P-3497

IMAGE STEGANOGRAPHY USING BIOMETRICS

By

M.NARMADHA DEVI

Reg. No. 0920107011

of

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution affiliated to Anna University of Technology, Coimbatore)

COIMBATORE - 641 049

A PROJECT REPORT

Submitted to the

FACULTY OF ELECTRONICS AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements

for the award of the degree

of

MASTER OF ENGINEERING

IN

COMMUNICATION SYSTEMS

APRIL 2011

BONAFIDE CERTIFICATE

Certified that this project report titled "**IMAGE STEGANOGRAPHY USING BIOMETRICS**" is the bonafide work of **Ms.M.Narmadha Devi** [Reg. No 0920107011] who carried out the research under my supervision. Certified further that, to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

07-04-2011

Project Guide

Dr.A.Vasuki

7/4/11

Head of the Department

Dr.Rajeswari Mariappan

The candidate with Register No. 0920107011 is examined by us in the project viva-voce examination held on ...21.4.2011...

D. 21/4/11

Internal Examiner

21/4/11

External Examiner

ACKNOWLEDGEMENT

First I would like to express my praise and gratitude to the Lord, who has showered his grace and blessing enabling me to complete this project in an excellent manner.

I express my sincere thanks to our beloved Director **Dr.J.Shanmugam**, Kumaraguru College of Technology, for his kind support and for providing necessary facilities to carry out the work.

I express my sincere thanks to our beloved Principal **Dr.S.Ramachandran**, Kumaraguru College of Technology, who encouraged me in each and every steps of the project work.

I would like to express my deep sense of gratitude to our HOD, **Dr.Rajeswari Mariappan**, Department of Electronics and Communication Engineering, for her valuable suggestions and encouragement which paved way for the successful completion of the project work.

In particular, I wish to thank with everlasting gratitude to the project coordinator **Ms.D.Mohanageetha (Ph.D)**, Associate Professor, Department of ECE, for her expert counseling and guidance to make this project to a great deal of success.

I am greatly privileged to express my heartfelt thanks to my project guide **Dr.A.Vasuki**, Professor, Department of ECE, throughout the course of this project and I wish to convey my deep sense of gratitude to all the teaching and non-teaching staffs of ECE Department for their help and cooperation.

Finally, I thank my parents and family members for giving me the moral support and abundant blessings in all of my activities and my dear friends who helped me to endure my difficult times with their unfailing support and warm wishes.

ABSTRACT

The advancements in multimedia communication through Internet have made the security of information as one of the important concerns in information technology and communication. Many data hiding techniques have been developed recently to protect digital audio, video and images. Steganography, Watermarking and Cryptography are the data hiding techniques that have potential applications for copyright protection, hiding executables for access control of digital multimedia data, secret communication, tamper detection etc. Steganography is the art and science of invisible communication that hides the existence of information in another transmission medium. Many steganographic methods are available for hiding the secret information in the cover medium. Image steganography is used to hide the secret image in the cover image. In this project, secret data is embedded using biometric feature i.e. within skin tone region of image that will provide an excellent secure location for data hiding. Skin tone detection will be performed using Hue, Saturation and Brightness Value color space. Secret data will be hidden in one of the high frequency subbands of the wavelet transformed image by tracing skin pixels in that subband. By adopting an object oriented steganography mechanism, a higher security will be obtained. Peak-Signal-to-Noise Ratio is the performance measure that is used to quantify the distortion in the stego image.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	**iv**
	LIST OF FIGURES	**vii**
	LIST OF TABLES	**ix**
	LIST OF ABBREVIATIONS	**x**
1	**INTRODUCTION**	**1**
	1.1 Cryptography	1
	1.2 Watermarking	2
	1.3 Steganography	3
	1.4 Characterizing data hiding techniques	6
	1.4.1 Hiding Capacity	6
	1.4.2 Perceptual Transparency	6
	1.4.3 Robustness	6
	1.4.4 Tamper Resistance	6
	1.4.5 Other Characteristics	6
2	**STEGANOGRAPHY TECHNIQUES**	**8**
	2.1 Steganography in Spatial Domain	8
	2.2 Steganography In Frequency Domain	10

2.2.1 Fast Fourier Transform 10

2.2.2 Discrete Cosine Transform 11

2.2.3 Discrete Wavelet Transform 12

2.3 Adaptive Steganography 13

2.4 Applications of Steganography 14

3 **PROPOSED METHODOLOGY** **17**

3.1 Skin Color Tone Detection 17

3.2 Discrete Wavelet Transform 19

3.3 Embedding Process 21

3.4 Implementation Steps 24

3.5 Extraction Process 25

3.6 JPEG Compression 27

3.7 Performance Measure 28

4 **RESULTS AND DISCUSSION** **30**

5 **CONCLUSION** **47**

REFERENCES

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
1.1	Different embodiment disciplines of information hiding	2
1.2	Basics of Steganography	3
2.1	Steganography in spatial domain	8
2.2	General process of embedding in DCT domain	12
3.1	Horizontal operations on the first row	20
3.2	Vertical operation	20
3.3	Flowchart.of Embedding Process	22
3.4	Raster scan order for embedding	23
3.5	Flowchart of Extraction Process	26
4.1	Secret Images to be hidden (a) Lena (b) Rice	30
4.2	Cover Images (a) Lena (b) Baby (c) Man (d) Girl	31
4.3	Mask Images (a) Lena (b) Baby (c) Man (d) Girl	32
4.4	Cropped Mask (a) Lena (b) Baby (c) Man (d) Girl	33
4.5	Cropped Cover Images	
	(a) Lena (b) Baby (c) Man (d) Girl	34
4.6	DWT of Cover Images	
	(a) Lena (b) Baby (c) Man (d) Girl	35

4.7 Cropped Stego Images

(a) Lena (b) Baby (c) Man (d) Girl 36

4.8 Final Stego Images

(a) Lena (b) Baby (c) Man (d) Girl 37

4.9 Retrieved Secret Images (a) Rice from Lena

(b) Rice from Baby (c) Rice from Man (d) Lena from Girl 38

4.10 Stego Images in DCT domain 43

4.11 Compressed Stego images

(a) Lena (b) Baby (c) Man (d) Girl 45

LIST OF TABLES

TABLE NO	TITLE	PAGE NO
1.1	Comparison of Steganography, Watermarking and Encryption	5
3.1	Sequence Mapping Table	23
4.1	Embedding the secret image (64 ×64) in B plane	39
4.2	Embedding the secret image (128 ×128) in B plane	40
4.3	Embedding the secret image (64 ×64) in G plane	40
4.4	Embedding the secret image (128×128) in G plane	41
4.5	Embedding the secret image (64 ×64) in R plane	41
4.6	Embedding the secret image (128×128) in R plane	42
4.7	Comparison of stego images in DCT domain and DWT domain	44
4.8	Performance Measure of JPEG Compression	46

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
BMP	Bit Map Format
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DSP	Digital Signal Processing
DWT	Discrete Wavelet Transform
ECG	Electrocardiogram
EPR	Electronic Patient Records
FFT	Fast Fourier Transform
GIF	Graphics Interchange Format
HH	High High
HL	High Low
HSV	Hue Saturation and Brightness Value
HVS	Human Visual System
JPEG	Joint Photographic Experts Group
LBG	Linde Buzo Gray
LH	Low High
LL	Low Low
LSB	Least Significant Bit
MSE	Mean Square Error

PSNR	Peak Signal to Noise Ratio
QIM	Quantization Index Modulation
ROI	Region Of Interest
RSA	Rivest Shamir Adleman
STD	Standard Deviation

CHAPTER 1

INTRODUCTION

With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. Since it is a worldwide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. However, message transmissions over the internet still have to face all kinds of security problems. Therefore, how to protect secret messages during transmission becomes an essential issue for the internet. This has driven the interest among computer security researchers to overcome the serious threats for secured data transmission. One method of providing more security to data is information hiding.

Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA). These methods scramble the secret message so that it cannot be understood by the unintended observer. However, it makes the message suspicious enough to attract eavesdropper's attention. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. Hence, a new scheme, called "steganography" arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files) so that it cannot be observed. Steganography differs from cryptography. Cryptography focuses on concealing the contents of a message, where as steganography focuses on concealing the existence of a message [1].

1.1 Cryptography

Cryptography is a technique, where the cover message is scrambled after information hiding using certain methodology which is accepted by the two parties in order to send the data securely. The scrambled message is transformed into another form using a secret key, known as the cipher text. Then, the cipher text is sent through the network to the recipient. At the receiver side, the same key is used to decrypt the secret information. In this technique, the intruders can easily suspect the hidden information in the cipher text. Even if, they couldn't retrieve the secret information, they can easily tamper the cipher text which will destroy the hidden information.

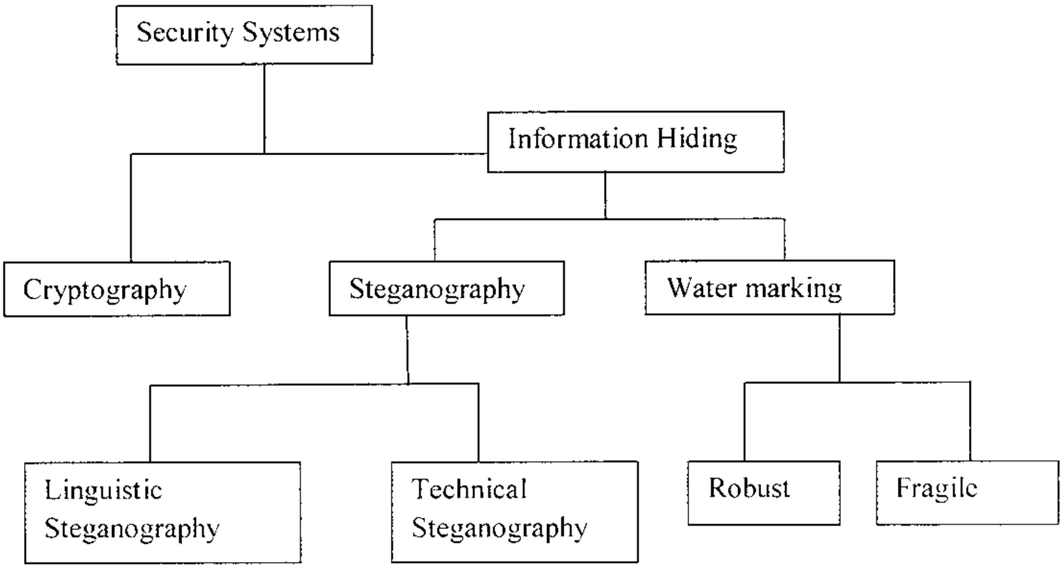


Figure 1.1 Different embodiment disciplines of information hiding

1.2 Watermarking

Watermarking is a protecting technique which protects the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. It should be impossible to remove the watermark that is being embedded within the image without degrading the image quality. A watermark is embedded in the original data using the embedding algorithm and a secret key. The embedded watermark may be visible or invisible watermark. A detection algorithm using the appropriate detection method can retrieve the watermark information. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself.

