CHAOS BASED IMAGE STEGANOGRAPHY IN WAVELET DOMAIN

A Thesis

Submitted in partial fulfilment for the award

of

Degree of Master of Technology

in

Signal Processing and Digital Designing

by

SHALU

Under the guidance of

Dr. NIDHI GOEL

Assistant Professor

Department of Electronics and Communication Engineering

Department of Electronics and Communication Engineering

Delhi Technological University

New Delhi-110042

JULY 2013

CERTIFICATE

This is to certify that the project entitled **"Chaos based image steganography in wavelet domain"** is the bonafide work carried out by SHALU GARG, student of M.tech (Part time), Delhi Technological University, New Delhi, during the year2012, in partial fulfillment of the requirements for the award of the Degree of Master of Technology(Signal Processing And Digital Designing) and that the project has not formed the basis for the award previously of any degree, diploma, associateship, fellowship or any other similar title.

Date :

Dr. Nidhi Goel

Assistant Professor

Department of E&C Engineering

Delhi Technological University

Acknowledgement

I owe a great many thanks to a great many people who helped and supported me during the writing of this project report. I would like to extend my sincere thanks to assistant professor **Dr. Nidhi Goel,** the project guide for guiding and correcting various documents of mine with attention and care. She has taken pain to go through the thesis and make necessary correction as and when needed. I express my thanks to the Vice-chancellor, **Prof. P.B.Sharma** of **DTU**, **New Delhi**, for extending his support. My deep sense of gratitude to **Prof. Rajiv Kapoor (H.O.D)**, **Department Of Electronics And Communication** for his support and guidance. Thanks and appreciation to the helpful classmates, for their support. I would also thank my Institution and my faculty members without whom this thesis would have been a distant reality. I also extend my heartfelt thanks to my family and well-wishers.

Shalu Garg

14/Spd/2010

M.Tech (SPDD)

Delhi Technological University

CONTENT

Abstract **i**

List Of Figures **ii**

List Of Acronyms **iv**

Chapter 1 – Introduction …………………………………………………………..1

1.1 History ……………………………………………………………………….....4

Chapter 2 - Literature Review……………………………………………………7

2.1 Literature Survey………………………………………………………..................7

Chapter 3 - Steganography Model……….......…………………………………..13

3.1 Frame Work of Steganography Model……..…………………………………….....15

Chapter 4 - Overview of Steganography……………………………………17

4.1 Image Steganography…...………………………………………………………….18

4.1.1 Image Files....……………………………………………………………..18

4.1.2 Taxonamy of steganography techniques…….…………………………………19

Chapter 5 - Techniques of steganograph……….……………………….....21

5.1 Spatial Domain Technique……………………………………………………....21

5.2 Transform Domain Technique…....……………………………………………..21

5.2.1 Jpeg compression……………………………………………………………22

5.2.2 Jpeg Steganography…………………………………………………………23

5.2.3 Wavelet Transform Technique……………………………………………...23

5.3 Spread Spectrum Technique….….……………………………………….…...25

5.4 Statistical Method……….…..…………………………………………………..…27

5.5 Distortion Technique…..………………………………………………………28

5.6 File Embedding..……..……………………………………………………………..29

5.7 Pallete Embedding…..…..………………………………………………………..29

5.8 Image Generation Technique...…….……………………………………………….30

5.9 Image Element Modification Technique..……………………………………………..30

5.10 Adaptive Steganography………………………………………………………………31

Chapter 6 - Evaluation Of Different Technique…………………………….33

Chapter 7 - Proposed Method Of Steganography…..……………………..36

7.1 DWT(Discrete Wavelet Transform)……..……………………………………………36

7.2 Arnold Transform……………………………………………………………………..38

7.3 FRWT(Fractional Wavalet Transform)…...…………………………………………..39

7.4 Alpha Blending………………………...……………………………………………..39

7.5 Implemented Algorithm………………………………………………………………41

7.5.1 Embedding Algorithm……………….…………………………………………41

7.5.2 Extracting Algorithm……………...……………………………………………43

Chapter 8 - Experimental Results And Attack Analysis…………………..45

8.1 Subjective Evaluation…..……………………………………………………………45

8.2 Performance Analysis……….………………………………………………………..45

8.3 Objective Evaluation….……………………………………………………………47

8.4 Results.............……………………………………………………………………48

8.5 Attack Analysis………...……………………………………………………………..48

Chapter 9- Applications….………………………………………………………..51

9.1 Usage in Modern Printers…..…………………………………………………………51

9.2 Used by terrorist………………………………………………………………………….51

9.3 Alleged use by intelligence services…...…………………………………………...51

9.4 Confidential communication and secret data storing…..……………………………...51

9.5 Protection of data alteration…………………………..………………………………52

9.6 Access control system for digital content distribution…..……………………………53

9.7 Media Database systems…………………………...………………………………..54

Chapter 10- Conclusion………...………………………………………………56

References

ABSTRACT

In this study, we proposed a method of hiding the stego image in cover image by using a technique called fractional fourier transform works with wavelet coefficients. Application of steganography is internet/web security, can be used at a time of war for communicating secret message. To maintain higher security Arnold transform is performed on host image with key, key only known to a receiver/sender. For embedding, performed a fractional fourier transform of cover image and secret image. Then apply DWT on both images. Cover image and secret image will add by using a technique called alpha blending which can add foreground with background color and wavelet coefficients of both images. Stego image will be extracted by applying IDWT (Inverse Discrete Wavelet Transform). For extracting, cover image will subtracted from stego image by using alpha blending. Secret image will produced. By considering different aspects we have investigated the results of our scheme. This proposed method provides higher security, robustness against different attacks, good feasibility.

LIST Of FIGURES

3.1 Steganography Model

3.1.1 Framework of Steganography Model

7.1.1 Coefficients of DWT

7.1.2 Steganography based on DWT

7.5.2 Extracting code of modified secure steganography

8.1.1 Cover image

8.1.2 Secret image

8.1.3 Scrambled secret image

8.1.4 Fractional fourier transform Of cover image.

8.1.5 Fractional fourier Transform of scrambled secret Image.

8.1.6 Stego image Transform of of scrambled secret Image

8.1.7 Extracted scrambled secret Image (decombined image)

8.1.8 Fractional fourier transform of scrambled secret image

8.1.9 Recovered secret image

8.5.1 Contrast variation

8.5.2 Addition of Gaussian white noise with 0 mean and 0.01 variance

8.5.3 Histogram attack

8.5.4 Sharpening effect

LIST oF ACRONYMS

2-D	Two Dimensional
A/D	Analog to Digital
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DIAS	Digital Image Authentication System
DWT	Discrete Wavelet Transform
FFT	Fast fourier Transform
FRWT	Fractional Wavelet Transform
HH	High-High
HL	High-Low
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
JPEG	Joint Photography Expert Group
LH	Low-High
LL	Low-Low
LSB	Least Significant Bit
MATLAB	Matrix Laboratory
MSE	Mean Square Error

NC	Normalized Cross Corellation
PSNR	Peak Signal to Noise Ratio
RGB	Red Green Blue
SVD	Singular Value Decomposition
YCbCr	Luminance; Chroma:Blue; Chroma:Red

CHAPTER 1

INTRODUCTION

Steganography is an art of science of hiding the secret message in such a way that no one apart from the intended recepient, even knows the message will exist. Data hiding is a method of hiding secret messages into a cover media such that an unintended observer will not be aware of the existence of the hidden messages. In this project 8-bit or 24 bit gray scale selected as a cover image. Cover images with the secret messages embedded in them are called stego images. For this purpose we can use some other techniques also, like cryptography and water marking. Steganography and Watermarking are basically interchangeable terms, both are using for same purpose that is hiding the information, but work in different domain. Watermarking can be invisible and visible but steganography always be invisible. Due to many factors steganography is different from other technique is higher capacity, security, feasibility, robustness and undetectibility. Steganography can be classified into different categories. Two broadly classified categories are spatial domain and transform domain. Spatial domain has less complexity but less robustness against attacks. In spatial domain pixel intensities of image is altered. In transform domain digital media converted into frequency domain by using different transform wavelet transform, fractional fourier transform, fourier transform, wavelet tansform, cosine transform, counterlet transform . Transform domain has good robustness in comparison to spatial domain.

For data hiding methods, the image quality refers to the quality of stego images. The most commonly used steganographic method is LSB (least significant bit) which replaces the least significant bits of cover image with secret information that would be embedded. Generally speaking, a good steganographic technique should have good visual quality of stego image and sufficient capacity of hidden secret data. Although LSB maintains a good visual quality of stegoimage, it can hide a small information. Considering the drawback of LSB, some methods take in account of the visual identity that human eye are insensitive to edge, texture and contrast areas when embedding secret information such as BPCS (bit plane complexity segmentation), PVD (pixel value differencing). With these methods, more secret information is embedded in edged, highly contrast areas than in smooth areas. The capacity of embedded information is thereby greatly improved while the quality of visual perceptibility is maintained. Thus to maintain higher security Fractional fourier wavelet transform is used. In this fractionalfourier transform of host image and cover image will take then apply DWT coefficients on both images. With the help of alpha blending background and foreground color of both images will add. After apply IDWT host image will extract from stego image. The extracted image will have high visual quality and better robustness.

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data and it has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography ultimate objectives and the main factors that separate it from related techniques such as watermarking and cryptography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet based coding provides substantial improvements in picture quality at higher compression ratios. Over the past few years, a variety of powerful and sophisticated wavelet-based schemes for image compression have been developed and implemented. Further those Schemes are being designed to address the requirements of very different kinds of applications, e.g. internet, color facsimile, printing, scanning, digital photography, remote sensing, mobile applications, medical imagery, digital library, military application and e-commerce. Information hiding is an old and interesting technology and it has become the focus of research now. Steganography (image hiding) means to embed the secret image into another image. The main targets of image hiding are to hide the secret image and avoid unauthorized attackers using the secret. The secure communication is main purpose of steganography, in such a way that the stego image (modified cover image which contains secret message) should not deviate much from original cover image (image not containing any secret message) and the observer could not be able to distinguish any sense between them with respecting to remain the real message invisible for the observer. Generally, there are two approaches that can be used for image steganography. These two broad categories are the spatial domain and the transform domain based techniques. In spatial domain techniques, the methods which modify the least significant bits of pixels in the cover image are the simplest for hiding a secret image. Despite the simplicity of these methods is an advantage, they have low robustness to even simple attacks such as low pass filtering, transforms, compression, etc. Although, image hiding techniques in transform domain are more robust against simple attacks and have high ability to tolerate noises and some signal processing operations and take advantage of features in human visual system for image hiding, but on the other hand they are computationally complex and hence slower than spatial domain techniques and they can provide a limited capacity regarding the size of secret image. In image Steganography techniques, transform domain approach with either Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT) are used to transform both of the cover image and the secret image into a set of frequency domain coefficients. Information hiding is done by using the less significant frequency coefficients of the cover image to embed the significant frequency coefficients of the secret information. In continue, for producing the stego image, inverse transform is used to modify frequency coefficients. These methods have good visual quality from the point of invisibility and they have high robustness against different image processing operations.

