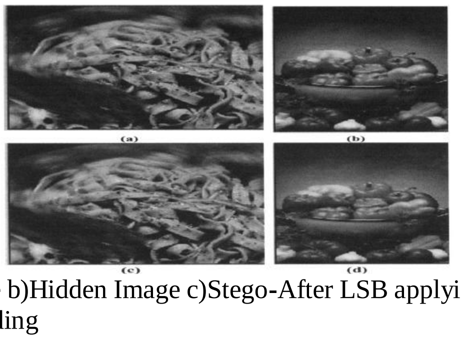

Fig.3 a)Cover Image b)Hidden Image c)Stego-After LSB applying d) Retrive Image

3.2 Image Spatial Domain Embedding

LSB based method are LSB replacement and LSB matching. In LSB replacement, the LSB bit of cover -image is replaced with secret bits. While in LSB matching the pixels are randomly incremented and decremented by secret bits. LSB based techniques pose a difficult challenges to a steganalyst in the passive warden model as it is difficult to differentiate cover image from stego-image.

In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs. This method although simpler, has a larger impact compared to the other methods. A practical example of embedding in the 1st LSB and up to the 4th LSB is illustrated in fig B. It can be seen that embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as „„non-natural□□.

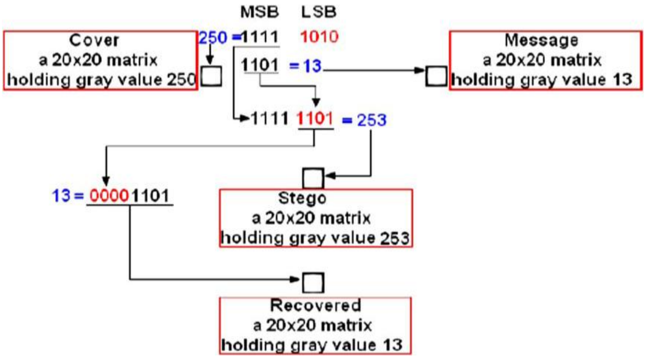

Fig. B Steganography in spatial domain.

3.3 Transform Domain Embedding

DCT domain embedding techniques is the most popular one, mostly because of the fact that DCT based image format are widely available in public domain as well as the common output format of digital camera.

JPEG image format for color components a descrete cosine transform (DCT) to transform successive 8 * 8 pixel block of the image into 64 DCT coefficients each. *The DCT coefficients F(u,v)* of an 8*8 block of pixel *f(x,y)* are given by

$$F(u,v)=\frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)*\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right],$$

Where u= horizontal spatial frequency, v=vertical spatial frequency.

$C(x)=1/\sqrt{2}$ when x=0 and C (x)=1 otherwise.

Embedding in DCT domain is simply done by altering the DCT coefficients. For example by changing the least significant of each coefficient. The modification of a single DCT coefficient affects all image pixels.

3.4 Huffman Encoding and Huffman Table

Before embedding the secret image into cover image, it is first encoded using Huffman coding. Huffman codes are optimal codes that map one symbol to one code word. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2 image is converted to a 1-D bits stream with length LH < M2 × N2.

Huffman encoding is used to serve the following three:

Lossless Compression =It increases the embedding capacity

Security by means of encoding =Huffman encoded bit stream cannot reveals anything. To extract the exact meaning, the Huffman table is required to decode. It provides one type of authentication, as any single bit change in the Huffman coded bit stream,

Huffman table is unable to decode[5].

3.5 Discrete Wavelet Transform

Wavelets are special functions which (in a form analogous to sins and cosines in Fourier analysis) are

used as basal functions for epresenting signals. The discrete wavelet transform
(DWT) we applied here is Haar-DWT, the simplest DWT. In Haar-DWT the low frequency wavelet
coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower
resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal
(HH)[5] .

IV. ALGORITHM

Problem definition: Given a cover image A and the image to be embedded (payload)B ;
the objective is,
1.To embed the payload in the cover image by replacing LSB bits of cover image by the image of the payload. The combined image is called stego-object(s).
2. To transform the stego-object from spatial domain to frequency domain using DCT.
3.To compress the frequency domain stego-object using quantization and runlength coding to generate a secure stegoobject.

Assumptions
1. Cover and payload objects are raw images of arbitrary size.
2. The LSBs of the cover image is utilized to embed the payload to minimize distortion in the cover image.
3. Stego-object is transmitted over the noiseless channel.Let A be the cover image, B be the hidden image, and S be the stego image. Let P be the number of bytes in cover image which are used to store one byte of the hidden image. Let I file be the input file and C file be the output file. The algorithm
Secured Steganography using LSB, DCT and Compression techniques

```
Input: Cover Image (A) and a Hidden Image (B) Output: Encoded Stego Image(S)
Repeat
1: Read the first byte of A and B into temporary
locations Ab and Bb respectively.
2: Run LSB()
3: Compute DCT()
4: Perform Quantization()
5: Apply Runlength Coding( on each block.)
 6: Copy the output as a Stego Image. Until (EOF)
```

V. Conclusion

The LSB techniques has been used to accommodate maximum payload. The entire payload is embedded into the cover image to obtain stego objec. The stego-object in the spatial domain is transformed into frequency domain by applying DCT. Stego- object compressed using runlength coading to derive a secure stego-object.The embedding process is hidden under the transformation (DWT) of cover image. These operation provide sufficient secrency. For privacy then it used huffman encoding.

Reference

[1]. N.F.Johnson &Sushil Jajodia,"Exploring Steganography: Seeing the Unseen",Survey PaperIEEE-1998.
[2]. K.B.Raja, C.R.Chowdary,"A Secure Image Steganography using LSB,DCT and compression Techniques on Raw Images", IEEE - 2005.
[3]. Mamta Juneja & Parvinder Singh Sandhu,"Designing of Roboust Image Steganography Technique Based on LSB Insertion and Encryption", 2009 ICARTCC
[4]. Piyush Marwaha & Paresh Marwaha,"Visual Cryptographic Steganography in Images", 2010 Second international conference on computing, communication and networking technologies.
[5]. Amitava Nag, Sushanta Biswas,"A Novel Techniques for image steganography based on DWT and Huffman Encoading", IJCSS, Vol(4): Issue (6)
[6]. Hniels Provos & Peter Honeyman,"Hide & Seek : An Introduction to Steganography" IEEE Computer Society Pub-2003.
[7]. Feng Pan, & Jun Li,"Image Steganography Method Based on PVD and Modules Function",IEEE-2011.
[8]. Pfitzmann & Wesrfeld.A,"High Capacity Despite Better Steganalysis," Kluwer Academic Publisher Boston Dodrecht London,2000.
[9]. Ming Chen,Z.Ru.N.Xin, "Analysis of Current Steganography Tools: Classification & Features", Information Security & Tele.Comm. Beijing Dec-2006.
[10]. Hassan mathkour,Batool Ai,sadoon, "A New Image Steganography Technology" ,IEEE-2008
[11]. Ge Huayong ,Huang ,"Steganography and Steganalysis Based on Digital Image", International conference & signal Processing-2011 IEEE
[12]. Saeed Sarreshtedari & Shahrokh ,"High Capacity Image Steganography in Wavelet Domain", IEEE CCNC 2010 Proceedings.