1.3 Steganography

Steganography is the art and science of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. The word "steganography" in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing"). The main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer i.e., unwanted parties should not be able to distinguish in any sense between cover-image (image not containing any secret message) and stego image (modified cover-image that containing secret message). Thus, the stego image should not deviate much from original cover image. Today, steganography is mostly used in computers with digital data being the carriers and networks being the high speed delivery channels.

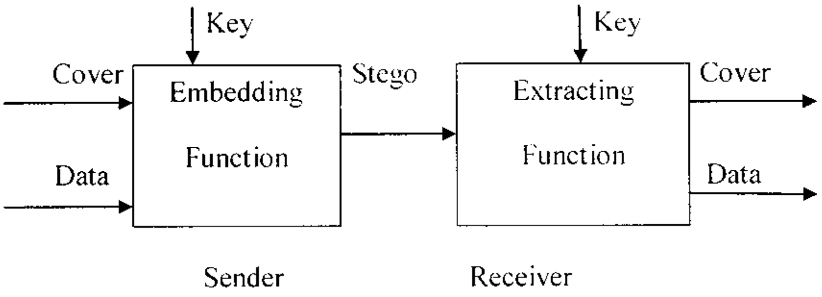


Figure 1.2 Basics of Steganography

Cover - Cover data in which secret data will be hidden

Data - Message to be hidden

Key - Parameter to be inserted for encryption

Stego - Cover data with the hidden message

The information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message [2].

A classical steganographic system's security relies on the encoding system's secrecy. An example of this type of system is a Roman general, who shaved a slave's head and tattooed a message on it. After the hair grew back, the slave was sent to deliver the now-hidden message. Although such a system might work for a time, once it is known, it is simple enough to shave the heads of all the people passing by to check for hidden messages. This led to the failure of classical steganographic system. Later, modern steganography attempts to be detectable only if secret key is known.

Three different aspects in information-hiding systems contend with each other:

- Capacity
- Security
- Robustness

Capacity refers to the amount of information that can be hidden in the cover medium; Security to an eavesdropper's inability to detect hidden information; Robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

The comparison of the three data hiding techniques namely Steganography, Watermarking and Encryption is given in Table 1.1

Table 1.1 Comparison of Steganography, Water marking and Encryption

Criteria /Method	Steganography	Watermarking	Encryption
Carrier	Any digital media	Mostly image/audio files	Usually text based with some extension to image files
Secret data	Payload	Watermark	Plain text
Key	Optional	Necessary	Necessary
Input files	At least two unless in self-embedding	Two	One
Detection	Blind	Informative(Original cover /water mark is necessary - recovery)	Blind
Authentication	Full retrieval of data	Usually achieved by cross correlation	Full retrieval of data
Objective	Secret communication	Copyright preserving	Data protection
Result	Stego-file	Water marked file	Cipher text
Concern	Detectability/capacity	Robustness	Robustness
Type of attacks	Steganalysis	Image processing	Cryptanalysis
Visibility	Never	Sometimes	Always
Fails when	It is detected	It is removed/replaced	Deciphered
Relation to cover	Not related to the cover. Message is more important than the cover image	Usually becomes an attribute of the cover image,more important than the message	Not Available
Flexibility	Free to choose any suitable cover.	Cover choice is restricted	Not Available
History	Very ancient except its digital version	Modern era	Modern era

1.4 Characterizing data hiding techniques

Various features characterize the strengths and weaknesses of the steganographic methods. The relative importance of each feature depends on the application [3].

1.4.1 Hiding Capacity

Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size, and thus decreases the bandwidth required to transmit the stego image.

1.4.2 Perceptual Transparency

In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stego image, the steganographic encoding has failed even if the attacker is unable to extract the message. Preserving perceptual transparency in an embedded watermark for copyright protection is also of paramount importance because the integrity of the original work must be maintained.

1.4.3 Robustness

Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion from digital to analog form and then reconversion back to digital form.

1.4.4 Tamper Resistance

Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego image, such as a pirate replacing a copyright mark with one claiming legal ownership. Applications that demand high robustness usually also demand a strong degree of tamper resistance.

1.4.5 Other Characteristics

Computational complexity of encoding and decoding is another consideration and individual applications may have additional requirements.

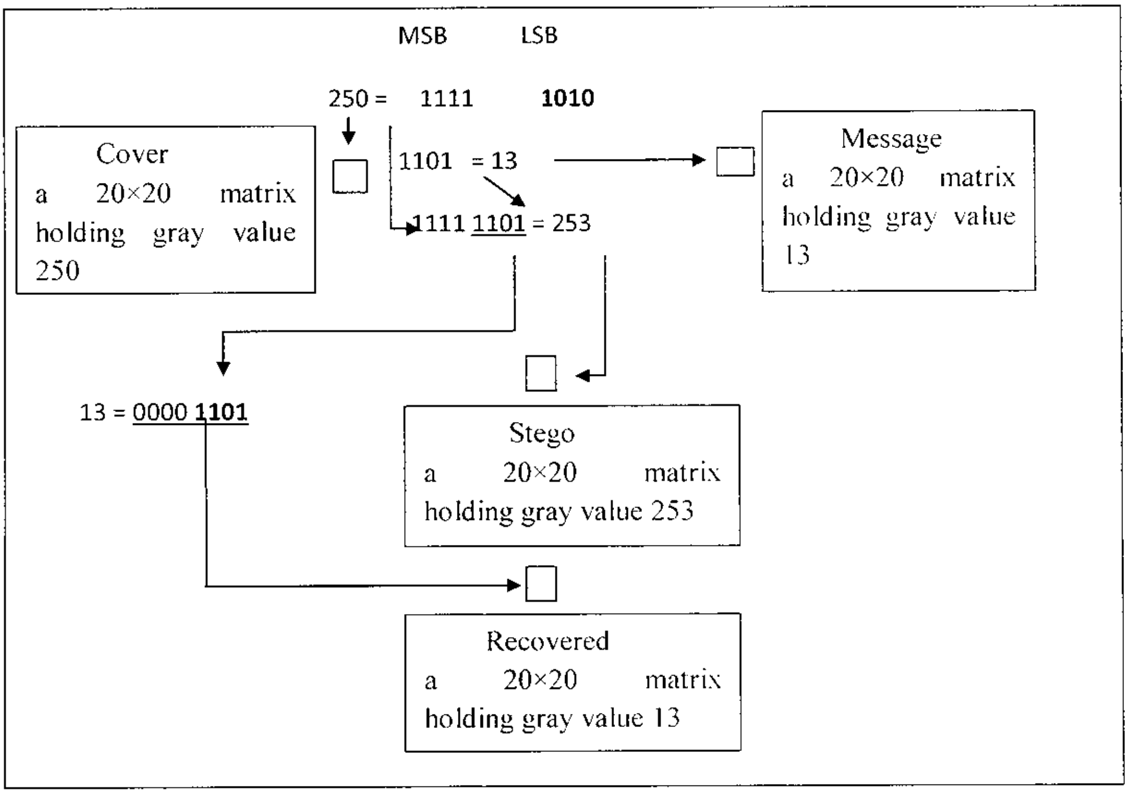
Chapter 2 deals with the steganography and its applications. Chapter 3 demonstrates the proposed methodology. Results and Discussion are given in Chapter 4. Finally, Conclusion is given in Chapter 5.

CHAPTER 2
STEGANOGRAPHY TECHNIQUES

Image steganographic techniques can be classified on the basis of the domains in which data is embedded. Basically there are two domains: the spatial domain and the transform domain. Steganographic techniques try to embed data in these domains.

2.1 Steganography in Spatial Domain

In the spatial domain image steganography, the simplest technique is to embed data in the Least Significant Bit of each pixel in the cover image. The LSB Replacement technique alters the insignificant information in the cover image.



MSB LSB
250 = 1111 1010
Cover
a 20×20 matrix holding gray value 250
1101 = 13
1111 1101 = 253
Message
a 20×20 matrix holding gray value 13
13 = 0000 1101
Stego
a 20×20 matrix holding gray value 253
Recovered
a 20×20 matrix holding gray value 13

Figure 2.1 Steganography in spatial domain

There are two types of LSB insertion methods: fixed-sized and variable-sized. The former embeds the same number of message bits in each pixel of the cover-image, whereas the latter embeds a random number of bits per pixel. In spatial domain methods, a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs.

Potdar [4] used a spatial domain technique in producing a fingerprinted secret sharing steganography for robustness against image cropping attacks. This paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub images and compress and encrypt the secret data. Polynomial was applied along with an encryption algorithm. The confidential data is initially preprocessed i.e. encrypted and compressed. The resulting data is then sub divided in turn and embedded into those image portions. The confidential data is now split into multiple data segments of equal size, and each of these segments undergoes mathematical processing and is finally embedded in the sub image. Here, secret sharing scheme is used to process the data segments. The processed data segments are now encrypted using the intended recipient's public key and finally embedded in the sub-images.

The embedding can be done by using any steganographic algorithm. A fingerprint function is now applied to the stego sub-images to check the integrity of the stego samples. To recover the data, a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The (k,n) threshold scheme was used to decide the minimum number of parts required to recover the secret data completely.

Li [5] propose lossless data hiding using the difference value of adjacent pixels. It is classified under "±1" data embedding algorithms. It exploits the correlation between adjacent pixels that results in a compact histogram characterized by a normal Gaussian distribution. The pixel difference, whose absolute value equals to threshold δ, is used to embed secret data. Before data embedding, the differences are modified to obtain extra space from the embedding procedure that the capacity of this method equals to the number of difference with value of ±δ.

Based on the assumption, there is no pixel with overflow and underflow in the embedding phase. In the worst case, all pixels are altered by 1. Alien to the embedding sequence, hidden data is acted reversely, from right to left in each row. At first, the location and grayscale value of pixels which equal to 0 or 255 is preserved, and reset them to 1 or 254 respectively. Then, compress this overhead information without loss and append it to the hidden data. As a result, the actual embedding capacity (pure payload) is less than or equal to the maximum size of embedded data. In this way, the overflow/underflow of pixels is prevented and restored the original image without any loss.

A novel steganographic method based on LSB replacement and Pixel Value Differencing (PVD) method is presented. First, a different value from two consecutive pixels by utilizing the PVD method is obtained. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess [10].

2.2 Steganography in Frequency Domain

The transform of a signal is another form of representing this signal. It does not change the information content present in it. The steganography can be implemented in Fast Fourier Transform, Discrete Cosine Transform and Discrete Wavelet Transform.

