REVIEW OF HIGH CAPACITY IMAGE STEGANOGRAPHY USING FREQUENCY DOMAIN

Ravinder Goyat¹, Suman Goyat²

¹M. Tech Student, Department of Computer Science and Engineering, Indus Institute of Engineering and Technology.
²Ph.D Student, Sharda University, Greater Noida, U. P.

ABSTRACT: Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. While commonly thought of as messages hidden in pictures, it is not limited to just pictures, although this is one of the common uses, but messages can be embedded in any number of digital media types. It can even be embedded into sound files. Usually a steganographic message will appear to be something else: a picture, an article, a shopping list or some other message - this is referred to as the cover text or in the case of digital file - the carrier. This paper is a review of the steganography technologies, which have been used. In this article the different approach used are discussed.

KEYWORDS: RSA, DES, AES, HPC, DCT, LSB.


INTRODUCTION:
With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. However, message transmissions over the Internet still have to face all kinds of security problems. Therefore, how to protect secret messages during transmission becomes an essential issue for the Internet. Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include DES (Data Encryption Standard),[2] AES (Advanced Encryption Standard),[2] and RSA.[3] These methods scramble the secret message, so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper’s attention. Hence, a new scheme, called “Steganography”,[3] arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files), so that it cannot be observed. Steganography differs from cryptography in the sense that where cryptography focuses on concealing the contents of a message, steganography focuses on concealing the existence of a message.[3]

Steganographic study is a technique to achieve authentication of images and secret communication between two parties that are inserted in hiding not only the content of secret message/image, but also act as communicating it. To this aim, steganography algorithms embed the secret information into different types of natural cover data like sound and images. The resulting altered data is referred to as stego-data and it must be perceptually indistinguishable from its natural cover. So, steganography is the art of secret communication. Security is a big concern in modern day image trafficking across the network.

Security can be achieved by hiding data within the image. Data hiding,[1] in the image has become an important technique for image authentication and identification. Ownership verification,[8] and authentication is the major task for military people, research institute and scientist. Image authentication is a technique for inserting information into an image for identification and authentication. Image authentication technology is becoming increasingly important due to the proliferation of digital images on the WWW and in e-commerce. So information security and image authentication has become very important to protect digital image document from unauthorized access.[9,10] These are tools and techniques used to protect the originality and to ensure the authenticity of the image document. Data hiding refers to the nearly invisible,[3] embedding of information within a host data set as message, image and video. In steganographic,[4] applications, the hidden data may be a secret message or a secret hologram or a secret video whose mere presence within the host data set should be undetectable. The data hiding represents a useful alternative to the construction of a hypermedia document or image, which is very less convenient to manipulate.

The goal of steganography is to hide the message/image in the source image by some key techniques as the result observer has no knowledge of the existence of the message/image and it is unlike cryptography, where the goal is to secure communications from an eavesdropper by making the data non-understandable. In some situations, sending encrypted information will arouse suspicion while invisible information will not do so. To hide a message into an image without changing its visible properties,[2] the source image may be altered. This paper intends to offer a state of the art overview of the different algorithms used for image steganography to illustrate the security potential of steganography for business and personal use. After the overview it briefly reflects on the suitability of various image steganography techniques for various applications. This reflection is based on a set of criteria that we have identified for image steganography using frequency domain.
Peak Signal to Noise Ratio (PSNR): The measurement of the quality between the cover image f and stego-image g of sizes \( N \times N \) shown in fig is defined as:

\[
\text{PSNR} = 10 \times \log(255^2/MSE)
\]

where \( MSE = \frac{\sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x, y) - g(x, y))^2}{N^2} \)

Where \( f(x, y) \) and \( g(x, y) \) means the pixel value at the position \((x, y)\) in the cover-image and the corresponding stego-image respectively. The PSNR is expressed in dB’s. The larger PSNR indicates the higher the image quality, i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego image.

Capacity:
- The larger the cover message is (in data content terms — number of bits) relative to the hidden message, the easier it is to hide the latter.
- For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media.

Security:
- The objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (The original signal) due to the injection of the payload (The signal to covertly embed) are visually (And ideally, statistically) negligible. That is to say the changes are indistinguishable from the noise floor of the carrier.
- From an information theoretical point of view, this means that the channel must have more capacity than the ‘Surface’ signal requires, that is there must be redundancy.
- In digital image there is noise from the imaging element; and digital audio there is noise from recording techniques or amplification equipment, which should be avoidable.
- In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise and shot noise.
- This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data.[6]

OVERVIEW OF STEGANOGRAPHIC TECHNIQUES: A lot of Research has been carried out on Steganography, because it is important to know how much data can be concealed without image distortion. Their description is as follows:

Ken Cabeen and Peter Gent.[11] have discussed the mathematical equations of Discrete Cosine Transform (DCT) and its uses in image compression. Andrew B Watson.[7] has discussed Discrete Cosine Transform (DCT) technique for converting a signal into elementary frequency component. He developed simple function to compute DCT and show how its used for image compression. Jessica Fridrich et al.[12] have discussed a reliable and accurate method for detecting Least Significant Bit (LSB) non-sequential embedding in digital images. The secret message length is derived by inspecting the loss less capacity in the LSB and shifted LSB plane. Mohesen Ashourian, Jain RC and Yo-Sung Ho.[13] have proposed a data hiding scheme to embed a signature image in the host image. They selected a grey scale host image of 512×512 pixels and signature image of 256×256 pixels. They developed image data hiding scheme on dithered quantization and a modified baseline JPEG coding scheme. A test of system performance has been done by JPEG compression, addition of Gaussian noise and Gaussian and Median filtering of host image. Krenn JR.[14] has proposed a method to embed message in LSB of DC coefficients of cover image. He proposed a simple pseudo-code algorithm to hide a message inside a JPEG image. Ren-Junn Hwang et al.[16] have proposed data hiding based on JPEG technique.

They proposed a method of compressing the stego image by lossy compression method to reduce the image size. The receiver then extracts complete data correctly from lossy compressed image. Tseng HW and Chang CC.[7] have proposed a novel high capacity data hiding method based on JPEG. They proposed a method that employs a capacity table to estimate the number of bits that can be hidden in each DCT component, so that significant distortions in the Stego-image can be avoided. Youngran Park et al.[18] have proposed a new image steganography method to verify whether the secret information had been deleted, forged or changed by attackers. They proposed a method that hides the secret information into special domain of digital image. Neeta Deshpande et al.[19] have embedded data in least significant bits of cover image. They explained the LSB embedding technique and presented the evaluation results. Anees Jain and Indranil Sengupta.[19] have proposed a scheme, which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and new image and this is also resistant to JPEG compression. Chaumont M and Puech W.[13] have proposed a method to hide the colour information in a compressed grey-level image, allow free access to the compressed grey level image and give colour image access only if you own a secret key. KokSheik Wong, Xiaojun Qi and Kiyoshi Tanaka.[17] have proposed Mod4 steganography method in Discrete Cosine Transform (DCT) domain. Mod4 is capable of embedding information into both uncompressed and JPEG compressed image. Takayuki Ishida et al. [13] have discussed a modified QIM-JPEG2000 steganography, which improve the previous JPEG2000 steganography using Quantization Index Modulation (QIM).

Elham Ghiasi, Jamshid Shanbehzadeh, Nima Fassihi proposed method embeds the message in Discrete Wavelet Transform coefficients based on GA and OPAP algorithm and then applied on the obtained embedded image. This section describes this method and embedding and extracting algorithms in detail.[6]

Following Techniques are Discussed in This Paper:
- A Novel Technique for Image Authentication In Frequency Domain Using Discrete Fourier Transformation Technique (IADFFT).
- An Analysis of LSB and DCT based Steganography.
A novel technique for image steganography based on Block-DCT and Huffman Encoding.

Labelling method.

Hiding data using bit level manipulation.

Images using parity checker.

Quantized-frequency Secure Audio Steganography algorithm Integer Transform based Secure Audio Steganography algorithm.

Echo transform.

DESCRIPTION OF THESE IS AS FOLLOWS:

A Novel Technique for Image Authentication in Frequency Domain Using Discrete Fourier Transformation Technique (IAFDDFTT): The IAFDDFTT provides security by embedding authenticating message/image in frequency domain. Before embedding, the digital image is transformed from time domain to frequency domain representation using DFT technique as given in equation 1. In IAFDDFTT to generate transformed values using DFT a $2 \times 2$ sub-matrix has been taken from source image matrix as a window and authenticating message/image bits are embedded within the real part of the transformed data (Excluding the 1st pixel in each $2 \times 2$ sub-matrix) of the window. One MD-5 key has been generated from authenticating message/image using well known message digest generation method. The size and content of authenticating message/image and MD-5 key is embedded to the transformed source image. After embedding, inverse DFT as given in equation 2 has been performed on the embedded image to transform the embedded image from frequency to spatial domain. The reverse operation is performed at the receiving end and extracting bits of authenticating message/image and MD-5(R) key for authentication at destination. The schematic diagram for this method is shown as:

![Schematic diagram of IAFDDFTT](image)

Comparison of LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of DCT based steganography scheme is high as compared to LSB based steganography scheme for all types of images (Grayscale as well as Colour).\[13\] DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme. Even though the amount of secret data that can be hidden using this technique is very small as compared to LSB based steganography scheme still, DCT based steganography scheme is recommended because of the minimum distortion of image quality.\[14\]

A. LSB BASED STEGANOGRAPHY:
Algorithm to embed text message:

![Algorithm diagram](image)
Step 1: Read the cover image and text message to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image.