Information hiding, steganography, and watermarking are three closely related fields that have a great deal of overlap and share many technical approaches. However, there are fundamental philosophical differences that affect the requirements, and thus the design, of a technical solution. Digital watermarking is mainly used in copyright protection, while steganography is a method of embedding the secret message into a camouflage media to ensure that unintended recipients will not be aware of the existence of the embedded secret data in cover media. Thus, whole system can be considered as secret communication. However, steganography is different from cryptography as it is a part of secret communication where its techniques may fail since a cipher text has meaningless form and thus easily arouses the curiosity of malicious attackers who are willing to consume the substantial amount of time and energy to recover or destroy data. Unlike cryptography, steganography conceals the fact that there is secret communication going on and still image may be represented as well suited camouflage media for embedding of secrete data. Even more, the advantage of cryptography techniques are executed on secret data before embedding into still image; to strengthen security level and also to suppress the energy compaction of secret data. Steganalysis on the other side is the science of detected hidden information. The main objective of steganalysis is to break steganography system and that condition is met if an algorithm can judge whether a given image contains a secret message

1.1 History

Johannes Trithemius (1462-1516) was a German Abbot is ostensibly a work describing methods to communicate with spirits. A very rough translation (with apologies to my Latin instructors) of this Latin title is: “Steganography: the art through which writing is hidden requiring recovery by the minds of men.” Published as a trilogy in Latin, the first two parts of his works are apparently some of the first books on cryptology describing methods to hide messages in writing. The third part of the trilogy is outwardly a book on occult astrology.

Throughout history, people have hidden information in different ways. The word 'steganography' was basically derived from the Greek words with the meaning “covered writing”. Soon after, researchers used it for thousands of years in various manners. During the 5th century BCE, the Greek tyrant Histiaeus was taken as a prisoner by King Darius in Susa. Histiaeus needed to send an abstruse message to his son-in-law, Aristagoras, who was in Miletus and in order to do this, Histiaeus shaved a slave’s head and tattooed the message on his scalp. As soon as the slave’s hair grew sufficiently to conceal the tattoo, he was sent to Miletus with the message. In ancient Greece, another method was to peal the wax off a wax-covered tablet, then write a message and to have the application of the wax again. The one in charge to receive the message would simply need to get rid of the wax from the tablet to see the message. Invisible ink was another popular form of steganography. Ancient Romans had their way in writing between the lines by using invisible ink, and by using substances such as fruit juice, urine, and milk. Using Invisible ink, though seems harmless, a letter might reflect a very different message written between the lines. Invisible ink was used as recently as World War II. In addition to invisible ink, the Germans used the Microdot technique during the Second World War. Information, particularly photographs, was made so small that they were very difficult to detect. In 1550, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user of such papers all what he needs is to write his secret message in such holes after placing the mask over a blank sheet of paper. This technique, steganography, is now highly used in computers files with digital data as the carrier and networks are considered as high-speed dispatch channels. The sections that follow illustrate the taxonomy of steganographic techniques for image files, including an overview of the most important steganographic techniques for digital images.

CHAPTER 2

LITERATURE REVIEW

2.1 LITERATURE SURVEY

Steganograpohy is a technique used for hiding data. It is always invisible, basically divided in two domains spatial domain and transfer domain. So I have survey literature in these both domains . The fractional wavelet packet transform to decompose a image, reference image is created by changing the frequency values of all subbands, singular values of refrence image will modify with singular values of watermark image. In this study, the concept of fractional wavelet packet transform is explored with its application in digital watermarking. The core idea of the proposed watermarking scheme is to decompose an image via fractional wavelet packet transform and then a reference image is created by changing the positions of all frequency sub-bands at each level with respect to some rule which is secret and only known to the owner/creator. For embedding, the reference image is segmented into non-overlapping blocks and modify its singular values with the watermark singular values. Finally, a reliable watermark extraction algorithm is developed for the extraction of watermark from the distorted image. The feasibility of this method and its robustness against different kind of attacks are verified by computer simulations [1]. The high capacity and security based steganography scheme used Arnold transformation to scrambled image, discrete wavelet transform, alpha blending. Steganography, the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. In this paper, we propose a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is performed to scrambles the secret image. Discrete Wavelet

Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image. We have investigated the performance of our scheme by comparing various qualities of the stego image and cover image. The results show that the proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility [2]. The current soft computing (SC) like neural network (NN), genetic algorithm (GA), support vector machine(SVM), fuzzy logic(FZ). SC is used for improving high quality of image, payload capacity, high imperceptibility. Most NN usage focuses on robustness, as well as the imperceptibility of the cover image by exploiting its learning capability to produce a higher quality stego-image. GA is mostly employed to increase the payload capacity to be embedded as well as to find the best bit positions for embedding position in image steganography. SVM is normally used to increase the imperceptibility of the stego image via its strength to classify the image blocks by learning the relationship between the secret-message and cover-image to be used in the embedding and extracting procedures. A few works have been done in FL especially in preserving the imperceptibility and the number is increasing. Based on this review and leveraging the complementary strengths of FCM in clustering and SVM in classification, we propose a novel hybrid fuzzy c-means (FCM) and SVM [3]. The simple least significant bit insertion. This method will increase secret message capacity and security level we propose a steganography method that applies a technique to embedding a wavelet compressed secret message within the Least Significant Bit (LSB) of the cover image pixels in a specific pattern. The proposed method results in increasing the secret message capacity and security level. The secret message won't be visible after embedding and can be extracted later [4]. The steganalysis based on neural networks to compute statistic features of images to get hidden information. The steganography is the process of hiding one medium of communication (Text, Sound, and Image) within another. It can work on JPEG

2000 compressed images & stir Mark images. The new method of steganalysis based on neural network to get the statistics features of images to identify the underlying hidden data. We first extract the features of image embedded information then input them into neural network to get the output. Experiment result indicates this method is valid in 'Steganalysis'. 'Steganalysis' is the field of detecting the covert messages. Almost all steganalysis consist of hand-crafted tests or human visual inspection to detect whether a file contains a message hidden by a specific steganography algorithm. The neural network in still images is used to overcome the hurdles by hiding the data indirectly into graphical image using neural network algorithm to get cipher bits, the generated cipher bits are then placed in the least significant bit position of the carrier image. The XOR propagation network model is used which acts as a multilayer perception [5]. The worked in wavelet domain by using laplace transform. The specific way of detection is as follows: First, decompose an image by using wavelet, calculate the co-occurrence matrix of the adjacent wavelet coefficients, and apply Laplace transform to the co-occurrence matrix. Then take the Laplace-transformed variances and characteristic function (CF) moments of the co-occurrence matrix as the statistical feature, and choose BP neural network classifiers to classify and detect. Experiments of detecting the four typical steganographic algorithms of Jsteg, F5, Jphide and Outguess in such JPEG images have been carried out at different embedded ratios by using the method mentioned in this article, and the results show that the blind detecting method has the higher accuracy and it has higher calculating speed compared with the typical blind detecting [6]. The proposed steganography based on pixel differencing of images, that pixels used for data hiding To increase the capacity of the hidden secret information and to provide a stego image imperceptible for human vision, a novel steganographic approach based on pixel-value differencing is presented. This approach uses the largest difference value between the other three pixels close to the target pixel to estimate how many secret bits will be embedded into the pixel. The theoretical estimation and experimental results demonstrate that the proposed scheme can provide a superior embedding. Besides, the embedded confidential information can be extracted from stego-images without the assistance of original images [7]. A high capacity method for transform domain work with wavelet transform provides large capacity without diminishing a picture quality of image. The proposed steganography algorithm works on the wavelet transform coefficients of the original image to embed the secret data. As compared to current transform domain data hiding methods, this scheme can provide a larger capacity for data hiding without sacrificing the cover image quality. This is achieved through retaining integrity of the wavelet coefficients at high capacity [8]. The steganalysis using Gabor filter coefficients to train a multi layer perceptronneural network and a support vector machine classifier, Gabor filter used for showing differencing between clear image and altered image This feature set employs the Gabor filter coefficients to train a multi-layer perceptron neural network and a support vector machine classifier. We show that incorporation of the Gabor filter coefficients to the feature sets of images could have a significant role in discrimination between clean and altered images. Experimental results show that the proposed method outperforms previous methods, introduced for steganalysis of LSB-matching image steganography, in terms of both discrimination accuracy and feature set dimensionality. This method provides high accuracy [9]. A steganography based on integer wavelet transform (IWT) it provides high security, capacity, high visual quality Steganography is used to hide a secret message within a over image, thereby yielding a stego image such that even the trace of the presence of secret information is wiped out. The purpose of steganography is to maintain secret communication capacity and imperceptibility. In this paper we propose a modern steganographic technique with Integer Wavelet transform (IWT) and double key to achieve high hiding capacity, high security and good visual quality. Here cover image is converted in to wavelet transform coefficients and coefficients are selected randomly by using Key-1 for embedding the data. Key-2 is used to calculate the number of bits to be embedded in the randomly selected coefficients. Finally the Optimum Pixel Adjustment Process (OPAP) is applied to the image to reduce the data embedding error [10]. Work with wavelet transform for providing high capacity and perceptibility. In order to provide large capacity of the secret data while maintaining good visual quality of stego-image, the embedding process is performed in transform domain of Discrete Wavelet transform (DWT) by modifying of transform coefficients in an appropriate manner. In addition, the proposed method do not require original image for successful extraction of the secret information. The experimental results show that the proposed method provides good capacity and excellent image quality [11]. A steganography technique based on integer wavelet transform and used Munkre's algorithm IWT is used to transform both cover and secret images from spatial domain to frequency domain, and assignment algorithm is used for best matching between blocks for embedding. They 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). Experimental results depict that stego image and extracted secret image could have high visual quality and they are perceptually similar to their original versions. In addition, this method shows high robustness against six different attacks. Embedding in diagonal detail . In this stego data is hide in frequency domain of cover image [12]. The steganography technique based on least significant bit insertion and pixel differencing of cover image [13]. A new robust adaptive data hiding method in the wavelet transform domain of an image is introduced in this paper. The proposed steganography method embeds the secret data in the blocks of an image that seems to be noisy based on the bit plane complexity of each block and does not destroy the co-occurrence matrix of wavelet coefficient. Most of the steganalysis methods are based on the moments of histogram or co-occurrence matrix of an image. Since the histogram is one dimensional case of co-occurrence matrix, we embed the data in blocks which causes minimal changes to the co-occurrence matrix. In our method we use the one-third and rounding methods for embedding data in wavelet coefficients, and retain the co-occurrence matrix of wavelet coefficient. Our method has more robustness in comparison with other steganography method in same capacity [14]. A technique for For distinguish the LSB (Least significant bit) replacement stego image from MLSB (Multiple least significant bits) stego image, which are two typical kinds of steganographical methods of image spatial domain and have been applied widely, a classification algorithm based on the shift of pixel value and irrelevance of pixel pairs is proposed. In this algorithm, a shift operator is adopted for each pixel value of test image, and then the irrelevance of a kind of special adjoint pixels is extracted as the feature, at last the BP (Back-Propagation) neural network is designed to classify LSB replacement and MLSB replacement images. Results of experiments show that the proposed method can distinguish the MLSB replacement stego images from LSB replacement stego mages reliably [15]. A new adaptive data-hiding method based on least-significant-bit (LSB) substitution and pixelvalue differencing (PVD) for grey-scale images. The proposed method partition the cover image into some non-overlapping blocks having three consecutive pixels and select the second pixel of each block as the central pixel (called base-pixel). Then k-bits of secret data are embedded in the base pixel by using LSB substitution and optimal pixel adjustment process (OPAP). The difference between the base-pixel value and other pixel values in the block are utilised to determine how many secret bits can be embedded in the two pixels. Also, the method divides all possible differences into lower level and higher level with a number of ranges. Then, it obtains the number of the secret bits that will be embedded into each block depending on the range which the difference values belong to. The experimental results show that the proposed method can embed a large amount of secret data while maintaining a high visual quality of the stego-images.