2.2.1 Fast Fourier Transform

In most Digital Signal Processing (DSP) applications, frequency content of the signal is very important. The Fourier Transform (FT) is probably the most popular transform used to obtain the frequency spectrum of a signal. But, the Fourier Transform is only suitable for stationary signals, i.e., signals whose frequency content does not change with time. The Fourier Transform, while it tells how much of each frequency exists in the signal, it does not tell at which time these frequency components occur. Fast Fourier Transform (FFT) methods introduce round off errors. It is not suitable for hidden communication.

P-3497

2.2.2 Discrete Cosine Transform

People often transmit digital pictures over email and other Internet communication. JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks. Visual attacks mean that one can see steganographic messages on the low bit planes of an image because they overwrite visual structures, this usually happens in BMP images. JPEG images acts as a vehicles to embed the data. JPEG compression uses the DCT to transform successive sub-image blocks (8× 8 pixel) into 64 coefficients. Data is inserted into these coefficients' insignificant bits. Altering any single coefficient would affect the entire 64 block pixels [7].

For each color component, the JPEG image format uses a discrete cosine transform to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients $F(u, v)$ of an 8 × 8 block of image pixels $f(x, y)$ are given by

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

MAHATMA GANDHI • CENTRAL LIBRARY • KCT CBE-6

Where $C(x) = 1/\sqrt{2}$ when x equal 0 and $C(x) = 1$ otherwise. The least-significant bits of the quantized DCT coefficients are used as redundant bits in which to embed the hidden message. The modification of a single DCT coefficient affects all 64 image pixels. In some image formats (such as GIF), an image's visual structure exists to some degree in all the image's bit layers [8]. Steganographic systems that modify least-significant bits of these image formats are often susceptible to visual attacks. This is not true for JPEGs. The modifications are in the frequency domain instead of the spatial domain, so there are no visual attacks against the JPEG image format.

The steganography based on DCT JPEG compression goes through different steps as shown in the following Figure 2.2.

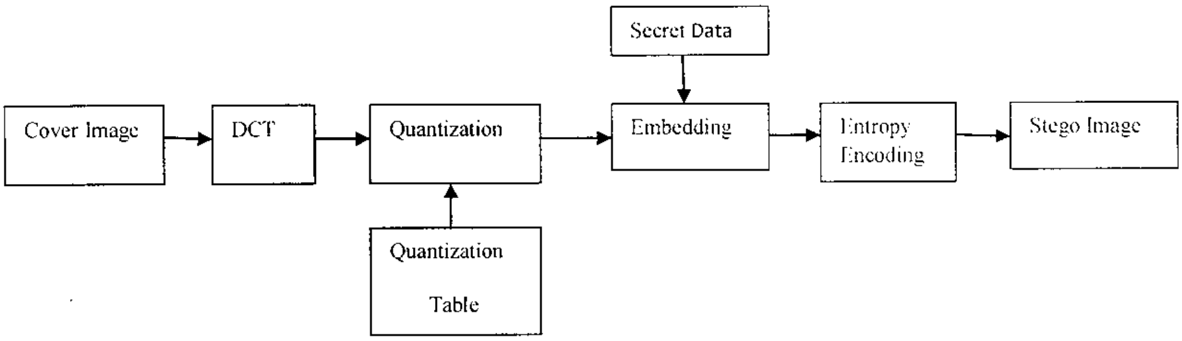


Figure 2.2 General process of embedding in DCT domain

DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT.

2.2.3 Discrete Wavelet Transform

Signals such as image or speech have different characteristics at different space or time, i.e., they are non-stationary. Most of the biological signals too, such as, Electrocardiogram, Electromyography, etc., are non-stationary. To analyze these signals, both frequency and time information are needed simultaneously, i.e., a time-frequency representation of the signal is needed. The Wavelet Transform provides a time-frequency representation of the signal. It uses multi-resolution technique by which different frequencies are analyzed with different resolutions. DWT has spatial frequency locality, which means if signal is embedded it will affect the image locally. Hence a wavelet transform provides both frequency and spatial description for an image.

Abdulaziz and Pang [9] use vector quantization called Linde-Buzo-Gray (LBG) coupled with block codes known as BCH code and 1-stage discrete Haar wavelet transforms. They reaffirm that modifying data using a wavelet transformation preserves good quality with little perceptual artifacts.

Abdelwahab and Hassan [10] propose a data hiding technique in the DWT domain. Both secret and cover images are decomposed using DWT (1st level). Each of divided into disjoint 4×4 blocks. Blocks of the secret image fit into the cover blocks to determine the best match. Error blocks are generated and embedded into coefficients of the best matched blocks in the HL of the cover image. Two keys must be communicated; one holds the indices to the matched blocks in the LL band of the cover image and another for the matched blocks in the HL of the cover image. The extracted payload is not totally identical to the embedded version as the only embedded and extracted bits belong to the secret image approximation while setting all the data in other sub-images to zeros during the reconstruction process.

2.3 Adaptive Steganography

Adaptive steganography is a special case of the two former methods. It is also known as "Statistics-aware embedding", "Masking" or "Model-Based". This method takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The statistics will dictate where to make the changes. It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD. The latter is meant to avoid areas of uniform color (smooth areas).

The wavelet transforms map integers to integers instead of using the conventional wavelet transforms [11]. This can overcome the difficulty of floating point conversion that occurs after embedding. This scheme embeds the payload in non overlapping 4×4 blocks of the low frequency, where two pixels at a time are chosen, one on either side of the principal diagonal. Cover image adjustments was required to prevent the problem of under/overflow of pixel values after embedding.

An adaptive data hiding method divides the host image in suitable and ineligible blocks. This classification is based on the DCT energy features from the synchronization horizontal, vertical and diagonal frequency information. Only the suitable blocks are used for data embedding using Quantization Index Modulation (QIM) [12].

An adaptive approach to steganography based on skin tone detection is implemented [13]. If rotation or translation applied to stego image, all of the hidden data will be lost. The remedy to this problem is by finding clusters of skin areas in the image 3D space. Based on experimentation, it is found that embedding into these regions produces less distortion to the carrier image compared to embedding in a sequential order or in any other areas. Such phenomena result from the fact that the eye does not respond with equal weight of sensitivity to all visual information. Human presence in digital photography and video files encourages such an approach. Typically, targeting specific regions would yield a reduction in space available for embedding, but comes at the benefit of robustness and perception. The embedding takes place in the 1st-level 2D Haar DWT with the symmetric-padding mode to resist noise impulse and compression. Algorithms based on DWT experience some losses of data since the reverse transform truncates the values if they go beyond the lower and upper boundaries (i.e., 0-255). Knowing that human skin tone resides along the middle range in the chromatic red of YC_bC_r color space allows us to embed in the DWT of the Cr channel. This would leave the perceptibility of the stego-image virtually unchanged since the changes made in the chrominance will be spread among the RGB colors when transformed.

2.4 Applications of Steganography

Steganography is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video–audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users), and also checksum embedding.

Steganographic techniques are applicable in many fields are as follows:

Military and intelligence agencies require unobtrusive communications. Even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaler. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard for the enemy to detect or jam.

Steganography may be used to communicate over public networks such as the Internet. One may embed bits into inconspicuous files that are routinely sent over such networks: images, video, audio files, etc. Users of such technology may include intelligence and military personnel, people that are subject to censorship, and more generally, people who have a need for privacy.

Steganography may also used to communicate over private networks. For instance, confidential documents within a commercial or governmental organization could be marked with identifiers that are hard to detect. The purpose is to trace unauthorized use of a document to a particular person who received a copy of this document. The recipient of the marked documents should not be aware of the presence of these identifiers.

Timing channels can be used to leak out information about computers. A pirate could modify the timing of packets sent by the computer, encoding data that reside on that computer. The pirate wishes to make this information leakage undetectable to avoid arousing suspicion. To disrupt potential leakage, the network could jam packet timings – hence, the network plays the role of an active warden.

Petticolas [14] demonstrated some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. A link must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure.

Medical records of patients are extremely sensitive information, needing uncompromising security during both storage and transmission. In addition, these records often have to be traceable to patient medical data such as X-ray or scan (CAT, MRI etc.) images.

It is an enabling technology to transmit Electronic Patient Records (EPR) across distances to hospitals and countries through the Internet. However, since EPR is a highly personal medical documentation, transmission of secure EPR is required to reduce the risk of security breach on the network and prevent accessing of data by unauthorized end-users. A bi-polar multiple-base data hiding technique is proposed in [15], where a pixel value difference between an original image and its default JPEG lossy decompressed image is taken to be a number conversion base. Doctors' digital seals and the EPR data is hidden within a still image by using this approach. The still image could be the mark of a hospital to identify where the EPR comes from. The doctors' digital seals are essential to the authentication of EPR A diagnostic report and a biomedical signal such as electrocardiogram (ECG) can also be hidden in the image. This approach allows multiple data types to be hidden in the same image. All the data can be separated and restored perfectly by intended users.

CHAPTER 3

PROPOSED METHODOLOGY

Most of the works done on steganography in the literature have neglected the facts that object oriented steganography can strengthen the embedding robustness. Recognizing and tracking elements in a given carrier while embedding can help survive major image processing attacks and compression. This manifests itself as an adaptive intelligent type where the embedding process affects only certain Regions Of Interest (ROI) rather than the entire image.

Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS. This takes advantage of Biometrics features such as skin tone, instead of embedding data anywhere in image; data will be embedded in selected regions [16].

At first skin tone detection is performed on input image using HSV color space. Secondly cover image is transformed in frequency domain. This is performed by applying Haar DWT, the simplest DWT on image leading to four subbands. Finally, secret data embedding is performed in one of the high frequency subband by tracing skin pixels in that band. Before performing all steps cropping on input image is performed and then in only cropped region embedding is done, not in whole image. Cropping results in more security than without cropping. The cropped region works as a key at the decoding side. Here, embedding process affects only certain ROI rather than the entire image. So utilizing objects within images can be more advantageous. This is also called as Object Oriented steganography.

3.1 Skin Color Tone Detection

A skin detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a decision boundary of the skin color class in the color space. Therefore, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination [17].

Another challenge comes from the fact that many objects in the real world might have skin-tone colors. This causes any skin detector to have much false detection in the background if the environment is not controlled. The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. There exists several color spaces. Mainly, two kinds of color spaces are exploited in the biometrics which are HSV and Yellow, Chromatic Blue, Chromatic red (YC_bC_r) spaces. Color space used for skin detection in this work is HSV.