**Algorithm to retrieve text message:**
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

### B. DCT BASED STEGANOGRAPHY

**Algorithm to embed text message:**
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with bit of secret message.

**Algorithm to retrieve text message:**
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

**Block-DCT and Huffman Encoding:** Hiding the secret message/image in the special domain can easily be extracted by unauthorized user.[10] We proposed a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image.[7] The 2-D DCT convert the image blocks from spatial domain to frequency domain. The schematic/block diagram of the whole process is given in figure 5 and 6.

![Figure 2: Insertion of a Secret image (or message) into a Cover image.](image)

![Figure 3: Removal of Secret Image (or message).](image)
Advantages:
- Improvement in security and image quality.
- A good invisibility.
- Less distortion after embedding process.
- Expected to be practical.
- Provides three layers of security.

Disadvantages:
- Robustness is not achieved.
- Can be distorted by unintended users.

Labelling Method in Steganography: In this method tried to find binary value of each character of text message and then in the next stage tried to find dark places of grey image (black) by converting the original image to binary image for labelling each object of image by considering on 8 connectivity. Then these images have been converted to RGB image in order to find dark places. Because in this way each sequence of grey colour turns into RGB colour and dark level of grey image is found by this way; if the Gary image is very light the histogram must be changed manually to find just dark places. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of steganography. [14]

Advantages
- Applicable for unobtrusive communications.
- Easy to implement.
- More effective and efficient.
- Reduce manual work load.

Disadvantages
- Less secure.
- Require skilful and intelligent programmer.
- Need an enhanced technique to make use of palette and composition of the GIF image for better results.

Hiding Data Using Bit Level Manipulation: In this method if 5th, 6th and 7th bit are 0, 2, 4 or 6 of the decimal values of the message, then these bits are replaced by 0. Similarly if the 5th, 6th and 7th bits are 1, 3, 5 or 7, then these are replaced by 1. If these are not the cases then either add or subtract 1 from the decimal values to make them either 0, 2, 4, 6 or 1, 3, 5. [14]

The basic results obtained from this method:
I. The message bit will be inserted at the pseudo random location at first chance is 99.2%.
II. Chance when message is inserted, no change in pixel value is required is 50%.

Advantages
- Simple and easy to implement.
- If intruder changes the LSB, then there will be no change in hidden message.
- If LSB changes due to noise imperfections message will not be distorted.

Disadvantages
- Not a general method.
- Less adopted when more security is desired.

Images Using Parity Checker: In this method concept of even and odd parity is used. Even parity means that the pixel value contain even number of 1 and odd parity means pixel contain odd number of 1. The 0 is inserted, 0 at a pixel value if it has odd parity. If odd parity is not present over there, then make the odd parity by adding or subtracting 1 to the pixel value; similarly in the case of even parity.

RESULTS:
I. The message bit will be inserted at the pseudo random location at first chance is 98.82%.
II. Chance when message is inserted, no change in pixel value is required 50.19%.

Advantages:
- It provides greater chance for message insertion.
- Change in image required is less as compared to other methods.
- Steganalysis is difficult because stress is on whole pixel rather than specific bits is used.

Disadvantages:
- As steganalysis is difficult, the retrieval of message is difficult for the receiver.

STEGANOGRAPHY USING QUANTIZED FREQUENCY DOMAIN EMBEDDING: 'Quantized-frequency Secure Audio Steganography algorithm (QSAS)' It is based on classical unitary transforms and quantization in the transform domain and is an extension of the work on watermarking presented in. The differences are that our algorithm is developed for steganography, wherein higher embedding capacity is relatively more important than the robustness requirements of watermarking. We also present a simple capacity measure to select an audio with the best embedding capacity [3]. In the QSAS algorithm, we select the Fourier transform as we are dealing with audio signals and its properties in the frequency domain are well known.

Advantages
- Changes in the embedded audio section are inaudible.
- Lower embedding capability, but much better SNR values.
- Reversible, simple and efficient with acceptable SNR values.
- Least distortion after the embedding process.

Echo Hiding: In this method secret message is embedded into cover audio signal as an echo. Three parameter of the echo of the cover signal namely amplitude decay rate and offset from original signal are varied to represent encoded secret binary message. Binary coding is done for converting echo image of the cover media, thus it is referenced as frequency domain.

CONCLUSION: These are the various techniques, whose effects are discussed for their implementation in the security purposes. Although only some of the main image
steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages with different strong and weak points respectively; where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most types of attacks, but can hide only a very small amount of information. Least Significant Bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. The most widely used technique today is hiding of secret message into a digital image. This steganography technique exploits the weakness of Human Visual System (HVS). HVS cannot detect the variation of colour vector at higher frequency side of visual spectrum. A picture can be represented by a collection of colour pixel. The individual pixel can be represented by their optical characteristics like brightness, Chroma etc. Each of these characteristics can be digitally expressed in terms of 1 and 0.

REFERENCES:


