IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC ENCRYPTION AND DECRYPTION

A PROJECT REPORT

Submitted by

DINESH KUMAR M	19106025
GOWSEKAN AP	19106032
HARISH	19106041
HARSANPRABU R	19106043

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY

Approved by AICTE, New Delhi, Accredited with 'A' Grade by NAAC

(An Autonomous Institution, Affiliated to Anna University, Chennai)

COIMBATORE – 641 032

APRIL 2023

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY

Approved by AICTE, New Delhi, Accredited with 'A' Grade by NAAC
(An Autonomous Institution, Affiliated to Anna University, Chennai)
COIMBATORE – 641 032

BONAFIDE CERTIFICATE

Certified that project report "**IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC ENCRYPTION AND DECRYPTION"** is the bonafide work of **DINESH KUMAR M (19106025), GOWSEKAN A P (19106032), HARISH V (19106041)** and **HARSANPRABU R (19106043)** who carried out the project work under my supervision.

SIGNATURE
HEAD OF THE DEPARTMENT
Dr.P.Vijayalakshmi, M.E., Ph.D.
Professor and Head of Department,
Department of Electronics and Communication Engineering.
Hindusthan College of Engineering and Technology, Coimbatore-641032

SIGNATURE
SUPERVISOR
Dr.D.Baskar, M.E., Ph.D.
Associate Professor,
Department of Electronics and Communication Engineering.
Hindusthan College of Engineering and Technology, Coimbatore-641032

Submitted for Autonomous Project Viva-Voce examination held on ……

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We express our profound gratitude to our Honourable Chairman, **Shri. T.S.R. KHANNAIYANN** and our Managing Trustee, **Smt.T.R.K. SARASUWATHI** of Hindusthan Educational and Charitable Trust for providing the necessary facilities and support for successful completion of the project within the college.

We extend our sincere thanks to our Chief Executive Officer, Hindusthan Institutions **DR. K. KARUNAKARAN, Ph.D.,** for his constant support and motivation.

We would like to express our heartfelt thanks to our Principal, **DR. J. JAYA, M. Tech., Ph.D.,** for her constant motivation and encouragement.

We are highly indebted to our Head of the Department **DR. P. VIJAYALAKSHMI, M.E, Ph.D.,** for her scholastic guidance and supervision in completing the project.

We are grateful to our Project guide **DR. D. BASKAR, M.E., Ph.D.,** for his valuable guidance and support to complete the assigned task.

We owe a whole hearted sense of reverence and gratitude to **DR. K. KALAISELVI M.E., Ph.D.,** our Project Coordinator for her valuable guidance and also for helping us to complete the assigned task.

We are also thankful to all our teaching and non-teaching staff members of the Department of Electronics and Communication Engineering for their kind cooperation and encouragement.

ABSTRACT

In today's era due to the growth of multimedia applications, security has become an important issue for communication and storage of images. So, proper watermarking, encryption and compression should be applied to transmit the data from one place to another place across the internet in order to prevent unauthorized access. This proposal is about watermarking of the image using 2D 3-level discrete wavelet transform, encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish algorithm and compression of the encrypted image using SPIHT (Set Partitioning in Hierarchical Tree) algorithm. These algorithms will give the increased security and improved performance of the transmitted image. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. In this project, we design a highly efficient image watermarking encryption then lossless compression (WETLC) system. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security.

TABLE OF CONTENTS

ABBREVIATIONS

SPIHT	-	Set Partitioning in Hierarchical Tree
WETLC	-	Watermarking Encryption Then Lossless Compression
HVS	-	Human Visual System
MRI	-	Magnetic Resonance Imaging
LSB	-	Least significant Byte (or) Bits
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DWT	-	Discrete Wavelet Transform
QR	-	Quick Response
JPEG	-	Joint Photographic Experts Group
dB	-	Decibels
PSNR	-	Peak Signal-To-Noise Ratio
PNG	-	Portable Network Graphics
GIF	-	Graphics Interchange Format
DES	-	Data Encryption Standard
RSA	-	Rivest-Shamir-Adleman
CTE	-	Compression Then Encryption
LDPC	-	Low Density Parity Check Code
CS	-	Compressive Sensing
AC	-	Arithmetic Coding
RLE	-	Run Length Encoding
VLC	-	Variable Length Coding
VQ	-	Vector Quantization
IFS	-	Iterated Function System
EZW	-	Embedded Zero tree Wavelet
MSR	-	Multi Scale Retinex