Normal color image is a three dimensional picture. Within a standard RGB image, there is a dimension containing only red values, a dimension containing only green values, a dimension containing only blue values. These RGB dimensions naturally mix together to produce full visible color spectrum. Any color image of RGB color space can be easily converted into HSV color space (i.e. separate dimensions of Saturation, Huc & Value of Intensity). HSV can be obtained by applying a non-linear transformation to the RGB color space as shown in Eq. 3.1

$$H = \begin{cases} h, & B \leq G \\ 2\pi\text{-}h. & B > G \end{cases}$$

where,

$$h = \cos^{-1} \frac{\tfrac{1}{2}\,[(R-G) + (R-B)]}{\sqrt{[(R-G)^{2} + (R-G)\,(R-B)]}}$$

$$S = \frac{\max(R, G, B) - \min(R, G, B)}{\max\,(R,G,B)}$$

$$V = \max\,(R, G, B) \qquad (3.1)$$

3.2 Discrete Wavelet Transform

This is another frequency domain in which steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT. DWT applies on cropped image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called subbands known as

LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically high pass
HL - Horizontally high pass and vertically low pass
HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL subband), secret message is hidden in other three parts without making any alteration in LL subband. As other three subbands are high frequency subband they contain insignificant data. Hiding secret data in these subbands doesn't degrade image quality that much. DWT used in this work is Haar-DWT; the simplest DWT. Equation for Haar wavelet is given in Eq 3.2

$$W_H(x) = \begin{cases} 1 & 0 < x < 1/2 \\ -1 & ½ < x < 1 \\ 0 & \text{otherwise} \end{cases} \tag{3.2}$$

A 2-dimensional Haar-DWT is a separable transform and it consists of two operations: One is the horizontal operation along the row and the other is the vertical along the column. Detail procedures of a 2-D Haar-DWT are described as follows:

At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 3.1.

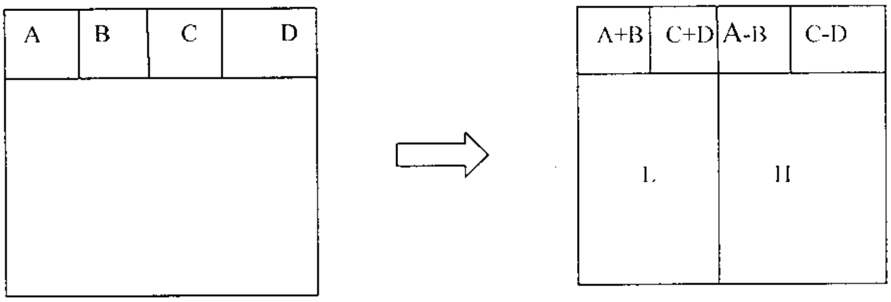


Figure 3.1 Horizontal operations on the first row

Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 3.2. Repeat this operations until all the columns are processed.

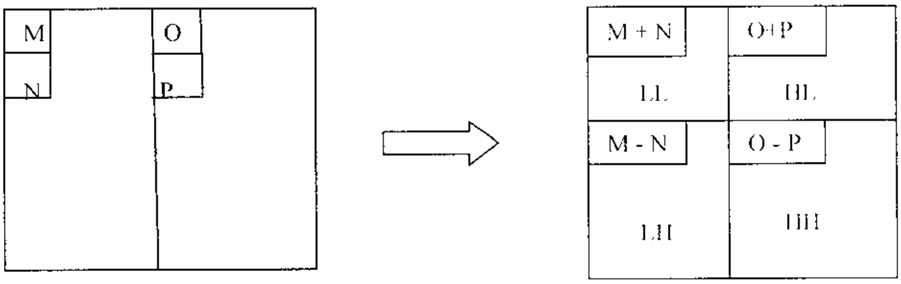


Figure 3.2 Vertical operation

Finally 4 subbands denoted as LL, HL, LH, and HH are obtained respectively. The LL subband is the low frequency portion and hence looks very similar to the original image. The whole procedure described above is called the first order 2-D Haar DWT.

The Haar wavelet transform has a number of advantages:

- Conceptually simple
- Fast
- Memory efficient, since it can be calculated in place without a temporary array
- Exactly reversible without the edge effects that are a problem with other wavelet transforms

The Haar transform also has limitations, which can be a problem for some applications.

In generating each set of averages for the next level and each set of coefficients, the Haar transform performs an average and difference on a pair of values. Then the algorithm shifts over by two values and calculates another average and difference on the next pair.

The high frequency coefficient spectrum should reflect all high frequency changes. The Haar window is only two elements wide. If a big change takes place from an even value to an odd value, the change will not be reflected in the high frequency coefficients.

3.3 Embedding Process

Suppose C is original 24-bit color cover image of M×N Size. It is denoted as:

$$C= \{x_{ij}, y_{ij}, z_{ij} \mid 1 \leq i \leq M,\ 1 \leq j \leq N,\ x_{ij}, y_{ij}, z_{ij} \in \{0,1,..,255\}\} \qquad (3.3)$$

Let size of cropped image is $M_c \times N_c$ where $M_c \leq M$ and $N_c \leq N$ and $M_c = N_c$. i.e. Cropped region must be exact square, DWT has to be applied later on this region. Let S is secret data. Here secret data considered is binary image of size a×b. Figure 3.3 represents flowchart of embedding process.

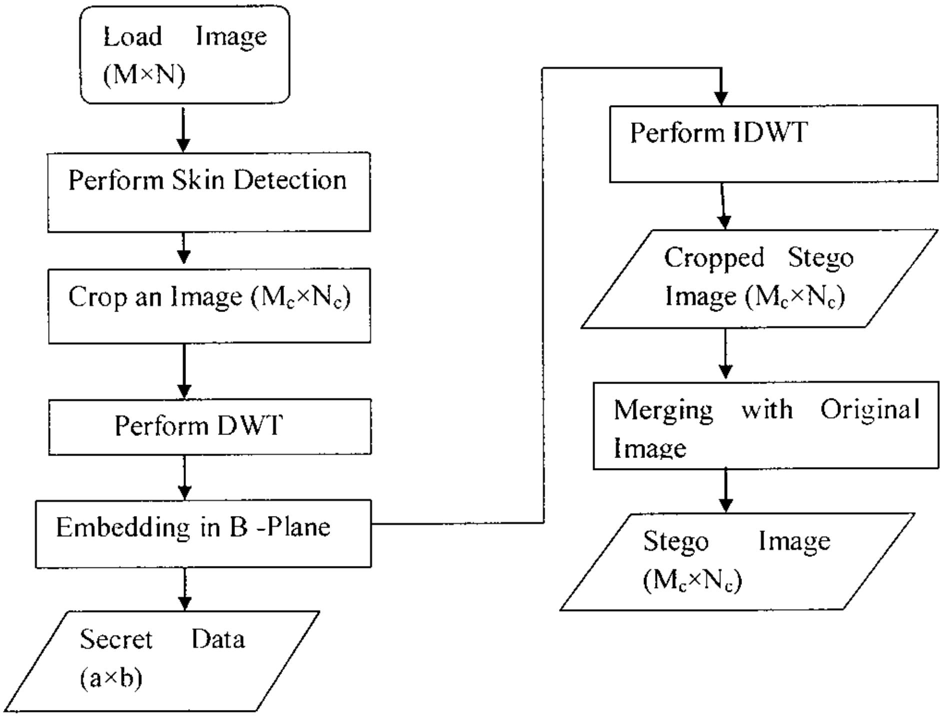


Figure 3.3 Flowchart of Embedding Process

For the first $1 \leq i \leq M \times N$ bits of secret data sequence, every 2 consecutive bits are combined to form a decimal value ranging from 0 to 3. For example, sequence 00110110 will be transformed to sequence 0312. Every 2 consecutive values in the resulted decimal sequence are further combined to perform subtraction operation and form a differential sequence ranging from -3 to 3. For example, sequence 0312 results in a differential sequence of -2 (0-3), -1(1-2). As shown in Table 3.1, there are only 4 possible absolute values (0, 1, 2 and 3) for the elements in this differential sequence. These absolute values are recorded in H_{HH} with 00, 01, 10 and 11 respectively. However, same absolute value might be consequence of different subtraction pairs (For example, 1 could be |3-2|, |2-1|, |1-0|, |2-3|, |1-2|, or |0-1|). Hence, more bits are needed to distinguish the subtraction status. In Table 3.1, the right Table coding is designed to record the possible subtraction pairs. The codes underlined are embedded in H_{HL}. Embedding positions in H_{LH} and H_{HL} are just the corresponding positions in H_{HH}

Table 3.1 Sequence Mapping Table

Left table: 4 possible absolute values

Latter / Former	0	1	2	3
0	|0|	|-1|	|-2|	|-3|
1	|1|	|0|	|-1|	|-2|
2	|2|	|1|	|0|	|-1|
3	|3|	|2|	|1|	|0|

⇨

Right table: Status of subtraction pairs

Latter / Former	0	1	2	3
0	$\underline{0}0$	$\underline{10}0$	$\underline{1}0$	$\underline{1}$
1	$\underline{00}0$	$\underline{0}1$	$\underline{10}1$	$\underline{1}1$
2	$\underline{0}0$	$\underline{00}1$	$\underline{1}0$	$\underline{11}0$
3	$\underline{0}$	$\underline{0}1$	$\underline{01}0$	$\underline{1}1$

The raster scan order is employed for embedding the secret data and is given in the following Figure 3.4.

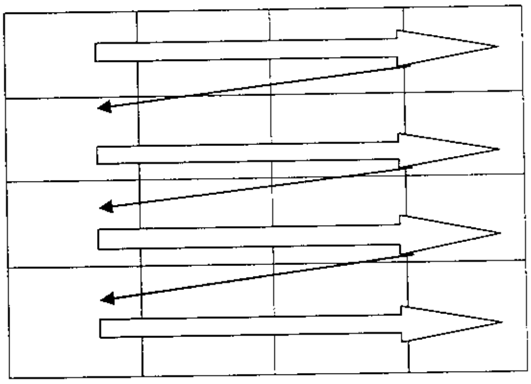


Figure 3.4 Raster scan order for embedding

The remaining bits of secret data are embedded at those unused LSBs in H_{LH} and then H_{HL} bit by bit. For example, if the value embedded in H_{HH} is 1, no more message bit is embedded at the corresponding position of H_{LH} but 1 more bit at the corresponding position in H_{LH}. After embedding all the message bits, the slightly modified coefficients matrix H is obtained. By performing the inverse DWT on H, the stego- image is obtained.

3.4 Implementation Steps

Step 1: Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.

Step 2: Cropping is performed interactively on mask image ($M_c \times N_c$). After this, original image is also cropped of same area. Cropped area must be in an exact square form as DWT has to be applied later and cropped area should contain skin region such as face, hand etc since data will be hidden in skin pixels of one of the subband of DWT. Here cropping is performed for security reasons. Cropped rectangle will act as key at receiving side. If it knows then only data retrieval is possible. Eavesdropper may try to perform DWT on whole image; in such a case attack will fail as we are applying DWT on specific cropped region only.

Step 3: Apply DWT to only cropped area (Mc×Nc) not on the whole image (M×N). This yields 4 subbands denoted as HLL, HHL, HLH, HHH (All 4 subband are of same size of Mc/2, Nc/2).