CHAPTER 3

STEGANOGRAPHY MODEL

Steganography is a technique used for hiding data. It contains a technical terms as a taxonomy for representing original image, message (host data), embedded image and security key. Due to high security and robustness steganography become most popular technique in communicating digital data. In different techniques we can use different terms for same data like original image called as cover image, secret data called as host data or stego data, embedded data called as stego image. Different taxonomy are as follows:

Cover-Image: An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc.Thecover image is sometimes called as the "host".

Stego Data: It is defined the image or data or information is to be hidden the digital media . Digital media can be a video, audio etc.

Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

Secret key: This is the key used as a password to encrypt and decrypt the cover and stego respectively in order to extract the hidden message.

With the help of these basic terms we can make a steganography model. Hence steganography model will be explained as: An original image will be called as cover image used as a data in which secret data will be hide. Secret data can be images, video, audio or any type of file. Cover image and secret data will be sent to encoder which is provided with a secret key. Secret key will be known to sender and receiver only. To maintain higher security secret key is provided. Both cover image and secret image will be embed by using different techniques like alpha blending, multiple embedding in different frequencies. That embedded data will be called as stego image. At the receiver side stego image is send to decoder which separate the original data from the stego image and gives secret data. The steganography model will be explained in fig3.1 are as follows.

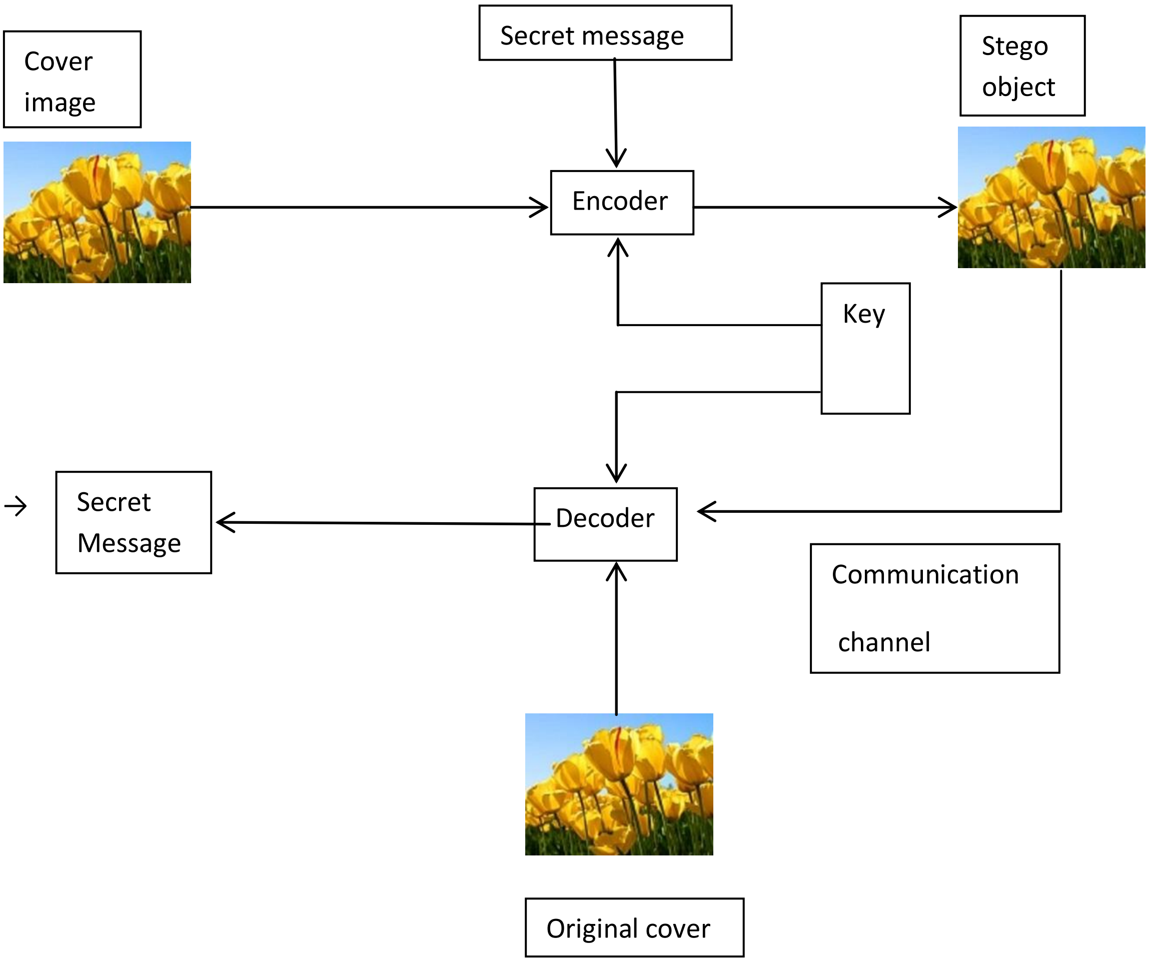

Figure 3.1 Steganography Model

3.1 FRAMEWORK OF STEGANOGRAPHY MODEL

In this I frame a basic model of steganography, which gives overview of steganography process. In this model, I representing the sequence of all necessary steps used for embedding and extracting the secret data. By considering this model as a basic any one can apply different strartigies or methods for embedding and extracting data. Methods can be DWT, FRWT, DCT, Fractional fourier transform etc. This framework model will be shown in fig.3.1.1.

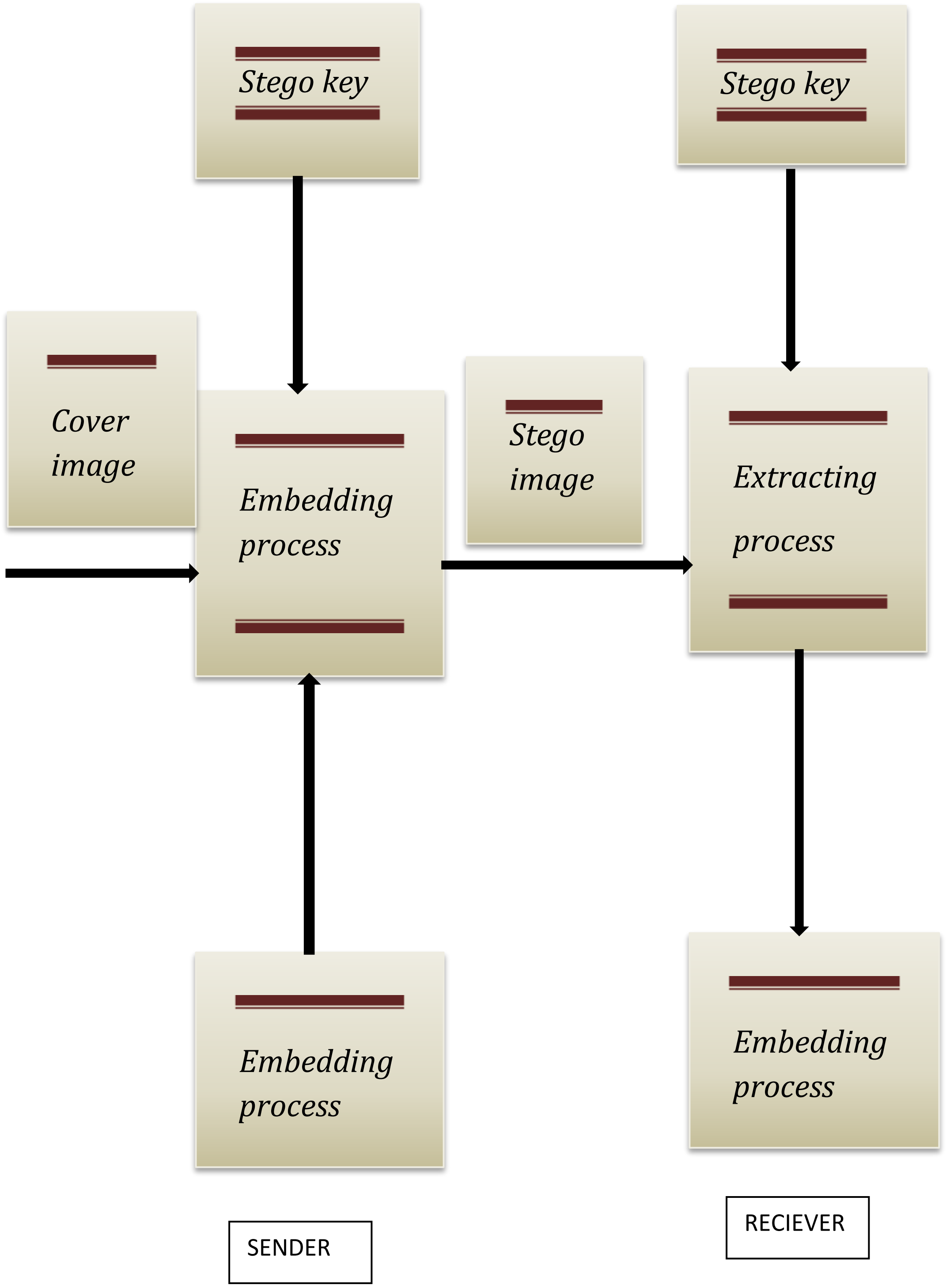

Figure 3.1.1 Framework of Steganography Model

CHAPTER 4

OVERVIEW OF STEGANOGRAPHY

Steganography is a powerful security tool that provides a high level of security, particularly when it is combined with encryption. Steganography differs from cryptography. The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the best solution for secure communication, it is only part of the solution. Both sciences can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well. Watermarking and fingerprinting, among technologies related to steganography, are basically used for intellectual property protection. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. Though this method keeps the data accessible, but it is permanently marked. The hidden information in a watermarked object is a signature referring to the origin or true ownership of the data in order to ensure copyright protection. In the case of fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups. The performance of a steganographic system can be measured using several properties. The most important property is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associated measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects , and robustness, which refers to how well the steganographic system resists the extraction of hidden data.

4.1 IMAGE STEGANOGRAPHY

As stated previously, images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS).

4.1.1 Image Files

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel. 8 bits are utilized to represent the color of each pixel. Both Monochrome and gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that digital color images are known for being saved in 24-bit files and for utilizing the RGB color model. Almost all the color variations for the pixels of a 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8 bits. Thus, in any given pixel, the number of different shades of red, green, and blue can reach 256 that adding up to more than 16 million combinations that finally result in more than 16 million colors. The most prominent image formats, exclusively on the internet, are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, and to a lesser degree, the portable network graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure.

4.1.2 TAXONAMY OF STEGANOGRAPHY TECHNIQUES

There are quite a lot of approaches in classifying steganographic techniques. These approachescan be classified in accordance with the type of covers used with secret communications. Another possibility is done via sorting such approaches depending on the type of cover modification already applied in the process of embedding. The second approach is adopted in this work, although in some cases an exact classification is not possible. In general, the process of embedding can be defined as follows:

Let C denote the cover carrier, and C ~ the stego-image. Let K represent an optional key (as a seed used to encrypt the message or to generate a pseudo-random noise, which can be set to{f } for simplicity), and let M be the message to be sent. Then, Em represents an embedded message and Ex represents the extracted message. Therefore, to distinguish between different steganographic techniques in a wide sense, one must take into consideration both the methods that modify the image and those that modify the image file format. However, the modifications to the file format are less robust. The important issue to mention here is the main role compression usually plays when it comes to deciding which steganographic algorithm is better. Though lossy compression methods result in smaller image file sizes, they increase the possibility of the partial loss of an embedded message because surplus image data is to be eliminated in these techniques. Lossless compression does not compress the image file as much. As a result, researchers have come up with different steganographic algorithms that suit such compression types. Steganographic techniques that modify image files for hiding information include the following:

1. Spatial domain
2. Transform domain
3. Spread spectrum
4. Statistical methods
5. Distortion techniques

Steganographic techniques that modify the image file format involve file embedding and palette embedding. In addition, there are techniques that modify the elements in the visual image including: The image generation technique; and the image element modification technique. Finally, there is a special type of the spatial and transform domain techniques called the adaptive steganography technique, which we also describe for completeness. The next section explains each steganographic approach in more detail.