BMP	-	Bitmap Format
OFDM	-	Orthogonal Frequency Division Multiplexing
IDWT	-	Inverse Discrete Wavelet Transform
PMT	-	Pixel Mapping Table
MSE	-	Mean Square Error

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In order to avoid unauthorised access, it is essential that adequate encryption and decryption be used while transferring data from one location to another across the internet. A colour image to be protected and a binary image used as key to encrypt and decrypt are taken as input. With the progress in data exchange by electronic system, the need for information security has become a necessity. This proposal is about encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. Image encryption has to be conducted prior to image compression. This has led to the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. In this paper, we design a highly efficient image encryption-then-compression system, where lossless compression is considered. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic coding- based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only slightly

worse, in terms of compression efficiency, than the state-of-the-art lossless image coders, which take original, unencrypted images as inputs. In contrast, most of the existing solutions induce significant penalties on the compression efficiency.

1.1 WATERMARKING

Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content. Digital watermarking technology is being adopted to ensure and facilitate data authentication, security and copyright protection of digital media. It is considered as the most important technology in today's world, to prevent illegal copying of data. Digital watermarking can be applied to audio, video, text or images. Digital watermarking hides the copyright information into the digital data through a certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden. in the digital data either visible or invisible. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermarks can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenarios.

1.1.1 ADVANTAGES OF WATERMARKING

- Easy to implement and understand.
- Low degradation of image quality.
- High perceptual transparency.
- Gain factor can be increased.
- High level of robustness against most types of attacks.
- This method hides data within the continuous random texture patterns of a picture.
- The visibility of the image will not get affected and the watermark will not be removed by any kind of attack
- Allows good localization both in time and spatial frequency domain. Higher compression ratio which is relevant to human perception.

1.1.2 DISADVANTAGES OF WATERMARKING

- Vulnerable to cropping, scaling and noise.
- It can hide only a very small amount of information.
- Image quality decreases due to very high increase in gain factor.
- This algorithm is only suitable for those areas with a large number of arbitrary texture images.
- Cost of computing may be higher.
- Longer compression time.

1.1.3 APPLICATIONS OF WATERMARKING

- Broadcast Monitoring.
- Ownership Assertion.

- Transaction Tracking.
- Content Authentication.
- Copy Control and Fingerprinting.
- Communication of ownership and copyrights.
- Document and image security.
- Rich media enhancement for mobile phones
- Video authentication.

1.2 ENCRYPTION

Image Encryption is one of the techniques that are used to ensure high security. Various fields such as medical science military in which image encryption can be used. Modem cryptography provides essential techniques for securing information and protecting multimedia data. In last some years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access. Due to some inherent features of the image like low cost and high availability. usage of communication networks has increased and it becomes a reason for rapid growth of the internet in the digital world today. In our society digital images play a more significant role than the traditional texts and it needs serious protection of the user's privacy for all applications. So the security of digital images has become more important and attracted much attention. The security of digital image can be achieved by digital image encryption technique. Basically Image Encryption means that convert the image into unreadable format so that third parties cannot interpret them. Many digital services require reliable security in storage and transmission of digital images. To prevent images from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital

information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. There are various encryption systems to encrypt and decrypt image data, but it can be said that there is no single encryption algorithm which satisfies the different image types. In general, most of the available traditional encryption algorithms are used for text data. Although we can use the traditional encryption algorithm to encrypt images directly, this may not be a good idea for some reasons. First, image data have their special features such as high redundancy, and high correlation among pixels. Second, they are usually huge in size, which makes traditional encryption methods difficult to apply and slow to process. Third, the decrypted text must be equal to the original text but this requirement is not necessary for image data because characteristic of human insight, a decrypted image containing small distortion is usually acceptable.