Step 4: Perform embedding of secret data in one of subband by tracing skin pixels in that subband. Other than the LL, low frequency subband any high frequency subband can be selected for embedding as LL subband contains significant information. Embedding in LL subband affects image quality greatly. High frequency HH subband is chosen.

While embedding, secret data will not be embedded in all pixels of DWT subband but to only those pixels that are skin pixels. So, skin pixels are traced using skin mask detected earlier and secret data is embedded. Embedding is performed in G-plane and B-plane but strictly not in R-plane as contribution of R plane in skin color is more than G or B plane. So, if there is any modification in the R plane pixel values, decoder side don't retrieve data at all as skin detection at decoder side gives different mask than encoder side. Embedding is done as per raster-scan order that embeds secret data coefficient by coefficient in selected subband, if coefficient is skin pixel.

Step 5: Perform IDWT to combine 4 subbands.

Step 6: A cropped stego image of size Mc×Nc is obtained in above step (step 5). This should be similar to original image after visual inspection but at this stage it is of size Mc×Nc, the cropped stego image has to be merged with original image to get the stego image of size M×N. To perform merging, coefficients of first and last pixels of cropped area in original image is required. Thus, a stego image is ready for quality evaluation.

3.5 Extraction Process

Secret data extraction is explained as follows:

24 bit color stego image of size M×N is input to extraction process. The value of cropped area to retrieve data is needed. Suppose cropped area value is stored in 'rect' variable that is same as in encoder. So this 'rect' will act as a key at decoder side. All steps of Decoder are opposite to Encoder. Cropping same size of square as per Encoder is needed. By tracing skin pixels in H_{HH} subband of DWT secret data is retrieved.

Performing DWT transform on stego image, matrix H' is obtained. The absolute values (0, 1, 2 and 3) from the 2 rightmost LSBs in H'_{HH} subband. According to the value extracted, LSBs of corresponding positions in H'_{LH} and H'_{HL} are used to determine the subtraction pair. Based on the mapping rules defined in Table 3.1, 2 values (former and latter) of the decimal sequence are reconstructed. Cue these decimal values in correct order and then expand them to a binary bit stream.

By extracting some more second LSBs in H'_{LH} and H'_{HL}, the remaining portion of secret sequence is obtained. Cascade it with the sequence obtained in the above step, the whole message bit stream is completely extracted.

Extraction procedure is represented using the following Figure 3.5.

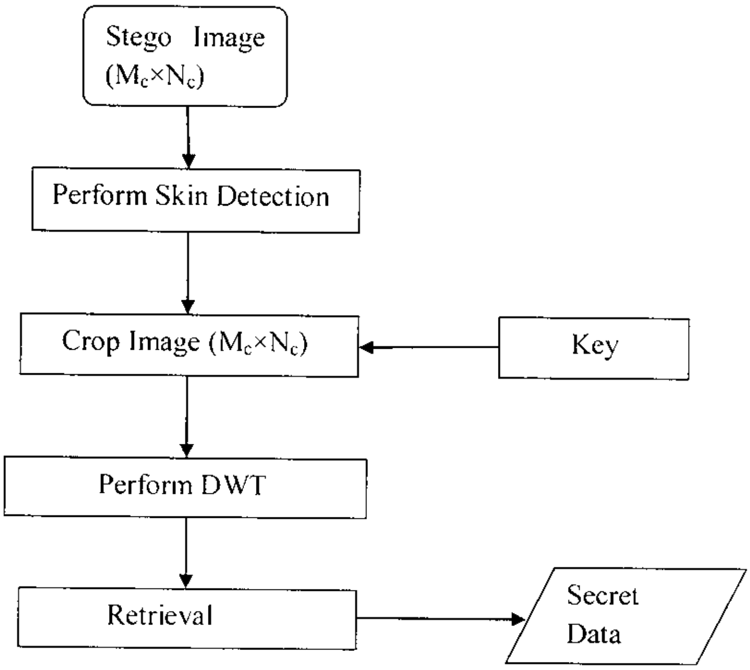


Figure 3.5 Flowchart of Extraction Process

3.6 JPEG Compression

To check the robustness of the proposed algorithm, stego file is subjected into JPEG compression. One of the most popular and comprehensive continuous tone, still frame compression standards is the JPEG standard [18].

JPEG defines three different coding systems:

- A lossy baseline coding system, which is based on the DCT and is adequate for most compression applications.
- An extended coding system for greater compression, higher precision or progressive reconstruction applications.
- A lossless independent coding system for reversible compression.

In the baseline system, often called the sequential baseline system, the input and output data precision is limited to 8 bits, where as the quantized DCT values are restricted to 11bits. The compression itself is performed in three sequential steps:

- DCT Computation
- Quantization
- Variable Length Code assignment

The image is first subdivided into pixel blocks of size 8 × 8, which are processed left to right, top to bottom. As each 8 × 8 block of sub image is encountered, its 64 pixels are level shifted by subtracting the quantity $2n^{-1}$, where 2^n is the maximum number of gray levels. The 2-D discrete cosine transform of the block is then computed, quantized and reordered, using the zigzag pattern to form a 1-D sequence of quantized coefficients.

The construction of the default JPEG code for the reordered coefficient sequence begins with the computation of the difference between the current DC coefficient and that of the previously encoded sub image. For a general DC difference category, an additional K bits are needed and computed as either the K LSBs of the positive difference or the K LSBs of the negative difference minus 1.

The nonzero AC coefficients of the reordered array are coded similarly. The principal difference is that each default AC Huffman code word depends on the number of zero-valued coefficients preceding the non zero coefficient to be coded, as well as the magnitude category of the nonzero coefficient.

To decompress a JPEG compressed sub image, the decoder must recreate the normalized transform coefficients that led to the compressed bit stream.

The compression ratio gives an indication of how much compression is achieved for a particular image. The compression ratio is equal to the size of the original image divided by the size of the compressed image. Most algorithms have a typical range of compression ratios that they can achieve over a variety of images. Because of this, it is usually more useful to look at an average compression ratio for a particular method.

The compression ratio typically affects the picture quality. Generally, the higher the compression ratio, the poorer the quality of the resulting image. The tradeoff between compression ratio and picture quality is an important one to consider when compressing images. Furthermore, some compression schemes produce compression ratios that are highly dependent on the image content.

$$\text{Compression Ratio} = \frac{\text{Number of bits in an Image before Compression}}{\text{Number of bits in an Image after Compression}} \qquad (3.4)$$

3.7 Performance Measure

As a performance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego-images. It is defined as:

$$PSNR = 10\log\left(\frac{C_{\max}^2}{MSE}\right) \qquad (3.5)$$

where MSE denotes mean square error which is given as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \qquad (3.6)$$

where x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego image and C_{xy} is the cover image.

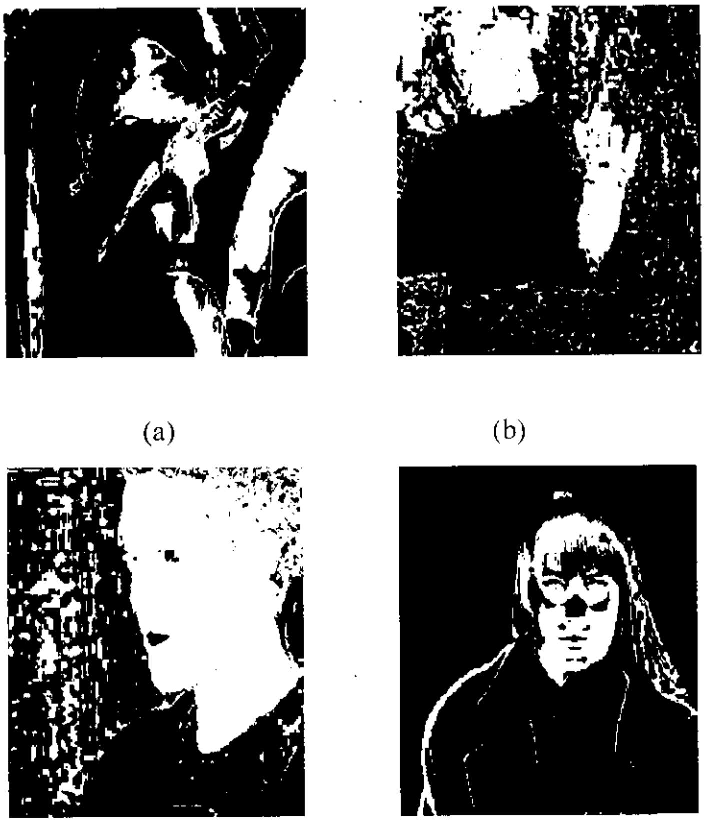
$C_{\max}^2$ holds the maximum value in the image, for example:

$$C_{\max}^2 \leq \begin{cases} 1, & \text{double precision} \\ 255, & \text{unint8 bit} \end{cases} \qquad (3.7)$$

Many authors consider $C_{\max} = 255$ as a default value for 8 bit images. C_{max} is raised to a power of 2 results in a severe change to the PSNR value. Thus C_{max} can be defined as the actual maximum value rather than the largest possible value. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 30 dB and above.

The embedding, extracting procedures for secret image and the performance measure for steganography are included in this chapter. The robustness of the proposed method is evaluated by JPEG compression. The simulated results and discussion are presented in the following chapter.

Mask image that contains skin (white region) and non skin pixels (black region) is obtained by employing skin tone detection and it is shown in Figure 4.3.

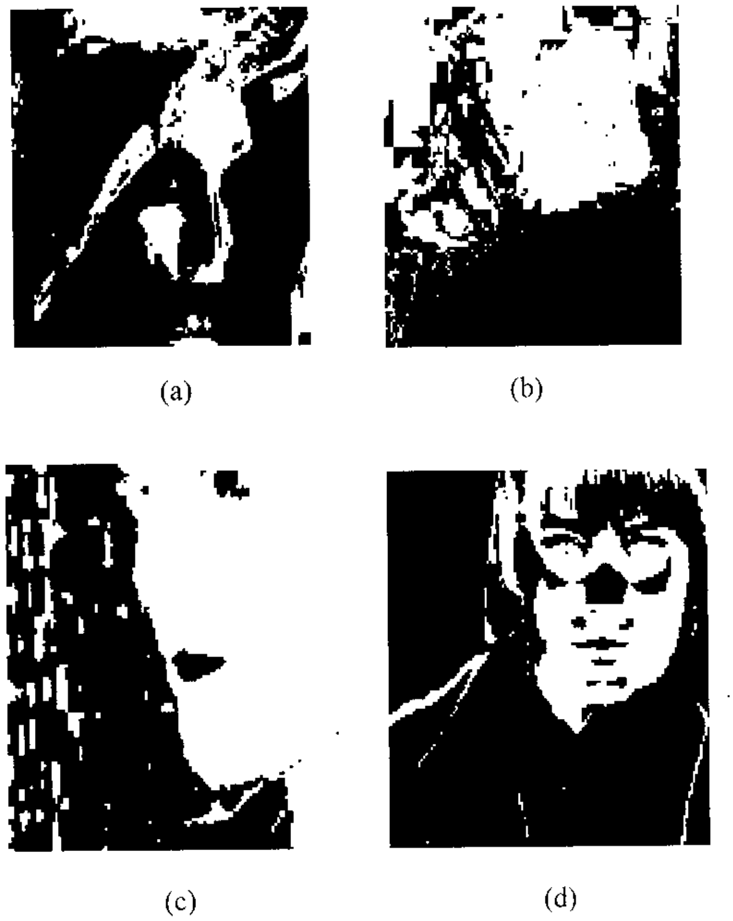


(a) (b)

(c) (d)

Figure 4.3 Mask Images: (a) Lena (b) Baby (c) Man (d) Girl

Mask image that contains skin (white region) and non skin pixels (black region) is cropped to the particular area, which will act as a key in shown in Figure 4.4.

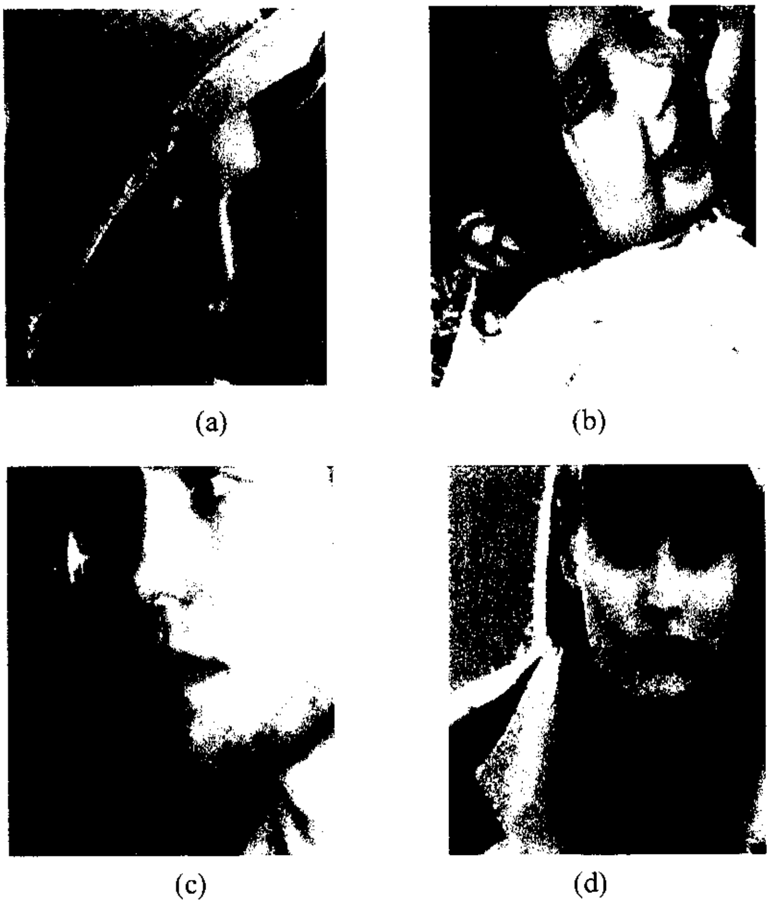


(a) (b)

(c) (d)

Figure 4.4 Cropped Mask: (a) Lena (b) Baby (c) Man (d) Girl

Cover image is also cropped to the same area, which will act as a key in shown in Figure 4.5.

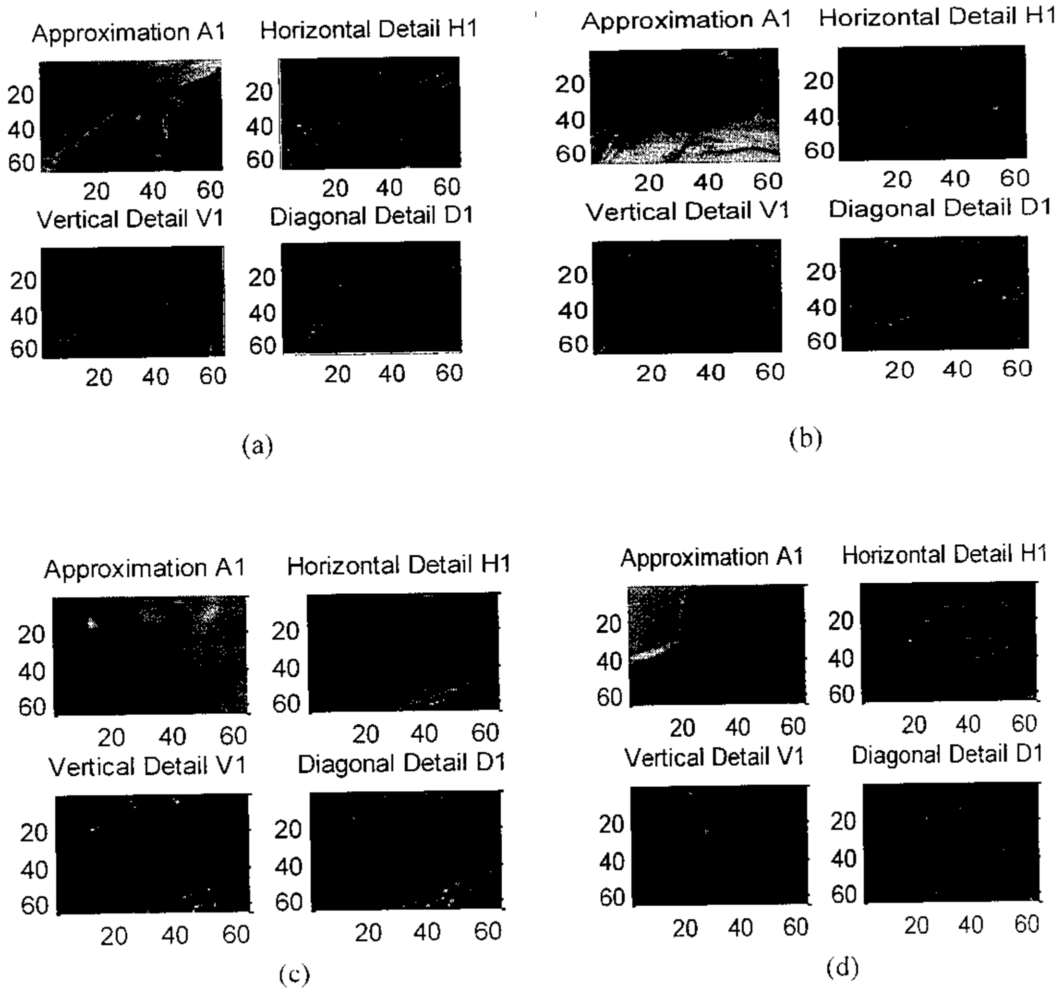


(a) (b)

(c) (d)

Figure 4.5 Cropped Cover Images: (a) Lady (b) Baby (c) Man (d) Girl

DWT is applied to the cropped cover images and it is given in the following Figure 4.6.



(a)

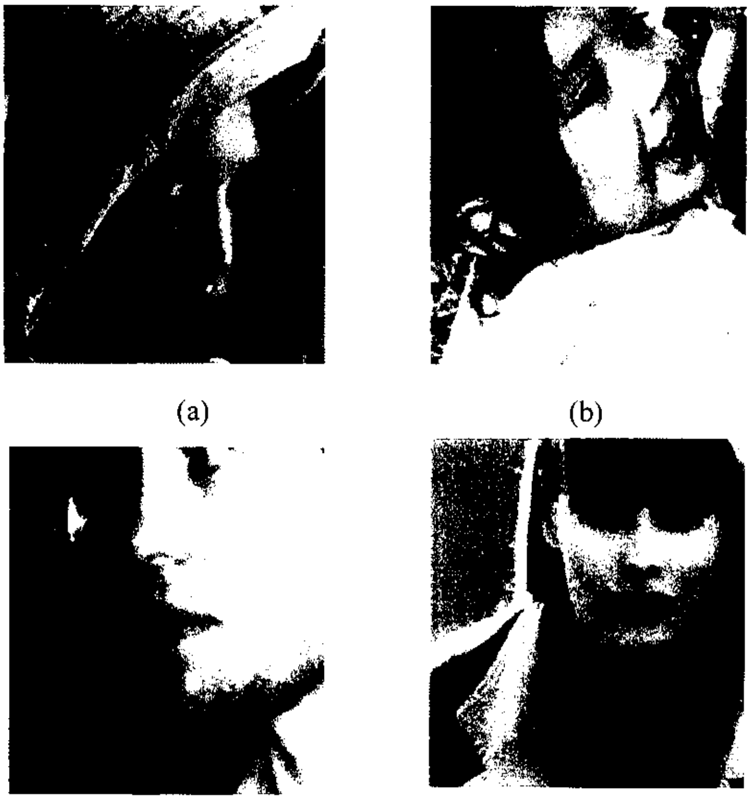
(b)

(c)

(d)

Figure 4.6 DWT of Cover Images: (a) Lena (b) Baby (c) Man (d) Girl

After embedding the secret data , cropped stego image is obained and is given in the following Figure 4.7.



(a) (b)

(c) (d)

Figure 4.7 Cropped Stego Images: (a) Lena (b) Baby (c) Man (d) Girl

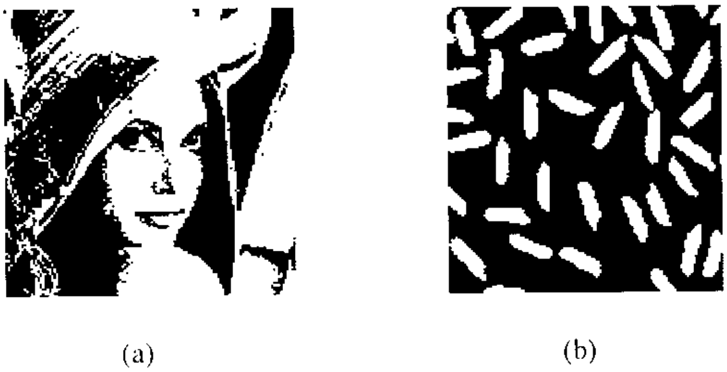
CHAPTER 4

RESULTS AND DISCUSSION

Data hiding within the skin region is implemented using MATLAB (Matrix LABoratory) which is a high performance language for technical computing. The implementation is done on Intel-Pentium processor with RAM Capacity of 1 GB and system clock of 3.00 GHz.