CHAPTER 5

TECHNIQUES OF STEGANOGRAPHY

In digital approach, steganography is defined as most common method for transferring secret data. So there are different techniques of steganography for communication between receiver and sender.

5.1 SPATIAL DOMAIN TECHNIQUE

Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be a bit scant when compared to the human visual system (HVS).One of the ways to do so is to hide information in the least significant bit (LSB) of the image data. This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image.

5.2 TRANSFORM DOMAIN TECHNIQUES

Transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. It is worth saying that most of the strong steganographic systems today operate within the transform domain. Transform domain techniques have an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it.

5.2.1 JPEG compression

If an image is to compress into JPEG format, the RGB color space is first turned into a YUV representation. Through this representation, the Y component represents brightness (or luminance) and the U and V components stand for color (or chrominance). It is known that the human eye is more sensitive to changes in the brightness of a pixel than to changes in its color. Down sampling the color information is taken as an advantage of the JPEG to reduce the size of the file Where the color components (U and V) are splitted in the horizontal and vertical directions and consequently reducing the file size by a factor of 2.

Then, the image is transformed. For JPEG images, the discrete cosine transform (DCT) is used; the pixels can be converted with such mathematical processing by simply “spreading” the position of the pixel values over the image or part of it. With DCT transformation, a signal is transformed from the representation of an image into the frequency domain, this is done by sorting the pixels into (8 × 8) pixel blocks and transforming these blocks into 64-DCT coefficients which are affected by any modification of a single DCT coefficient.

The quantization phase of the compression is counted as the next step. Besides it is considered as biological property where the human eye is imposed. Basically, the human eye is known for being capable of identifying small differences in brightness over a relatively large area. The same does not apply when considering the distinction between different strengths in high-frequency brightness. Consequently, the strength of higher frequencies can be reduced without any change in the image appearance. The JPEG format is done by dividing all the values in a block via a quantization coefficient, so the results are made approximate to integer values. The last point is to encode the coefficients by using Huffman coding just to reduce the size.

5.2.2 JPEG Steganography

Previously, it was believed that steganography could not be used with JPEG images owing to the lossy compression, which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise. Data in most of the steganographic systems seems to be embedded into the non-zero discrete cosine transform (DCT) coefficients of JPEG images. The major JPEG steganographic methods can be described as follows: JSteg/JPHide. Jsteg and JPHide are two classic JPEG steganographic tools that employ the LSB embedding technique . JSteg functions to hide the secret data in a cover image by simply exchanging the LSBs of non-zero quantized DCT coefficients with secret message bits. The quantized DCT coefficients, already used to conceal secret message bits in JPHide, are selected randomly by a pseudo-random number generator. JPHide, on the other hand, tends not only to modify the LSBs of the selected coefficients.

5.2.3 Wavelet transform technique

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. The discrete wavelet transform (DWT) method is favored over the discrete cosine transform (DCT) method, owing to the resolution that the WT provides to the image at various levels. Wavelets are mathematical functions that divide data into frequency components, which makes them ideal for image compression. In contrast with the JPEG format, they are far better at approximating data with sharp discontinuities. A steganography technique, based on wavelet compression techniques, that attaches attribute information to images in order to reduce the amount ofinformation stored in a database of images. They use the homogenous connected region interested ordered transmission (HCRIOT) wavelet algorithm for image encoding and compression. This technique embeds secret information in the edge and detail regions of the image where the human eye is less sensitive to the noise generated by the technique. In general, the human eye is more sensitive to noise in the smooth regions of an image. In the project described in, researchers use vector quantization, called Linde-Buzo-Gray (LBG), associated with block codes, known as BCH codes and one-stage discrete Haar wavelet transforms. They emphasize that modifying data by using a wavelet transformation produces good quality with few perceptual artifacts. A group of scientists at Iowa State University are developing an advanced application called artificial neural network technology for steganography (ANNTS), with the aim of detecting all current steganography methods, which include DCT, DWT, and DFT. They found that the inverse discrete Fourier transform (IDFT) includes a rounding error that makes DFT inappropriate for steganography applications. The research discussed in proposes, a data hiding technique in the DWT domain. DWT with the first level is used to decompose both secret and cover images, where each is broken into disjoint (4 × 4) blocks. Then a comparison is made between the blocks of the secret image and the cover blocks to determine the best match. Later, error blocks are produced and embedded into the coefficients of the best matched blocks in the HL part of the cover image. In, the authors proposed high capacity and high security steganography using the discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and the payload are merged into a single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to minimize the pixel range to ensure accurate recovery of the payload at the receiving end. The capacity of the proposed algorithm is increased as only the approximation band of the payload is considered. The entropy, mean square error (MSE) and capacity are improved with an acceptable peak signal to noise ratio (PSNR).

5.3 SPREAD SPECTRUM TECHNIQUE

Spread spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image.

Cover image as noise A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub images . When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum steganography. When the sub cover images consist of separate point distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum steganography. These techniques require searching the image for the carrier in order to then retrieve the data. These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier. In this case, after the carrier is created, and before the message is added, the carrier is compressed using JPEG compression and decompression such that it will be unaffected by later JPEG compression of the cover image. The capacity can be traded directly for robustness, and it depends greatly on the image. Pseudo-noise this technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect. Spread spectrum image steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error control coding and image processing to hide information in images, is an example of this technique. The general additive embedding scheme can be described as follows: In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible not only to the human eye but also through computer analysis without access to the original image.The last few years witnessed the development of several steganography techniques oneof which is spread spectrum steganography. In 1996, Smith and Comiskey describedthree schemes, namely direct sequence, frequency hopping, and chirp. In imagesteganography, it is noticed that high frequencies usually aid the invisibility of the hiddeninformation, but at the same time, they are not efficient as far as robustness is concerned. In contrast, low frequencies are better with respect to robustness, but are far too visible to be useful. Such conflicting points are reconciled by the spread spectrum technique via allowing the embedding of a low-energy signal in each one of the frequency bands, and as illustrated in. Instead of using direct sequences, two new processing methods are proposed .Such methods include block spread spectrum and duplicate spreading. Spread spectrum techniques are capable of being combined with transform embedding by using transformation techniques in order to get the payload capacity increased. In, the authors introduce a technique based on discrete Fourier transform (DFT) that can significantly increase the number of transform coefficients that can transmit hidden information. A blind image steganography, based on a hybrid direct sequence/frequency hopping (DS/FH) technique, is described in, in which the system retrieves the hidden message without needing the original image. The authors in found that using a signature vector, when embedding a spread spectrum (SS) message, maximizes the signal-to-interference-plus-noise ratio (SINR) at the output of the corresponding maximum-SINR linear filter. The research in describes the benefits of combining the spread spectrum technique with the advantages of error correction coding and DFT simply to the robustness of the system increased. Finally, an analysis proposes using a code division multiple access (CDMA) spread spectrum for both the spatial domain and the transform domain for image steganography in MMS. Their experimental results reveal that the spread spectrum detection method is highly robust for normal signal manipulation.

5.4 STATISTICAL METHOD

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation. Statistical steganographic techniques exploit the existence of a “1-bit”, where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a “1” is transmitted, otherwise it is left unchanged. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message. Another technique called data masking. According to this technique, the message signal is processed such that it views the properties of an arbitrary cover signal. In work, the authors propose a method where the transformed image coefficients are broken down into two parts to allow the coded message signal to replace the perceptually insignificant component. Hence, the statistics of the quantized (non-zero) AC DCT coefficients are modified taking into consideration the parametric density function. This process requires a low precision histogram of each frequency channel in addition to matching the model with each histogram by deciding the corresponding model parameters. However, statistical steganographic methods in their simplest form, for which sub-images are simply sub-rectangles of the original image, are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. To counter these attacks, the sub-images could be selected based on picture elements, for example, the faces in crowd, and error correction coding could be utilized within the message. These defenses can make the statistical steganographic method approximately as robust as the underlying watermarking scheme .

5.5 DISTORTION TECHNIQUE

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, then the message bit is a “1.” Otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such manner that the statistical properties of the image are not affected (which is different from many LSB methods). However, the need for sending the cover image limits the benefits of this technique. As in any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, rotating, or scaling, the receiver can easily detect the modification. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be fully recovered. An early approach to hiding information was to do so in text. Most text-based hiding techniques are of the distortion type. For example, the layout of a document or the arrangement of words might show or reflect the presence of information. Considering one of these techniques, can show the adjustment of the positions of lines and words where spaces and “invisible” characters are added to the text, providing a method of sending hidden information.

5.6 FILE EMBEDDING

Different image file formats are known for having different header file structures. In addition to the data values, such as pixels, palette, and DCT coefficients also can used. For example, the comment fields in the header of JPEG images usually contain data hidden by the invisible Secrets and Steganozorus. Camouflage, PGE10, and PGE20 add data to the end of a JPEG image. Image storage formats such as TIFF, GIF, PNG and WMF have a file header that can be exploited to hide arbitrary information. In this case, that arbitrary data may be a secret message. It is possible to append data to many image storage formats without affecting the image. When the image is processed for display, the image user will decode the image size from the file header, and any tracking information attached to the end of the file will be ignored. Using this technique, it is possible to attach a message of any size to a cover image. However, the message could be removed from the cover image by simply resaving the image in the same file format. The limitations of this method are that despite the large payload, it is not that difficult to identify and defeat, it is weak when lossy compression and image filtering are concerned, and the resaving of the image implies complete loss of hidden data.

5.7 PALLET EMBEDDING

In a palette-based image, what matters is the fact that only a subset of colors from a particular color space is used to colorize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colors as a list of indexed pairs (,) i i c, assigning a color vector i c to every index i, and the actual image data, which specifies a palette index for each pixel, rather than the color value itself. The file size gets decreased via this approach when only a limited number of color values are used in the image. Two of the most popular formats are the graphics interchange format (GIF) and the bitmap format (BMP). However, owing to the availability of advanced compression techniques, their use has diminished. In some cases, the palette itself can be used to hide secret information. Because the order of the colors in the palette usually does not matter, the ordering of colors can be used to transfer information. In essence, a hidden message can be embedded using the difference between two colors in the palette (i.e., one secret message bit for every two colors in the palette). Color palettes are used to minimize the amount of information images that are used to represent colors. Since steganographic message within the bits of the palette and/or the indices is embedded in the palette-based steganography, one must be careful not to exceed the maximum number of colors.