1.2.1 ADVANTAGES OF ENCRYPTION PROCESS

- It provides security for data at all times.
- Encrypted data maintains integrity. It protects privacy.
- Encryption is part of compliance.
- Encryption protects data across devices.
- Backup information is safe. > Secure outsourcing and licensing.

1.2.2 DISADVANTAGES OF ENCRYPTION PROCESS

- Forgetting passwords.
- Rising suspicions.
- Developing a false sense of security. Requiring cooperation.
- Slow in speed.

- Certification problems.
- False sense of security.
- Expensive.

1.2.3 APPLICATIONS OF ENCRYPTION PROCESS

- Astronomical applications.
- Medical applications.
- Ultrasound imaging.
- 3D image processing.
- Defense.
- Security.
- Confidential videoconferences.
- Streaming media.

1.3 COMPRESSION

Compression refers to reducing the quantity of data used to represent a file, image or video content without excessively reducing the quality of the original data. Image compression is the application of data compression on digital images. The main purpose of image compression is to reduce the redundancy and irrelevancy present in the image, so that it can be stored and transferred efficiently. The compressed image is represented by less number of bits compared to original. Hence, the required storage size will be reduced, consequently maximum images can be stored and it can be transferred in a faster way to save time, transmission bandwidth. In image compression, redundancies are classified into three types namely coding redundancy, inter-pixel redundancy and psycho visual system. Coding redundancy is present

when less than optimal code words are used, which results in coding redundancy. A result from correlations between the pixels of an image is called inter-pixel redundancy. Due to data, omitted by the Human Visual System (HVS) that is visually non-essential information is called psycho visual redundancy. The reconstructed image can be obtained by compressed data. This process is called inverse process or decompression.

1.3.1 ADVANTAGES OF COMPRESSION PROCESS

- Size reduction.
- Transmission time is shorter.
- Stores and transmit images efficiently.
- Less storage space.
- No loss of quality.
- Portable.
- Compatible with many applications.
- Reduces redundancy.
- Used to store high resolution fast moving images.

1.3.2 DISADVANTAGES OF COMPRESSION PROCESS

- There is a chance of losing data.
- Image degradation can occur.
- Time consuming.
- Larger file size.
- Quality of image is reduced.
- Chance of losing the actual contents.
- It does not support layered images.

- High maintenance.
- Costlier.

1.3.3 APPLICATIONS OF COMPRESSION PROCESS

- Broadcast television.
- Remote sensing via satellite.
- Military communication via radar, sonar.
- Teleconferencing.
- Computer communications.
- Facsimile transmission.
- Magnetic Resonance Imaging (MRI)
- Satellite images, geological surveys, weather maps.

CHAPTER 2

LITERATURE SURVEY

In this chapter, literature survey on the existing methodologies used to watermark, encrypt and compress the digital image is done. This section also explains the broad classification of each process.

2.1 SURVEY ON WATERMARKING TECHNIQUES

Digital watermarking is the technique of embedding digital marks inside a container so that there is a logical way of extracting the data embedded, while not harming the container in any perceived way. Watermarking uses cover files to deliver its messages. On the other hand, watermarking considers the cover file as the important data that is to be preserved. In Watermarking the purpose of embedded data is to deliver secret communication. In watermarking, the purpose of embedded data is to supply some additional information about the cover image such as image owner to verify image's ownership to achieve control over the copy process of digital data. In Watermarking, the object of communication is the hidden message. In digital water-marks, the object of communication is the cover. In short, Watermarking pay attention to the degree of invisibility while Watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations (rotation, cropping,

filtering). Digital watermarking is a method used to improve the ownership over an image by replacing low level signals directly into the image. Digital watermarking method is also used for tamper proofing and authentication. The digital image watermarking is divided into two parts (watermark embedding and watermark extraction).

2.1.1 BROAD CLASSIFICATION OF WATERMARKING TECHNIQUES

Visible watermarks: A visible alteration of the digital image by appending a "stamp" on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.