The original color image is converted into HSV color space. Mask image that contains skin (white region) and non skin pixels (black region) is obtained by employing skin tone detection. The cropped mask image contains the skin region. The original cover image is also cropped of the same area as that of mask. The original image is separated into three planes (R plane, G plane, B plane). DWT is applied to the any one of the plane. The secret image is a binary image and it is converted into sequence of 1's and 0's. Secret data is embedded into the skin region. If the data is embedded in a particular region like skin, it will improve the security. The simulated results are shown below:

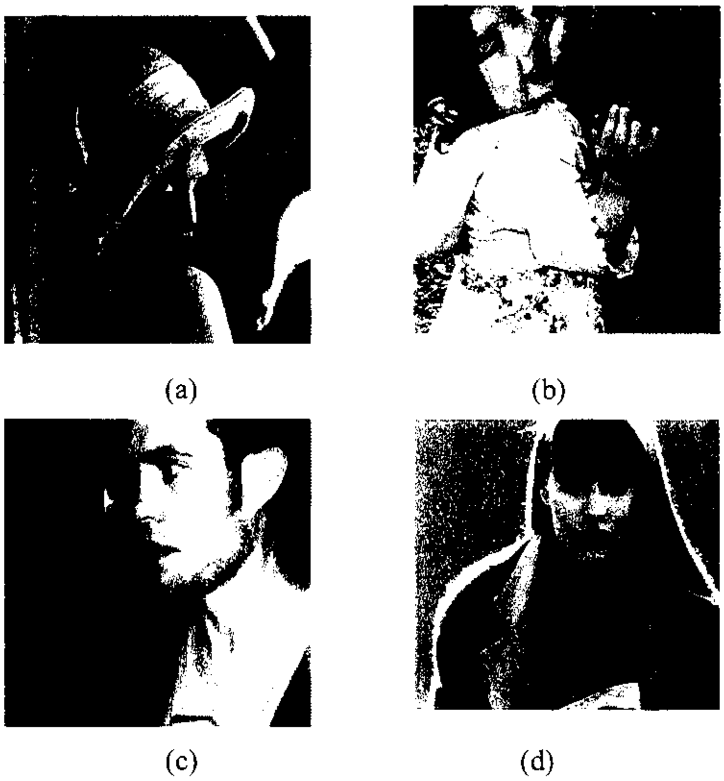
The Secret Images to be hidden is shown in Figure 4.1.



(a) (b)

Figure 4.1 Secret Images to Be Hidden (a) Lena (b) Rice

The cover images inside which the secret data is embedding is shown in Figure 4.2.The size of the cover image is (256×256).

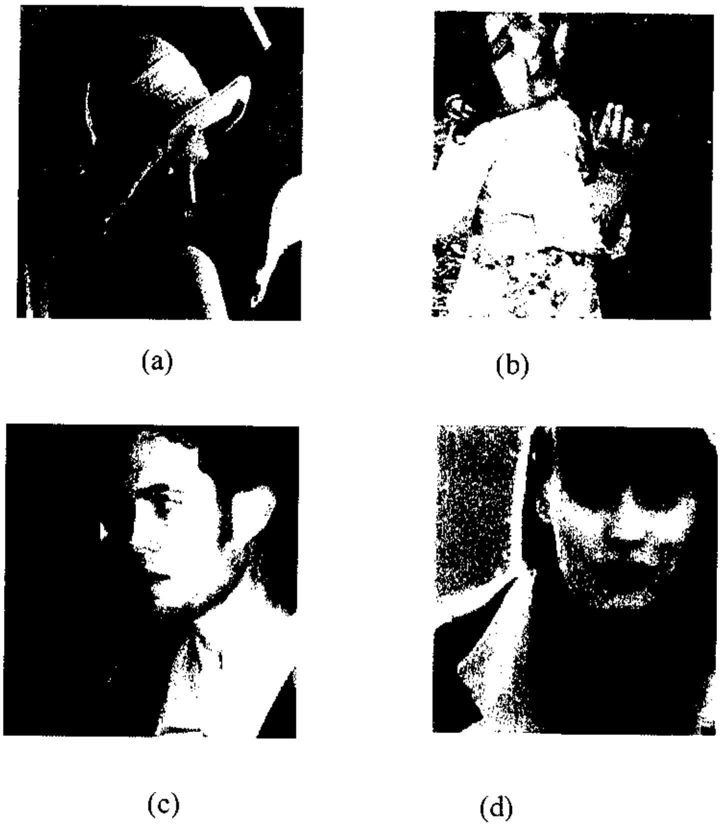


(a) (b)

(c) (d)

Figure 4.2 Cover Images: (a) Lena (b) Baby (c) Man (d) Girl

When digital data are transmitted over a noisy channel, there is always a chance that the received data will contain errors. These errors can be considered as a result of either an attacker or by the noise presented within the received signal. Error correction coding can often be used to reduce errors to a level at which they can be tolerated, and hence improve the reliability of communication on digital channels. Any stego image may be transferred through a noisy channel or undergo compression. To check the robustness of the proposed method, the stego image is subjected to JPEG compression and the compression ratio is calculated and it is shown in the following Figure 4.11.



(a) (b)

(c) (d)

Figure 4.11 Compressed Stego images (a) Lena (b) Baby (c) Man (d) Girl

The Performance Measure of JPEG Compression is given in the following Table 4.8

Table 4.8 Performance Measure of JPEG Compression

Cover Image	Stego Image size in Kilobytes	Compressed Image size in Kilobytes	Compression Ratio	PSNR in dB
Lena	11	9	13.11	38.52
Baby	18	15	7.43	32.87
Man	9	7	16.40	40.11
Girl	12	10	12.50	39.71

From the above Table, it is inferred that compression ratio is smaller and it does not degrade the compressed image quality. PSNR value between the stego image before compression and after compression falls above 30 dB. A fine image quality is reconstructed.

The secret data is embedded into the skin region and the performance measure is calculated for stego images in different planes. The security of the secret image is further enhanced by embedding in skin pixels. A high image quality is obtained for the stego image by employing the proposed method. The robustness of the proposed method is enhanced by JPEG compression.

CHAPTER 5

CONCLUSION

Proposed method embeds the secret image into the skin region of the cover image. Image cropping provides security so that no one can extract message without having cropped region. The security of the secret image is further enhanced by embedding in skin pixels. A high image quality is obtained for the stego image by employing the proposed method. The proposed method provides high robustness when the stego image is subjected to JPEG compression. When comparing the proposed method which is based on DWT with DCT based steganography, it is inferred that DCT introduces annoying blocking artifacts. DWT offers better energy compaction than DCT without any blocking artifacts.

The steganography methods usually struggle with achieving a high embedding rate. As an alternative channel to images, video files have many excellent features for information hiding such as large capacity and good imperceptibility. The challenge is to embed the secret message into a group of images which are highly inter-correlated and often manipulated in a compressed form. The future work of the proposed method will continue in the embedding of secret data into the video files.

REFERENCES

[1] Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing 90 (2010) 727–752.

[2] N. Provos, P. Honeyman, "Hide and seek: an introduction to steganography", IEEE Security and Privacy 1 (3) (2003) 32–44.

[3] Eugene T. Lin and Edward J. Delp, "A review of data hiding in digital images", Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999.

[4] V.M. Potdar, S. Han, E. Chang, "Fingerprinted secret sharing steganography for robustness against image cropping attacks", in: Proceedings of IEEE Third International Conference on Industrial Informatics (INDIN), Perth, Australia, 10–12 August 2005, pp. 717–724.

[5] Z. Li, X. Chen, X. Pan, X. Zeng, "Lossless data hiding scheme based on adjacent pixel difference", in: Proceedings of the International Conference on Computer Engineering and Technology, 2009, pp. 588–59.

[6] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang "Image steganographic scheme based on pixel-value differencing and LSB replacement methods" IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005,pp 611-615.

[7] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, "A new genetic algorithm approach for secure JPEG steganography", in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April 2006, pp. 1–6.

[8] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik, "A secure image steganography using LSB, DCT and compression techniques on raw images", in: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP'05, Bangalore, India, 14–17 December 2005, pp. 170–176.

[9] N.K. Abdulaziz, K.K. Pang, "Robust data hiding for images", in: Proceedings of IEEE International Conference on Communication Technology, WCC-ICCT'02, vol. 1, 21–25 August 2000, pp. 380–383.

[10] Ahmed A.Abdelwahab and Lobna A. Hasaan, "A Discrete Wavelet Transform Based Technique for Image Data Hiding, 25th National Radio Science Conference (NRSC 2008), March 18-20, 2008.

[11] K.B. Raja, S. Sindhu, T.D. Mahalakshmi, S. Akshatha, B.K. Nithin, M. Sarvajith, K.R. Venugopal, L.M. Patnaik, "Robust image adaptive steganography using integer wavelets", in: Proceedings of the Third International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE'08, 6–10 January 2008, pp. 614–621.

[12] Velasco, Nakano, Perez, Martinez, Yamaguchi,"Adaptive JPEG Steganography using convolutional codes and synchronization bits in DCT domain", Circuits and Systems 2009,MWSCAS'09, 52nd IEEE International Midwest Symposium,2009, pp:842 – 847.

[13] Abbas Chedda, Joan Condell, Kevin Curran and Paul Mc Kevitt "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography" , School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, BT487JL, Londonderry, Northern Ireland, UK, 2008.

[14] F.A.P. Petitcolas, " Introduction to information hiding", in: S. Katzen- beisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[15] S. Miaou, C. Hsu, Y. Tsai, H. Chao, "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records", in: Proceedings of the IEEE 22nd Annual EMBS International Conference, Chicago, USA, July 23–28, 2000, pp. 280–283.

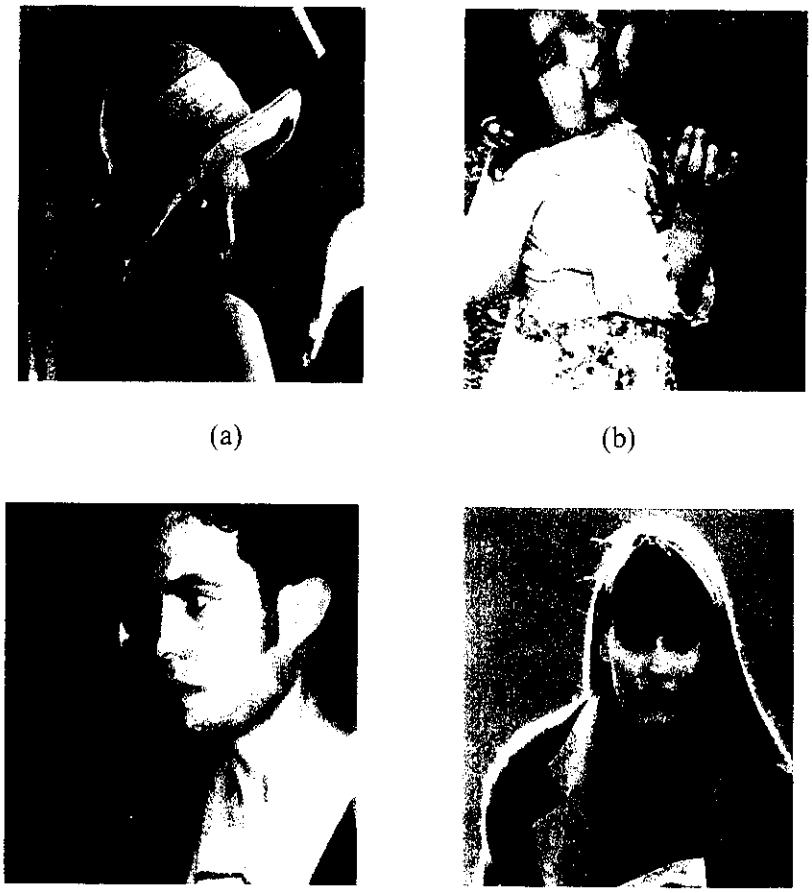
[16] Anjali A.Shejul, "A DWT Based Approach for Steganography Using Biometrics", Proceedings of International Conference on Data Storage and Data Engineering, 2010.