5.8 IMAGE GENERATION TECHNIQUE

Many techniques have been proposed that encrypt messages so that they are unreadable or as secret as possible. Big Play Maker hides information by converting the secret text message into a larger and a slightly manipulated text format. The same principle can be employed in image creation, in which a message is converted to picture elements and then collected into a complete stego-image. This method cannot be broken by rotating or scaling the image, or by lossy compression. Parts of the message may be destroyed or lost because of cropping, but it is still possible to recover other parts of the message by encoding the message with error correcting information. Generally, this technique uses pseudo-random images, because if a malicious third party detects a group of images passing through a network without any reason for them being there (i.e., random images), he or she may suspect that the images contain secret information and block their transmission.

5.9 IMAGE ELEMENT MODIFICATION TECHNIQUES

Some steganographic techniques do not try to hide information using the actual elements of the image. Instead, they adjust the image elements in completely undetectable ways, for example, by modifying the eye color or hair color of some person in a photograph. In addition, this information will survive rotations, scaling, and lossy compression. The feasibility of modifying objects within images as a tactic for hiding information has been discussed by. It is important to keep in mind that when this method is used, the same cover image must not be used more than once, because the elements used will become apparent. This technique can be achieved manually with any photo editing software. With the advent of computer vision systems that identify objects within pictures, these methods have become more viable.

5.10 ADAPTIVE STEGANOGRAPHY

Adaptive steganography is a special case of the spatial and transform techniques. Moreover, it is introduced as statistics-aware embedding and masking. Global statistical characteristics of the image are basically used before any attempt to deal with its frequency transformed coefficients. These statistics decide what changes can be made. A random adaptive selection of pixels actually characterizes this method, relying on the cover image and the selection of pixels in a block with a large standard deviation (STD). The latter is intended to avoid areas of uniform color, such as smooth areas. This technique is known for exploiting images with existing or deliberately added noise and with images that show color complexity. An adaptive technique applied to the LSB substitution method has been proposed in. The idea behind this method is to make use of the correlation between neighboring pixels so as to calculate the degree of smoothness. The researchers shed light on the options of having two-, three-, and four-sided matches. The payload (embedding capacity) they were able to obtain was high. A technique called the “adaptive more surrounding pixels using” (A-MSPU) technique, which improves the imperceptibility problems of multiple base notational systems (MBNS). This technique pays attention to the edge areas of a cover image while reexpressing the secret bits in multiple base notational systems. The suggested approach uses the same probability parameter to get the secret bits scattered and it also uses surrounding pixels with the maximum number to determine the capacity of every target pixel. Most steganographic techniques use either three or four adjacent pixels of a target pixel.

CHAPTER 6

EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. These parameters are as follows:

1.Undetectability (imperceptibility):This parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.

2. Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique (out of the scope of this paper).

3. Payload capacity: it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests. The following paragraphs compare the previously mentioned steganographic techniques in terms of the competing parameters.

4. LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression. Although LSB techniques can hide large quantities of information i.e. high payload capacity, they often compensate the statistical properties of the image and thus indicate a low robustness against statistical attacks as well as image manipulation.

5. The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms. The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers' attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival .

6. Spread spectrum techniques are generally quite robust against statistical attacks, since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction .

7. The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling

attacks, along with any attacks that work against the watermarking technique. Defenses could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depends on the cover image selected.

8. Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS.

9. Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data .

10. Hiding information via steganographic techniques that modify the elements in the visual image results in a stego image that will survive rotation, scaling.

CHAPTER 7
PROPOSED METHOD OF STEGANOGRAPHY

In this study, we proposed method of embedding host image into original image with the help of alpha blending. For embedding firstly calculate the DWT of both original image and host image, then determine FRWT of both images. After this addition of both images will take place by using alpha blending then apply IDWT and in result stego image wiil produced. Basically stegoimage is addition of original and host image. For extraction alpha blending will apply on DWT coefficients of stego image and host image. Then apply IDWT and IFRWT get host image (secret image).

7.1 DWT(DISCRETE WAVELET TRANSFORM)

In this wavelet are discretely sampled . It has advantage over fourier transform that it captures both frequency and location information .

1.One level of the transform: DWT of a signal x is calculated by passing it through a series of filters. First the signal is passed through a low pass filter with impulse response g resulting in aconvolution of the two:

$$y[n] = (x*g)[n] = \sum x[k]g[n-k]$$

The signal is also decomposed simultaneously using a high pass filter. The output giving the detailed coefficients (from high pass filter) and approximation coefficients (from low pass filter) . However, since half the frequencies of the signal have now removed, half the samples can be discarded according to Nyquist‘s rule. The filter outputs are then subsampled by 2.

$$y_{low}[n] = \sum x[k]g[2n-k]$$

$y_{high}[n] = \sum x[k]h[2n-k]$

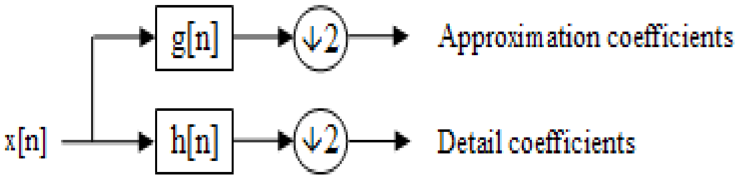

Figure 7.1.1 Coefficients of DWT

2. Second level of wavelet Transform: In this entire process the execution of 1-D subband decomposition will take place twice. First in horizontal direction and second in vertical direction. For example low pass subband (Li) resulting from the horizontal direction and is further decomposed into vertical direction and gives LLi and LHi subbands. Similarly (Hi) is further decomposed into HLi and HHi. After this 2D decomposition will apply. LLi is low resolution band and LHi, HLi, HHi are horizontal, vertical and diagonal contain residual information.

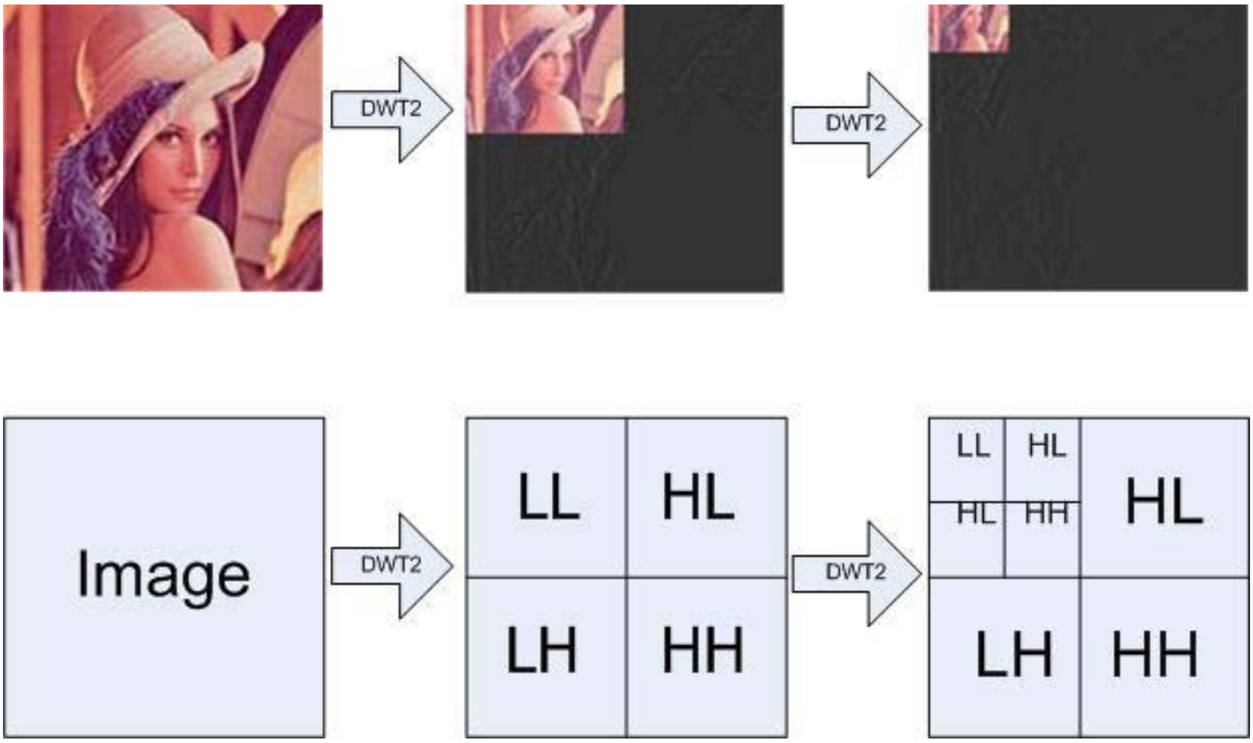

Figure 7.1.2 Steganography based on DWT

7.2 ARNOLD TRANSFORM

It is defined as a chaotic map named after Vladimir Arnold basically used for scrambling the images so that data security can be maintained. Digital image is put as a matrix. After Arnold transform this image will be chaotic. Due to a correlation between elements discrete digital image is a class of special matrix. After Arnold transform new matrix can be obtained which provides image scrambling processing. Then set the image pixel coordinates. The order of image matrix is N, i, j € (0, 1, 2,......., N-1) and the Arnold transform is as in (1):

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} (Mod\ N)$$

.

The above transformation is one to one correspondence; the iteration can be done in image and image number is used as a secret key for extracting the secret image. This algorithm gives more security and robustness.

7.3 FRWT(FRACTIONAL WAVELET TRANSFORM)

It is defined as the transform in which firstly take fractional fourier transform of images . Then DWT apply on these images. In fourier transform, it transfer a function in intermediate domain between time and frequency. It’s application filter design, pattern recognition and signal analysis to phase retrieval. Basically fractional transform is domain signal. It’s a rotation of time-frequency domain. Then apply discrete wavelet transform on fractional fourier transform signal and calculate detailed and approximation coefficients.

7.4 ALPHA BLENDING

It is defined as the process of combining a trasnslucent foreground color with a background color, thereby producing a new blended color. The degree of the foreground color translucency may range from completely transparent to completely opaque. If foreground color is completely transparent the blended color will be background color.

If foreground color is completely opaque, the blended color will be foreground color. Of course, translucency can range between these extremes, in which blended color is weighted average of the foreground and background.

Alpha is the color code ranges from 0.0 to 1.0 where 0.0 represent fully transparent color and 1.0 represent fully opaque color. Alpha Blending combines two images the first one is the input image and the other one is referred as “ image to blend.” It is a concept of merging two or more images into one. So one can see imaginary detail through just one image. We cannot allow any pixel channel integer to possess a value greater than 255 otherwise these would exist an overflow.

Alpha blending just take the summation divide the num of inputs to yield the arithmetic mean.

e = c + d / 2;

It’s a way of mixing two colors of two images together to form a final image. Alpha blending sometime called as alpha blending “translucency” when the blending factor changes with time , alpha blending is called “cross fade” or “dissolve”. We will call the two input images as “source image” the output image as the “blended image”. The blended factor or percentage of colors from the first source image used in the blended image is called “alpha”. Alpha range from 0.0 to 1.0 instead of 0 to 100%.

ALGORITHM: Alpha Blending can be accomplish in computer graphics by blending each pixel from the first source image with the corresponding pixel in the second image.

Final pixel= alpha *(Final image source pixel)+(1.0-alpha)*(second images source pixel)

7.5 IMPLEMENTED ALGORITHM

7.5.1 Embedding Algorithm

It is defined as an algorithm basically used for embedding secret information in cover media. For embedding this information we follow different steps through which security can be maintained. In our application secret data is embedding in original data with the help of alpha blending technique, which add the DWT coefficients of secret image and original image. On addition of original image and secret image we get stego image. Stego image will be produced by taking IDWT of combination of original image and secret image. Embedding algorithm should be highly secret for maintaining higher security. Steps of Embedding process:

Step1: Firstly take cover image(C) of size NxN and secret image of size MxM. Then apply Arnold Transform with key on Secret image(S) through which image will scramble. Key will be known to only intended user. With the help of Arnold Transform we can attain high security.