Invisible watermarks: By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non- repudiation.

Another way of classifying watermarking technique is a factor of its usage: robust, fragile, or semi-fragile, and spatial or spectral watermarks.

Robust watermarks: Watermarks can be used to hold knowledge of ownership. Such watermarks need to remain steadfast to the original image to do what they advertise. The intactness of the watermark is a measure of its robustness. These watermarks must be able to withstand normal manipulations

to the image such as reduction of image size, lossy compression of image, changing the contrast of the Images, etc.

Fragile watermarks: These are complementary to robust watermarks and are, as a rule, more change-sensitive than robust watermarks. Their use lies in being able to pin-point the exact region that has been changed in the original watermarked image. The methods of fragile watermarking range from checksums and pseudo- random sequences in the LSB locale to hash functions to sniff any changes to the watermark.

Semi-fragile watermarks: These watermarks are a middle ground between fragile watermarks and fragile watermarks. They engulf the best of both worlds and are more resilient than fragile ones in terms of their robustness. They also are better than robust watermarks in terms of locating the regions that have been modified by an unintended recipient.

Spatial watermarks: Watermarks that are applied to the "spatial domain of the image" are said to be spatial watermarks.

Spectral watermarks: These are watermarks that are applied to the "transform coefficients of the image".

2.1.2 VITAL PARAMETERS IN DIGITAL WATERMARKING

1. Data payload: is the amount of information, i.e. the number of bits that is encoded by the watermark.

2. Fidelity: the distortion that the watermarking process is bound to introduce, should remain imperceptible to a human observer.

3. Robustness: the ability of the detector to extract the hidden watermark from some altered watermarked data.

4. Security: it enhances the difficulty for the attackers to extract the watermark.

2.1.3 CRITERIA FOR A GOOD WATERMARK

Though watermarks belong to different categories, some of the general characteristics that watermarks must possess are the following:

1. The watermark must be strongly bound to the image and any changes to the watermark must be apparent in the image.

2. Watermark must also be able to withstand changes made to the image. Such changes include modifications and enhancements of images such as size modifications, cropping, lossy compression, to name a few.

3. The watermark must not undermine the visual appeal of the image by its presence (especially for invisible watermarks).

4. Watermark must be indelible and must be able to survive linear or nonlinear operations on the image.

The following are criteria for a visible watermark:

1. The watermark must be apparent on all kinds of images.

2. The size of the watermark is crucial. The more pervasive the watermark the better so that the watermarked area cannot be modified without tampering with the image itself.

3. The watermark must be fairly easy to implant in the image.

2.1.4 THE WATERMARKING PROCESS.

The watermarking process comprises of the following stages:

1. Embedding stage
2. Extraction phase
3. Distribution stage
4. Decision stage

Embedding stage: In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients.

Distribution stage: The watermarked image obtained above is then distributed through digital channels (on an Internet site). In the process, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a few. Peter Meerwald refers to the above as "coincidental attack". Any of the above may put the watermarking scheme to test, as we will see in the ensuing section. In addition, malicious attacks also are possible in this stage

to battle with the watermark. These are referred to in Meerwald's work as "hostile attacks".

Extraction stage: In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image.

Decision stage: In this stage, the extracted watermark is compared with the original watermark to test for any discrepancies that might have set in during distribution. A common way of doing this is by computing the Hamming distance.

2.1.5 WATERMARKING TECHNIQUES

Watermarking is the technique to hide the secret information into the digital media using appropriate algorithms. There are various algorithms used to hide the information. They are categorized as:

A. Spatial Domain

B. Frequency or transform domain

A. Spatial Domain Approach

The earliest watermarking techniques are mainly this kind and the simplest example is to embed the watermark into least significant bits (LSBs) of the image pixels. However, this technique has relatively low information hiding capacity and can be easily erased by lossy image compression.

B. Frequency Domain Approach

Another way to produce high quality watermarked images is by first transforming the original image into the frequency domain by the use of Fourier. Discrete Cosine or Wavelet transforms for example. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then inverse-transforming the marked coefficient forms the watermarked image. The use of frequency based transforms allows the direct understanding of the content of the image; therefore, characteristics of the human visual system can be taken into account more easily.