[17] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009.

[18] Rafael C.Gonzalez, Richard E. Woods, "Digital Image Processing", Second Edition, pp-520-527.

[19] Ekta Walia , Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology Vol. 10 Issue 1 (Ver. 1.0), April 2010.

The cropped stego image has to be merged with original image to get the stego image of size M×N and the final stego image is given in the following Figure 4.8.

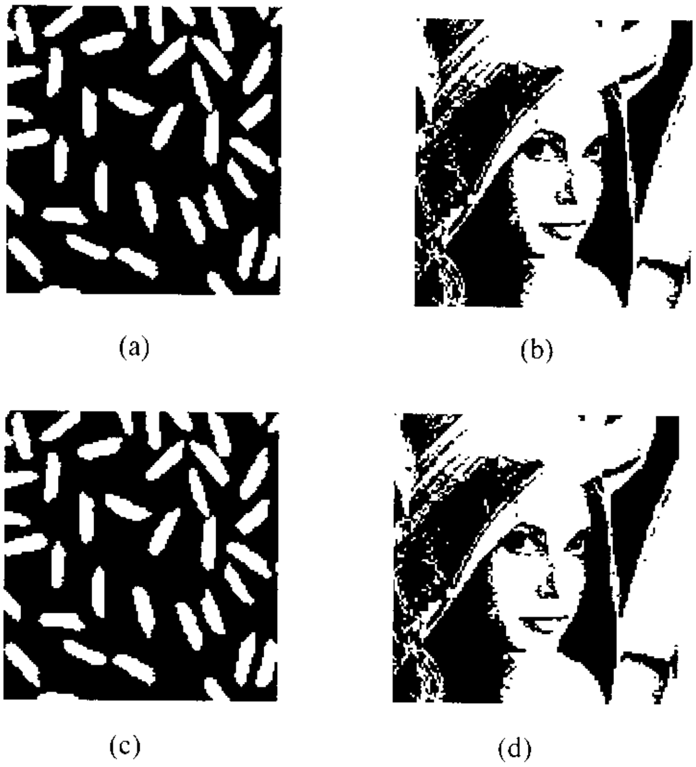


(a) (b)

(c) (d)

Figure 4.8 Final Stego Images: (a) Lena (b) Baby (c) Man (d) Girl

The secret images are obtained from the final stego images and are shown in the Figure 4.9.



(a)

(b)

(c)

(d)

Figure 4.9 Retrieved Secret Images: (a) Rice from Lena (b) Lena from Baby (c) Rice from Man (d) Lena from Girl

From the above simulated results, it is observed that the stego image is similar to that of the cover image. The true message is not visible to the observer. That is, unwanted parties should not be able to distinguish in any sense between cover-image and stego image. Thus, proposed methodology fulfills the objective of the steganography by focusing on concealing the existence of a message.

The secret images of size (64 ×64) and (128 ×128) is embedded into different planes and it is shown in the following Tables.

Table 4.1 Embedding the secret image (64 ×64) in B plane

Cover Images (256×256)	Secret Images (64 ×64)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	35.91	41.19	41.18
	Rice	35.92	41.20	41.19
Baby	Lena	31.22	37.98	37.97
	Rice	31.22	37.98	37.97
Man	Lena	36.57	42.19	42.18
	Rice	36.57	42.22	42.21
Girl	Lena	35.85	38.72	38.71
	Rice	35.85	38.73	38.72

Table 4.2 Embedding the secret image (128 ×128) in B plane

Cover Images (256×256)	Secret Images (128×128)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	35.92	41.19	41.22
	Rice	35.94	41.20	41.31
Baby	Lena	31.23	37.97	37.99
	Rice	31.24	37.98	38.04
Man	Lena	36.60	42.24	42.22
	Rice	36.63	42.34	42.31
Girl	Lena	35.85	38.78	38.74
	Rice	35.87	38.83	38.80

Table 4.3 Embedding the secret image (64 ×64) in G plane

Cover Images (256×256)	Secret Images (64 ×64)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	35.27	40.38	40.37
	Rice	35.27	40.39	40.38
Baby	Lena	31.22	37.99	37.99
	Rice	31.22	38.01	37.99
Man	Lena	36.57	41.98	41.98
	Rice	36.57	42.01	42.01
Girl	Lena	35.87	39.37	39.36
	Rice	35.87	39.38	39.37

Table 4.4 Embedding the secret image (128×128) in G plane

Cover Images (256×256)	Secret Images (128×128)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	35.28	40.45	40.41
	Rice	35.29	40.52	40.48
Baby	Lena	31.23	38.05	38.02
	Rice	31.24	38.10	38.07
Man	Lena	36.58	42.04	42.04
	Rice	36.61	42.13	42.65
Girl	Lena	35.88	39.42	39.38
	Rice	35.90	39.47	39.44

Table 4.5 Embedding the secret image (64 ×64) in R plane

Cover Images (256×256)	Secret Images (64 ×64)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	36.23	40.56	40.55
	Rice	36.24	40.57	40.56
Baby	Lena	31.22	38.02	38.02
	Rice	31.22	38.04	38.03
Man	Lena	36.36	42.01	42.01
	Rice	36.37	42.04	42.04
Girl	Lena	35.72	39.11	39.10
	Rice	35.72	39.13	39.11

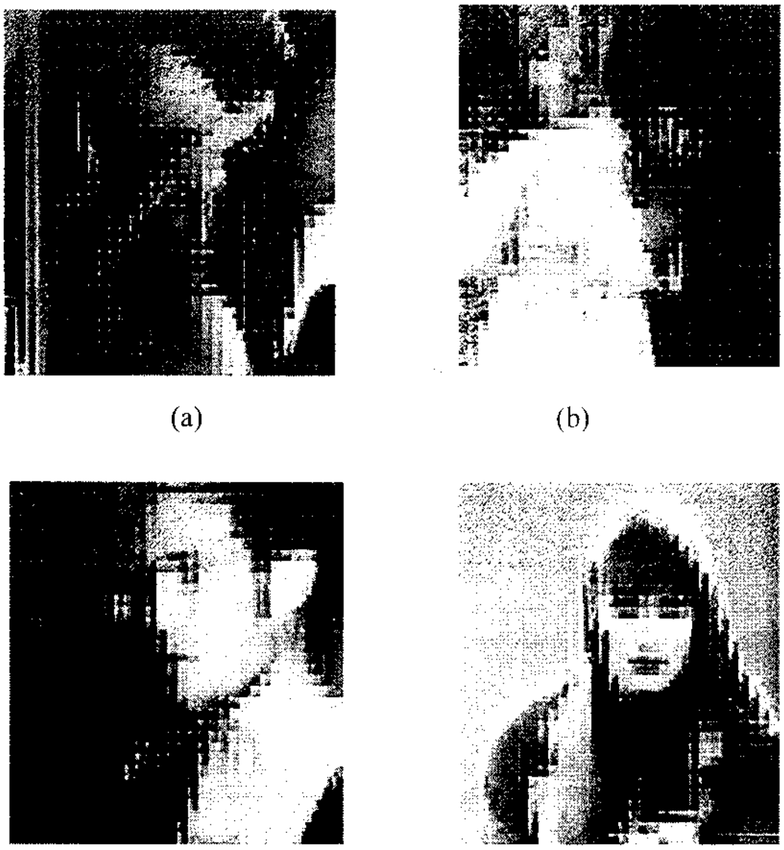
Table 4.6 Embedding the secret image (128 × 128) in R plane

Cover Images (256×256)	Secret Images (128×128)	PSNR in dB		
		Embedding in all pixels		Embedding in skin pixels
		Without Cropping	With Cropping	
Lena	Lena	36.24	40.62	40.60
	Rice	36.26	40.70	40.67
Baby	Lena	31.23	38.07	38.04
	Rice	31.24	38.12	38.09
Man	Lena	36.37	42.14	42.05
	Rice	36.40	42.05	42.13
Girl	Lena	35.72	39.16	39.13
	Rice	35.74	39.23	39.20

From the results obtained, it is observed that PSNR value is higher for stego images with cropping than without cropping. Embedding the secret images in skin pixels also gives higher PSNR and enhances the security. PSNR value is falling above 30 dB. This shows that distortion caused by embedding is very less. A high image quality is obtained for the stego image by employing the proposed method.

The proposed method is compared with the embedding of secret image in DCT domain. The embedding of secret image into LSB of DC coefficients in DCT domain requires large cover image if the secret data size is larger. The secret image is embedded into LSB of each AC coefficients in DCT domain [19].

DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifacts. This drawback of DCT is eliminated using DWT. DWT offers better energy compaction than DCT without any blocking artifact. The comparison is performed in a cover image of size 256×256 by embedding different secret images of size 128×128. The stego images in DCT domain is given in the following Figure 4.10.



(a) (b)

(c) (d)

Figure 4.10 Stego Images in DCT domain

PSNR value is calculated for different images and it is shown in the following Table 8.7.

Table 4.7 Comparison of stego images in DCT domain and DWT domain

Cover Images (256×256)	Secret Images (128×128)	PSNR in dB			
		DCT Based steganography	Embedding in all pixels (DWT Based Steganography)		Embedding in skin pixels (DWT)
			Without Cropping	With Cropping	
Lena	Lena	17.36	35.85	38.78	38.74
	Rice	17.99	35.87	38.83	38.80
Baby	Lena	17.46	31.23	37.97	37.99
	Rice	18.04	31.24	37.98	38.04
Man	Lena	19.67	36.60	42.24	42.22
	Rice	20.83	36.64	42.34	42.31
Girl	Lena	18.43	35.92	41.18	41.22
	Rice	19.16	35.94	41.19	41.30

From the Table 4.7, it is observed that PSNR value is higher for DWT based stego images than DCT. Also, PSNR value is higher for DWT based stego images with cropping than without cropping. Cropping enhances the security of the secret image. PSNR value obtained is above 30 dB while applying DWT. This shows that distortion caused by embedding in DWT is very less. The security of the secret image is further enhanced by embedding in skin pixels. A high image quality is obtained for the stego image by employing the proposed method.