Step2: Take fourier transform of cover image(C) and scrambled secret image (SS), which separate the real and imaginary part of images.

Step3: Real part of both images will transform into wavelet domain. 2D DWT of level1 will apply on both images. Through which we extract approximation (LL) coefficient and detailed coefficient {LH, HL, HH}. Horizontal approximation coefficient is used for embedding data.

Step4: Extract the approximation coefficient of matrix A and detailed coefficient matrices HL, LH & HH of level1 of the cover image(C).

Step5: Extract the detailed coefficient of matrix A1 and detailed coefficient matrices HL1, LH2, HH2 of level1 of scrambled secret image (SS).

Step6: Apply Alpha Blending on image C and image SS which add approximation coefficients of image C and image SS.

Step7:Apply 2D IDWT (inverse discrete wavelet transform) to get stego image (SI).

In this way embedding algorithm will apply in fig.7.5.1. For higher security secret image will be scrambled using Arnold transform, using a key. Key will be known to sender and receiver. Key is applied for higher security and robustness.

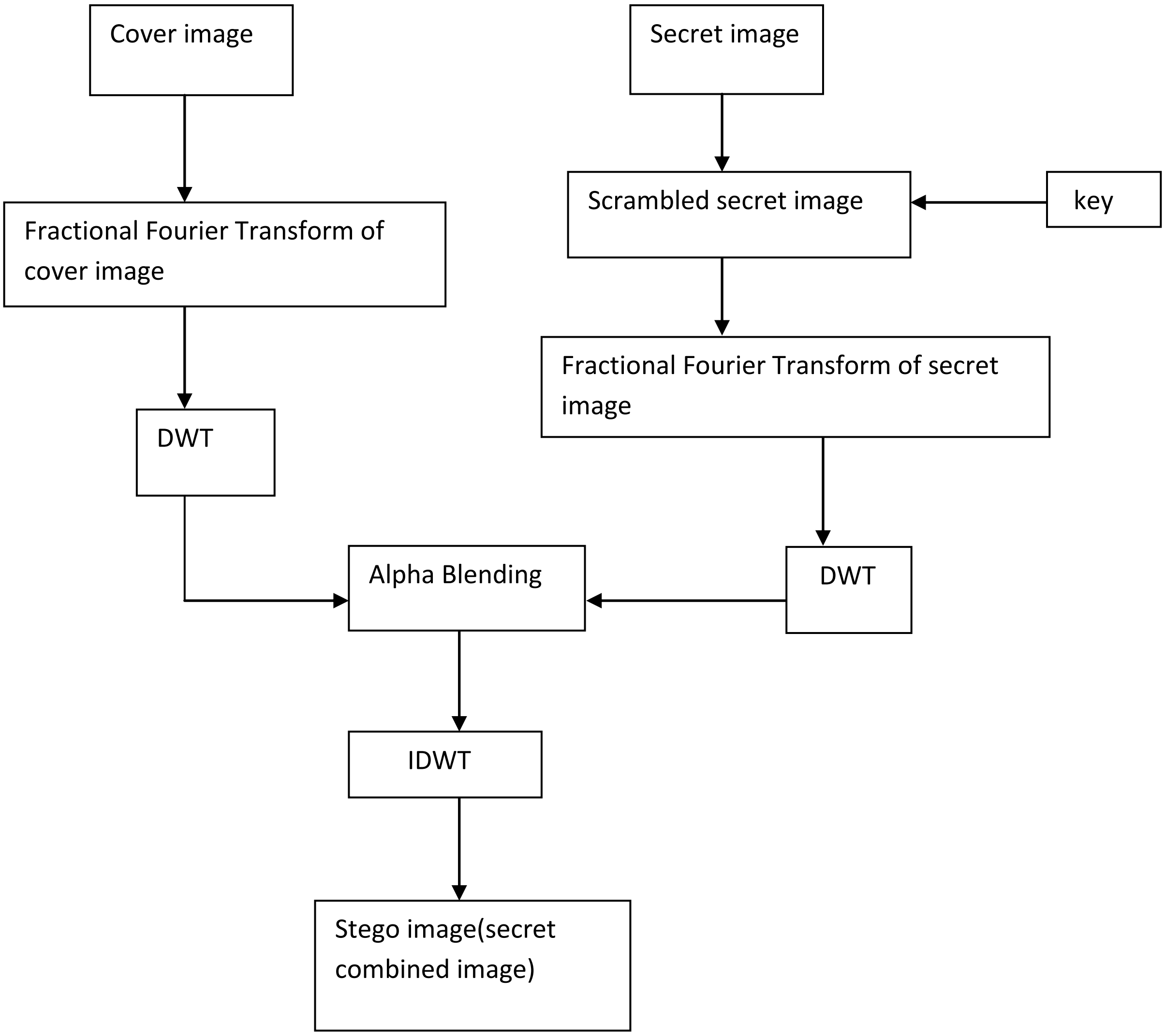
Cover image
Secret image
Scrambled secret image
key
Fractional Fourier Transform of cover image
Fractional Fourier Transform of secret image
DWT
Alpha Blending
DWT
IDWT
Stego image(secret combined image)

Figure.7.5.1 Embedding code of modified secure steganography.

7.5.2 Extraction Algorithm

In extraction process from stego image we will get secret data by using alpha blending, inverse IDWT, inverse Arnold transform, inverse FRWT. With the help of alpha blending we will subtract coefficients of cover image from secret image. Then by applying IDWT we will get scrambled secret image. Then Arnold transform with fractional wavelet transform will apply on this, produced secret image. Secret image is almost similar in appearance. Embedding process should be highly effective so through which image authentication can be maintained.

Steps of Extracting Process:

Step1: Apply 2-D DWT of level 1 on both stego image (SI) and cover image(C).

Step2: Apply Alpha Blending on both SI and C.

Step3: Perform IDWT on separated wavelet coefficients and get scrambled secret image.

Step4: Take fourier transform of scrambled secret image.

Step5: Take inverse Arnold of scrambled secret image .

Step6: Recovered secret image (which is almost in similar to secret image).

This extracting algorithm will represent by fig.7.5.2.

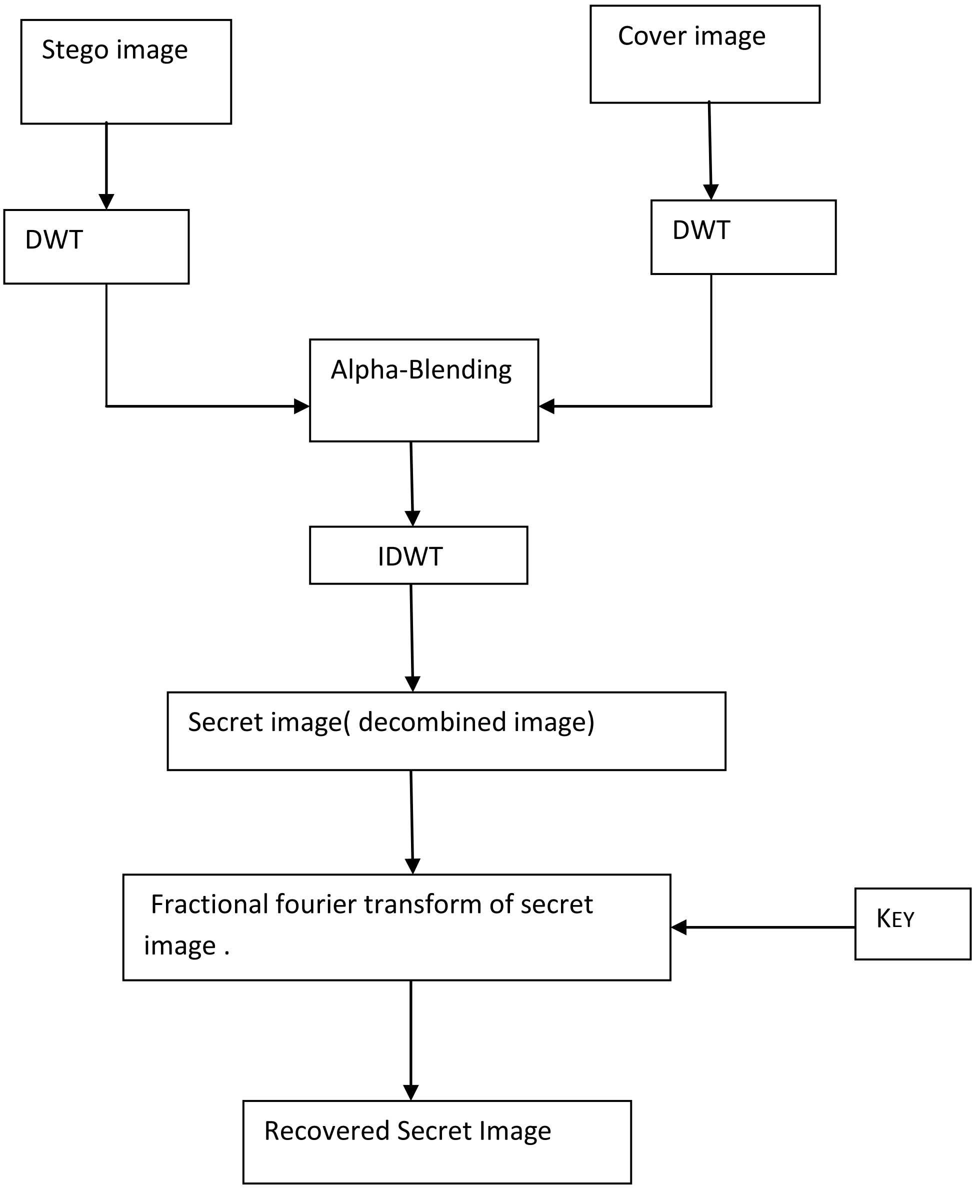
Stego image
Cover image
DWT
DWT
Alpha-Blending
IDWT
Secret image(decombined image)
Fractional fourier transform of secret image .
KEY
Recovered Secret Image

Figure.7.5.2 Extracting code of modified secure steganography

CHAPTER 8

EXPERIMENTAL RESULTS AND ATTACK ANALYSIS

8.1 SUBJECTIVE EVOLUTION

The performance of purposed steganography method is implemented by using Matlab 2010 and 7.10 version. Experimental result and attack analysis will be discussed in this section. In our experiment we considered different gray scale images of size 256x256 images like cameraman, circles, goldhill, peppers, lena etc .

8.2 PERFORMANCE ANALYSIS

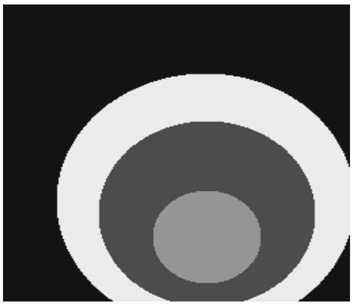

Figure.8.1.1 Cover image

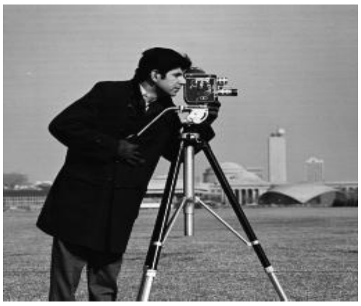

Figure.8.1.2 secret image

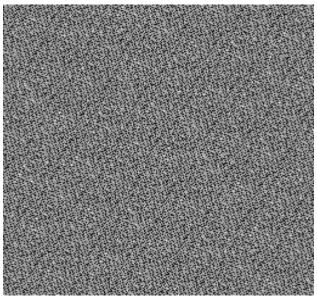

Figure.8.1.3 Scrambled secret image.