Examples of Implementation

1. Cox et al. used the spread spectrum communication for digital multimedia watermark.

2. Hsu and Wu embedded an image watermark into selectively modified middle frequency of discrete cosine transform (DCT) coefficients of container image.

3. Joseph et al. developed a digital image watermarking using the Fourier-Mellin transform that is invariant to image manipulations or attacks due to rotation, scaling and translation.

2.1.6 REVIEW ON IMAGE WATERMARKING TECHNIQUES

M. Barni et al.[1] have developed an improved wavelet-based watermarking through pixel-wise masking. It is based on masking watermarks

according to characteristics of HVS. The watermark is adaptively added to the largest detail bands. The watermark weighing function is calculated as a simple product of data extracted from the HVS model. The watermark is detected by correlation.

N. Kaewkamnerd[7] and K.R. Rao developed a wavelet based image adaptive watermarking scheme. Embedding is performed in the higher level sub- bands of wavelet transform, even though this can clearly change the image fidelity. In order to avoid perceptual degradation of image, the watermark insertion is carefully performed while using HVS.

Bo Chen and Hang Shen[2] developed a new robust fragile double image watermarking algorithm using improved pixel-wise masking model and a new bit substitution based on pseudorandom sequence. The method embeds robust and fragile watermarks into the insensitive part and sensitive part of wavelet coefficients making two watermarks non interfering.

Peng Liu and Zhizhong Ding[17] proposed a blind image watermarking scheme based on wavelet tree quantization. The largest two coefficients are selected as significant coefficients and the difference between them is taken as a significant difference. A watermark bit is embedded by comparing the significant difference with an average significant difference value and maximum difference coefficients are quantized

Gupta et al.[25]implemented a robust and secured image watermarking using DWT and Encryption with QR Codes. In this algorithm embedding watermarking is presented by using DWT and encrypted with QR codes. Here the cover image is selected and DWT is applied on it. A key K is selected to generate the QR code as a secret key. QR code and watermark image is encrypted by using XOR operation. Then the encrypted watermark is embedded into the cover image and inverse DWT is applied on the embedded

watermark image. For extraction, simply apply the DWT on the cover image. This algorithm is quite simple because of the use of simple X-OR operation for encryption. This algorithm is suitable on different kind of attacks on watermarked images like JPEG Compression, Poisson Noise Attack, Salt & Pepper Noise and Gaussian Noise

Hina Lala [5]proposed a digital image watermarking technique based on discrete wavelet transform using alpha blending technique. This technique embeds visible watermarks into the cover image. The cover image is required in the extraction process. The quality of recovered watermark image and watermarked image depends on the scaling factors k and q.

Xiang-Gen Xia et al.[26] proposed a watermarking technique based on the Discrete Wavelet Transform (DWT) with multiresolution watermarking method. They perform two-level decomposition using the Haar wavelet filters. The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross- correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. They test algorithm with common image distortions

Maha Sharkas et al.[11] Senior Members IEEE, proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded the secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the

watermarked image. They applied compression, low pass filtering, salt and pepper noise and luminance change attack into the watermarked image to increase the robustness of the technique. In all four attacks the secondary watermark was detectable. PSNR value was calculated as 44.1065dB.The disadvantage of this method was Secondary watermark was still detectable when multi threshold DWT technology was applied on the watermarked image.

Cheng et al.[10] proposed an algorithm which was based on embedding the watermark image three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter.

P.Ramana Reddy et al.[19] proposed an algorithm that embeds and extracts the watermark in frequency domain and it is checked for salt and pepper & Gaussian noise attacks. They applied watermark in the DWT coefficients of the original image Robustness of the watermarked image increases with the increase in gain k but the quality of the final watermarked image is reduced.