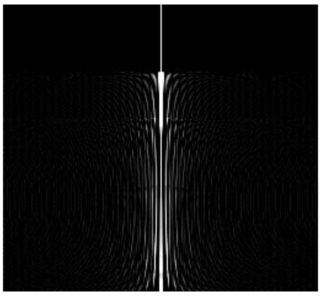

Figure.8.1.4 Fractional fourier transform Of cover image.

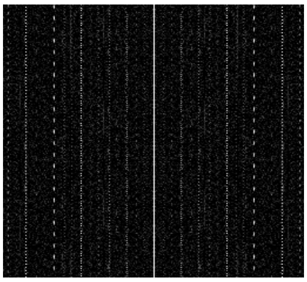

Figure.8.1.5 Fractional fourier Transform of scrambled secret Image.

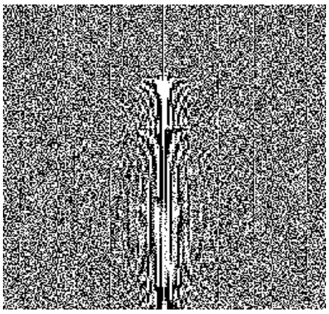

Figure.8.1.6 Stego image Transform of of scrambled secret Image.

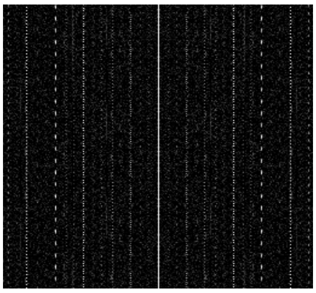

Figure.8.1.7 Extracted scrambled secret Image (decombined image).

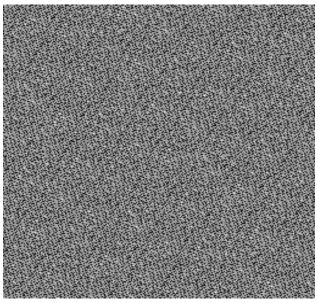

Figure.8.1.8 Fractional fourier transform of scrambled secret image.

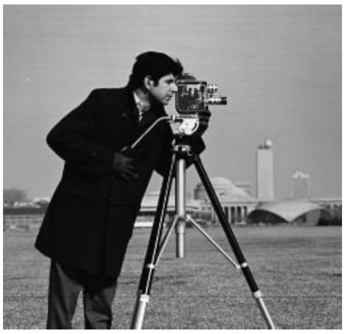

Figure.8.1.9 Recovered secret image.

8.3 OBJECTIVE EVALUTION

As a performance measure for image distortion due to embedding, the well-known peak-signal-tonoise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. The good visual quality of stego images (ie- images embedded with a secret image) is the most important property of steganography system because it is hard to detect by detectors. It is defined as:

PSNR = $10\frac{\log_{10}(255)^2}{MSE}$ db

MSE $=\frac{1}{MN}\sum_{J=1}^{M}\sum_{K=1}^{N}(X_{J,K}-X_{J,K}^{'})^2$

MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N, and the Xj,k and X'j,k are pixel located at the jth row the kth column of images x and x', respectively_ A large PSNR value means that the stego image is most similar to original image and vice versa_ It is hard for the Human eyes to distinguish between original cover image and stego image when the PSNR ratio is larger than 30db. The other Image quality parameters normalized cross correlation, average difference, structural content, maximum difference and normalized absolute error are taken for our experiment.

N CC = $\sum_{J=1}^{M}\sum_{K=1}^{N}(X_{J,K}-X_{J,K}^{'})\frac{1}{\sum_{J=1}^{M}\sum_{K=1}^{N}X_{J,K}^{2}}$

AD = $\frac{\sum_{J=1}^{M}\sum_{K=1}^{N}(X_{J,K}-X_{J,K}^{'})}{MN}$

SC=$\frac{\sum_{J=1}^{M}\sum_{K=1}^{N}(X_{J,K}^{2})}{\sum_{J=1}^{M}\sum_{K=1}^{N}(X_{J,K}^{'})^2}$

NAE = $\frac{\sum_{J=1}^{M}\sum_{K=1}^{N}|X_{J,K}-X_{J,K}^{'}|}{\sum_{J=1}^{M}\sum_{K=1}^{N}|X_{J,K}^{'}|}$

MD = Max$\left(|X_{J,K}-X_{J,K}^{'}|\right)$

The original cover image x sized M x N and the stego image x' sized M x N, and the Xj,k and X'j,k are pixel located at the /' row the kth column of images x and x', respectively.

8.4 Result

In this section, comparison of various quality measurements on embedded secret image and extracted secret image with cover image and stego image has done.

Cover image	**Secret image**	**MSE**	**PSNR**	**SC**	**MD**	**NC**	**NAE**
Circles	camera	0.0018	75.435	1.00	1.268e-007	0.998	1.6298e-0014
Lena	goldhill	0.0018	75.262	1.00	1.5618e-007	0.998	2.1237e-014
Camera	circles	0.0018	74.794	1.00	1.36e-007	0.998	2.204e-0014
Goldhill	lena	0.0018	74.477	1.00	1.3217e-007	0.997	1.6258e-014
Lena	circles	0,0018	74.794	1.00	1.5375e-007	0.998	2.4913e-014
Circles	lena	0.0018	74.977	1.00	1.2724e-007	0.997	1.5632e-014
Peppers	lena	0.0018	74.977	1.00	1.5665e-007	0.997	1.9269e-014

Table 1 MSE, PSNR, SC, MD, NC, NAE for test images

8.5 ATTACK ANALYSIS

In order to measure the robustness of proposed scheme various attacks have been performed on test image. The scheme can withstand number of attacks like Gaussian white' noise of zero mean and 0.001 variance, contrast variations , histogram attack , sharpening attack , median filtering attack . Recovered watermark with accuracy rate and correlation coefficient are shown below in figure 5 for camera man .

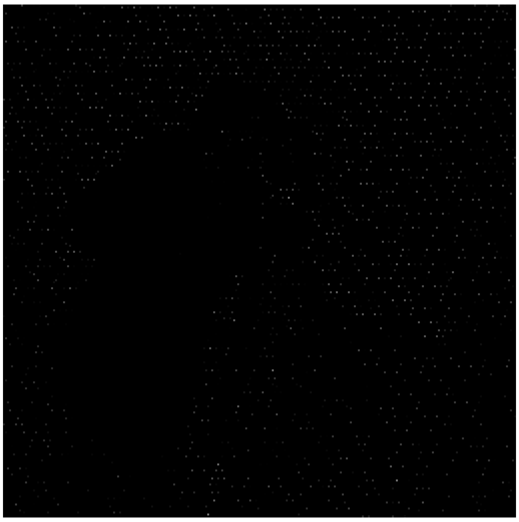

Figure.8.5.1 Contrast variation

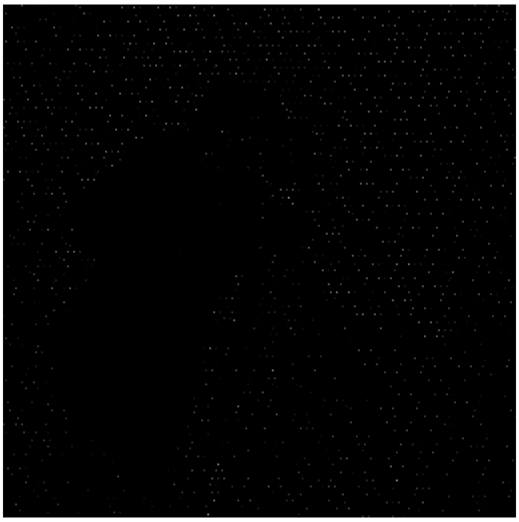

Figure.8.5.2 Addition of Gaussian white noise with 0 mean and 0.01 variance

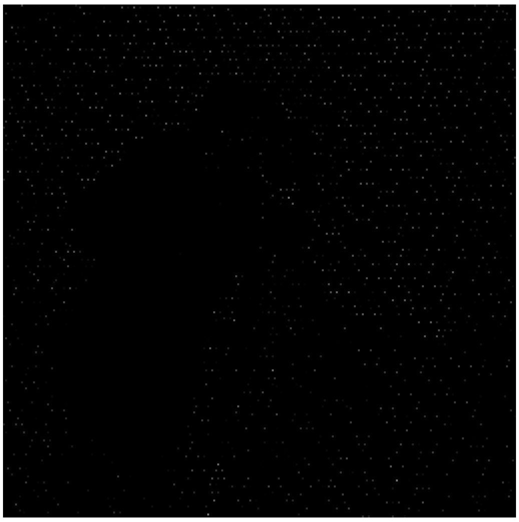

Figure.8.5.3 Histogram attack

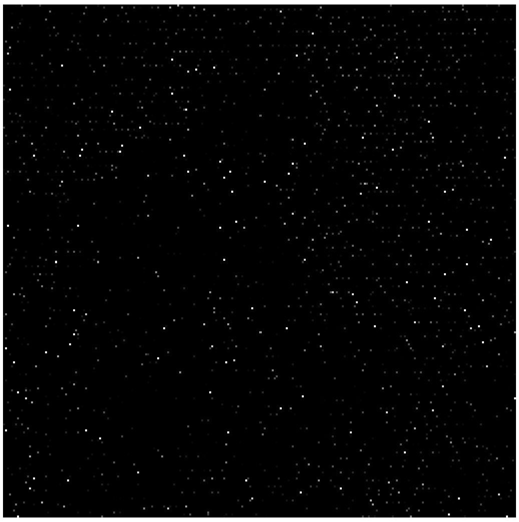

Figure.8.5.4 Sharpening effect

CHAPTER 9

APPLICATIONS

9.1 USAGE IN MODERN PRINTERS

Steganography is used by some modern printers, including HP and Xeroxbrand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

9.2 USE BY TERRORIST

When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once.

9.3 ALLEGED USE BY INTALLIGENCE SERVICES

In 2010, the Federal Bureau of Investigation show that the Russian foreign intelligence uses customized steganography software for embedding encrypted text messages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad.

9.4 CONFIDENTIAL COMMUNICATION AND SECRET DATA STORING

The "secrecy" of the embedded data is essential in this area.

Historically, steganography have been approached in this area. Steganography provides us with:

1. Potential capability to hide the existence of confidential data

2. Hardness of detecting the hidden (i.e., embedded) data

3. Strengthening of the secrecy of the encrypted data

In practice, when you use some steganography, you must first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the steganography software) together with some key. When extracting, you (or your party) extracting program (another component) to recover the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" before you start communication.

Attaching a stego file to an e-mail message is the simplest example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method.

There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System." See the reference.

There is some other communication method that uses the Internet Webpage. In this method you don't need to send anything to your party, and no one can detect your communication. Each secrecy based application needs an embedding process which leaves the smallest embedding evidence. You may follow the following.

1. Choose a large vessel, larger the better, compared with the embedding data.

2. Discard the original vessel after embedding.

For example, in the case of Qtech Hide & View, it leaves some latent embedding evidence even if the vessel has a very large embedding capacity. You are recommended to embed only 25% or less (for PNG / BMP output) of the maximum capacity, or only 3% of the vessel size (for JPEG output).