Preeti Gupta[18] proposed cryptography based blind image watermarking techniques that embed more number of watermark bits in the grayscale cover image. They applied blind watermarking technique that uses watermark nesting and encryption. An extra watermark is embedded into the main watermark then the main watermark is embedded into the DWT domain of the cover image. This technique embeds more bits in the cover image.

2.2 SURVEY ON ENCRYPTION PROCESS

Recently, the transmission of data through the network is increasing rapidly. This provides instant access or distribution of digital data. Visual

cryptography is the technique used in the latest technology to transmit the secret information in images i.e., called secret image. Secret image sharing is an important subject in the field of communication technology, information security and production. However, security can be introduced in many ways like transmitting password, image hiding, watermarking technique, authentication and identification. But the drawback of these methods is that the secret images can be protected in a single information carrier. If it is lost once, the information carrier is either damaged or destroyed. To overcome this problem, VCS secret sharing scheme was introduced by Naor and shamir, the secret image is split up into the number of shares and transmitted to the number of participants. A visual secret sharing scheme is a technique used to encrypt the secret image by splitting the shares into several pieces and distributing it into the corresponding participants. A set of qualified participants can be able to retrieve the secret image by overlapping the shares in correct order.

A traditional VCS takes the secret image as input and number of shares as output, it satisfies two conditions

1) secret images can be recovered by any qualified subset of shares;

2) any forbidden subset of shares cannot gain any information about the secret image.

For example, In traditional (k,n)-VCS, the secret image is revealed if k of n shares are known. Any number of shares less than k is not sufficient to reveal a secret image where, k is the number of participants and n is the number of shares.

Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received

person can decrypt the transparencies using our tool, thus getting the original image. Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using our application here sender gets the two or more transparencies of the same image. It provides an option to the end user of encryption. The end user can divide the original image into a number of different images. Using our application, we can send encrypted images that are in the format of GIF and PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended person by other means [source]

Image

An image is essentially a 2-D signal processed by the human visual system. The signals representing images are usually in analog form. However, for image processing, storage and transmission, they are converted from analog to digital form. A digital image is basically a 2-D array of pixels.

Images are formed of the significant part of data, particularly in remote sensing, biomedical and video conferencing applications. The use of and dependence on information and computers continue to grow, so does our need for efficient ways of storing and transmitting large amounts of data.

Pixel

In a digital image, a pixel is a single point in a raster image. It is the smallest unit of picture that can be controlled, and is the smallest addressable screen element Each pixel has its own address. The address of a pixel corresponds to its coordinates. They are usually arranged in a 2-D grid, and are often represented with dots or squares,

2.2.1 PURPOSE OF CRYPTOGRAPHY

Cryptography provides security to ensure the privacy of data, non-alteration of data and so on. Nowadays cryptography is widely used due to its great security. There are various cryptography goals are following as,

A. Confidentiality

The transmission of data from one computer to another computer has to be accessed by an authorized user and is not accessed by anyone else.

B. Authentication

The transmission of data from one computer to another computer has to be accessed by an authorized user and is not accessed by anyone else.

C. Integrity

Only the authorized party is allowed to modify the transmitted information. And an unauthorized person should not modify it between the sender and receiver.

D. Non Repudiation

Ensures the message that the sender or the receiver should be able to deny the transmission.

E. Access Control

The authorized persons are only able to access the information while in transfer.

2.2.2 TYPES OF CRYPTOGRAPHY

Cryptography technique is to secure the secret message when it is transferred from one place to another place over the networks. The cryptography contains the two main categories as follows,

A. Symmetric Key Cryptography

B. Asymmetric Key Cryptography

A. Symmetric Key Cryptography

Secret key cryptography is also known as symmetric key cryptography. In this type both the sender and the receiver know the same secret key. The sender encrypts the data or the information using the secret key and the receiver decrypts the information using the same secret key which is playing a very important role.

B. Asymmetric Key Cryptography

Asymmetric cryptography is used as an encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys. Public key cryptography, also called asymmetric key cryptography which is using a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The cryptography technique is using the secret message transfer from one place to another place over the networks. The cryptography technique requires some algorithms for encrypting the data.