9.5 PROTECTION OF DATA ALTERATION

We take advantage of the fragility of the embedded data in this application area.We asserted in the Home Page that "the embedded data can rather be fragile than be very robust." Actually, embedded data are fragile in most steganography programs. Especially, Qtech Hide & View program embeds data in an extremely fragile manner.

However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

9.6 ACCESS CONTROL SYSTEM FOR DIGITAL CONTENT DISTRIBUTION

In this area embedded data is "hidden", but is "explained" to publicize the content. Today, digital contents are getting more and more commonly distributed by Internet than ever before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who accessed the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital content to e-mail messages and send to the customers. But it will takes a lot of cost in time and labor.

If you have some valuable content, which you think it is okay to provide others if they really need it, and if it is possible to upload such content on the Web in some covert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize a this type of system. We have developed a prototype of an "Access Control System" for digital content distribution through Internet. The following steps explain the scheme.

1. A content owner classify his/her digital contents in a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.

2. On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address, e-mail address, phone number, etc.) will be posted there.

3. The owner may receive an access-request from a customer who watched that Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged).

In this mechanism the most important point is, a "**selective extraction**" is possible or not.We have already developed such a selective extraction program to implement the system.

9.7 MEDIA DATABASE SYSTEMS

In this application area of steganography secrecy is not important, but unifying two types of data into one is the most important. Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.

1. The title of the picture and some physical object information.

2. The date and the time when the picture was taken.

3. The camera and the photographer's information.

Formerly, these are annotated beside the each picture in the album. Recently, almost all cameras are digitalized. They are cheap in price, easy to use, quick to shoot. They eventually made people feel reluctant to work on annotating each picture. Now, most home PC's are stuck with the huge amount of photo files. In this situation it is very hard to find a specific shot in the piles of pictures. A "photo album software" may help a little. You can sort the pictures and put a couple of annotation words to each photo. When you want to find a specific picture, you can make a search by keywords for the target picture. However, the annotation data in such software are not unified with the target pictures. Each annotation only has a link to the picture. Therefore, when you transfer the pictures to a different album software, all the annotation data are lost. This problem is technically referred to as "Metadata (e.g., annotation data) in a media database system (a photo album software) are separated from the media data (photo data) in the database managing system (DBMS)." This is a big problem.

Steganography can solve this problem because a steganography program unifies two types of data into one by way of embedding operation. So, metadata can easily be transferred from one system to another without hitch. Specifically, you can embed all your good/bad memory (of your sight-seeing trip) in each snap shot of the digital photo. You can either send the embedded picture to your friend to extract your memory on his/her PC, or you may keep it silent in your own PC to enjoy extracting the memory ten years after.

If a "motion picture steganography system" has been developed in the near future, a keyword based movie-scene retrieving system will be implemented. It will be a step to a "semantic movie retrieval system.

CHAPTER 10

CONCLUSION

In this, a steganography technique in the DWT domain is suggested and implemented using the MATLAB software. FRWT (Fractional wavelet transform)algorithm is used to embed secret data in low frequency range to achieve both robustness and higher security.

For maintaining higher security Arnold Transform is used. With the Arnold transform a image can be scrambled and using inverse Arnold transform we can receive the unscrambled image back. By using FRWT computational time will reduced. The measured performance of the technique proves its robustness against several kinds of image processing attacks. Hence it can serve as a best means to prove the authenticity and ownership of intellectual images. So, common methods of attack, experimental results and analysis show that the proposed algorithm is effective and can be used in a practical system.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, P. McKevitt, “Digital image steganography: Survey andanalysis of current methods,” Elevier.

[2] S. Bhattacharyya, I. Banerjee, G. Sanyal, “A survey of steganography and steganalysis technique in image, Text, Audio, and video as cover .carrier,” Journal of global research in computer science, vol. 2, no.4,Apr. 2011.

[3] C. K. Chan, L. M. Chang, “Hiding data in image by simple LSB substitution,” Pattern Recognition, vol. 37, pp. 469–471, 2003.

[4] C. C. Chang, C. L. Chiang, J.Y. Hsiao, “A DCT-domain System for Hiding Fractal Compressed Images,” In AINA’05, Proceeding of the19th international Conf. on Advanced Information Networking and Applications, 2005.

[5] C. Y. Lin, Y.T. Ching, “A Robust Image Hiding Method Using Wavelet Technique,” Journal of Information Science andEngineering, Vol. 22, pp. 163-174, 2006.

[6] A. A. Abdelwahab, A. L. Hassaan, “A Discrete Wavelet Transform based Technique for Image Data Hiding,” 25th National RadioConference, pp. 1–9, Egypt, 2008.

[7] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, “A Novel Technique for Image Steganograpy Based on DWT and Huffman Encoding, ”International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6),pp. 497-610,2011.

[8] T. Morkel, J.H.P. Eloff, and M.S. Oliver. “An overview of image steganography.” in Proc.ISSA, 2005, pp. 1-11.

[9] L. Chun-Shien. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. USA: Idea Group Publishing, 2005, pp. 1-253.

[10] R.J. Anderson and F.A.P. Petitcolas. (1998, May). “On the limits of steganography.” IEEE Journal of Selected Area in Communications. [On line]. 16(4), pp. 474-481.Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[11] I.J.Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert. “Digital watermarking and steganography.” USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[12] N.F. Johnson and S. Jajodia. (1998, Feb.). “Exploring steganography: seeing the unseen.” IEEE Computer Journal. [On line]. 31(2), pp. 26-34.

[13] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). “Digital image steganography: survey and analysis of current methods.” Signal Processing Journal. [On line]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[14] M. Fortrini. “Steganography and digital watermarking: A global view.” University of California,DavisAvailable:http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini /project.pdf. [June 2011].

[15] N. Provos and P. Honeyman. (2003, Jun.). “Hide and seek: An introduction to steganography.” IEEE Security and Privacy Journal. [On line], 1(3), pp. 32-44.Available: http://niels.xtdnet.nl/papers/practical.pdf [Jul., 2011].

[16] N.F. Johnson. (1995, Nov.). “Steganography. Technical report.”Available: http://www.jjtc.com/pub/tr_95_11_nfj/ [Sep., 2011].

[17]ID.Sellars.“Anintroductiontosteganography.Internet:http://www.cs.uct.ac.za/courses/CS400W/papers99/stego.html [Jul., 2011].

[18] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), “A survey of steganography techniques for image files.” Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

[19] M.S. Prasad, S. Naganjaneyulu, CH.G. Krishna, and C. Nagaraju. (2009, Oct.). “A novel

information hiding technique for security by using image steganography.” Journal of Theoretical and Applied Informaion Technology. [On line]. 8(1), pp. 35-39.

[20] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). “Image steganography: Conceptsand practice.” WSPC/Lecture Notes Series: 9in x 6in, [On line], pp. 1-49. Available: http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf [Aug. 2011].

[21] B. Li, J. He, J. Huang, and Y.Q. Shi. (2011, Apr.). “A survey on image steganography and steganalysis.” Journal of Information Hiding and Multimedia Signal Processing. 2(2), [On line], pp. 142-172. Available: http://bit.kuas.edu.tw/~jihmsp/2011/vol2/JIH-MSP-2011-03-005.pdf [Dec., 2011].

[22] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. (1996). “Techniques for data hiding.” IBM System Journal. 35(3/4), [On line], pp. 313-336.

[23] M. Juneja and P.S. Sandhu. “Designing of robust image steganography technique based on LSB insertion and encryption.” IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.

[24] N. F. Johnson, S. Katzenbeisser. “A Survey of steganographic techniques.” in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[25] K. Curran and K. Baily. (2006, Jul.). “An evaluation of image based steganography methods.” Multimedia Tools and Applications Journal. [On line]. 30(1), pp. 55-88. Available: http://dl.acm.org/citation.cfm?id=1164470 [May, 2011].

[26] A.R. Naghsh-Nilchi, L. Pourmohammadbagher. (2006, Jun.). “A new approach to steganography using sinc-convolution method.” PWASET Journal. [On line]. 14(1), pp. 324-329. Available: http://www.waset.org/journals/waset/v20/v20-4.pdf [May, 2011].

[27] D.L. Currie and C.E. Irvine. “Surmounting the effects of lossy compression on steganography.” in Proc. of the 19th National Information Systems Security Conference, 1996, pp. 194-201.

[28] A. Westfeld. “F5-A steganographic algorithm: high capacity despite better steganalysis.” In Proc. of the 4th Information Hiding Workshop, LNCS, 2001, pp. 289-302.

[29] A. Westfeld and A. Pfittzmann. “Attacks on steganographic systems- breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned.” in Proc. of the 3rd Internet Workshop on Information Hiding, 1999, pp. 61-76.

[30] N. Provos. “Defending against statistical steganalysis.” in Proc. of the 10th USENIX Security Symposium, 2001, pp. 323-325.

[31] P. Sallee. “Model-based steganography.” in Proc. the 2nd International Workshop on Digital Watermarking, LNCS, 2004. pp. 254-260.

[32] K. Solanki and B.S. Manjunath. “Yass: Yet another steganographic scheme that resists blind steganalysis.” in Proc. of the 9th Information Hiding Workshop, LNCS, 2007. pp. 1-16.

[33] H.S. Majunatha Reddy and K.B. Raja. (2009). “High capacity and security steganography using discrete wavelet transform.” International Journal of Computer Science and Security.

[34] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. “Exploring on steganography for low bit rate Wavelet based coder in image retrieval system.” in Proc. of IEEE TENCON, 2000. pp. 250-255.

[35] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. “Steganography for low bitrate Wavelet based image coder.” in Proc. of IEEE ICIP, 2000. pp. 597-600.

[36] N.K. Abdulaziz and K.K. Pang. “Robust data hiding for images.” in Proc. of IEEE International Conference on Communication Technology, 2000. pp. 380-383.

[37] L.D. Paulson. (2006, Aug.). “New system fights steganography. News briefs.” IEEE Computer Society. [On line]. 39(8), pp. 25-27.

[38] A.A. Abdelwahab and L.A. Hasan. “A discrete Wavelet Transform based technique for image data hiding.” in Proc. of 25th National Radio Science Conference, 2008. pp. 1-9.

[39] J.R. Smith and B.O. Comiskey. “Modulation and information hiding in images.” in Proc. of the 1st Information Hiding Workshop, 1996. pp. 207-226.

[40] H. Wang and S. Wang. (2004, Oct.). “Cyber Warfare: steganography vs. steganalysis.” Communications of the ACM. [On line]. 47(10), pp. 76-82. Available: www.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf [Mar., 2011].

[41] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. (1999). “Spread spectrum image steganography.” IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083. Available: http://www.mendeley.com/research/spread-spectrum-image-steganography-1/ [Apr., 2011].

[42] C.L.Tsai, K.C. Fan, and C.D. Chung. “Secure information by using digital data embedding and spread spectrum techniques.” IEEE 35th International Carnahan Conference on Security Technology, 2001. pp. 156-162.

[43] F.Alturki and R.Merserau. “Secure blind image steganographic technique using Discrete Fourier Transform.” in Proc. IEEE International Conference on Image Processing, 2001. pp. 16-162.

[44] M. Gkizeli, D.A., and M.J. Medley. (2007, Feb.). “Optimal signature design for spreadspectrum steganography.” IEEE Signal Processing Society. [On line]. 16(2), pp. 391-405. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4060938 [Oct. 2011].