2.2.3 EXISTING SYSTEM

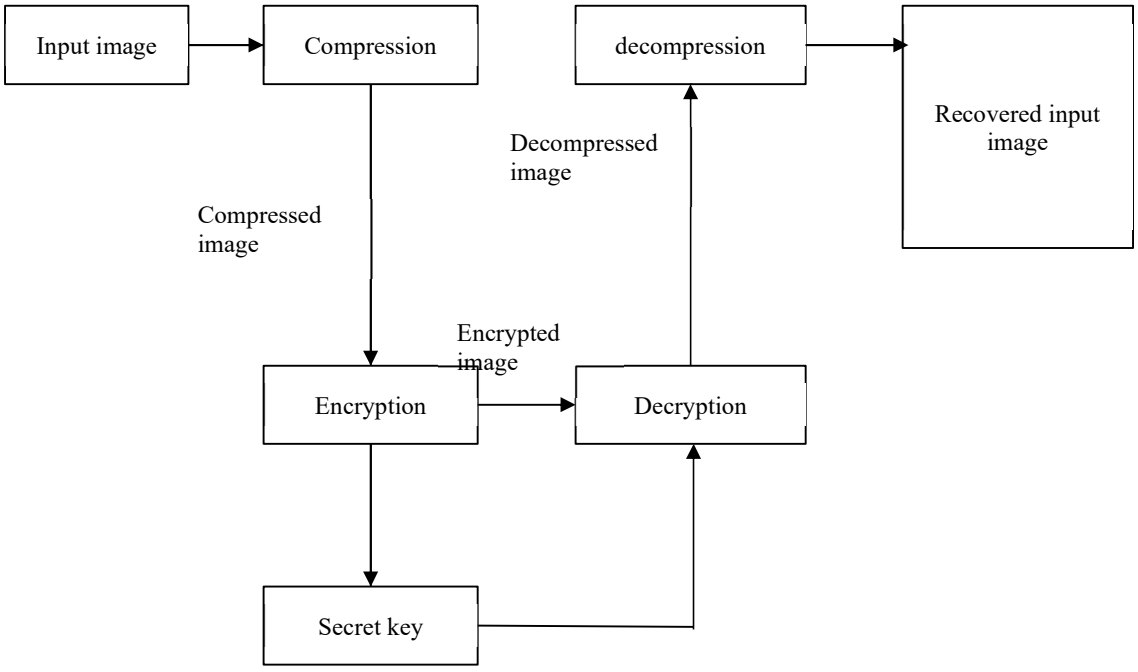

Figure 2.1: Existing system using compression and encryption

In figure 2.1 the first operation is encryption, which aims to modify the compressed information to make them unreadable to whoever does not have the necessary authorization to see them; the second is an operation of compression which consists in reducing the size of information to be transmitted, by removing redundant information from them. However, these two operations are often carried out separately, although they are strongly bound and one influences the other. In the existing system, to carry out these two operations (compression and encryption) together with a new system able to amalgamate spectral information. This system is based on one hand on the rarity of similitude in two different images and on the second hand on the Discrete Cosine Transformation "DCT", a transformation used for a long time in JPEG compression.

2.2.4 RANDOM PERMUTATION

The technique involves three different phases in the encryption process.

A. Image encryption phase

B. Key generation phase

C. Decryption phase

The first phase is the image encryption where the image is split into blocks and these blocks are permuted. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is generated with valid information about the values used in the encryption process. Most of the encryption processes first generate the key and then do the encryption process. This technique generates a relation between the encryption process and the key.

A. Image encryption phase

The image encryption process first selects a random color image of n*n size. This image is split into 4 blocks and numbered. These numbered blocks are shuffled based on the 24 permutations available. Each sub block is further shuffled. A random number is selected which lies in the range of 0 to 255. These rows and columns of the images are shifted based on the random number that is selected.

B. Key generation phase

All the information about encryption is kept in the key. Most of the encryption processes happen based on the key. Here as stated the key is built after the encryption process. The information used in the encryption process is embedded in the key. The key is 64 hits in size. Each byte is divided into a segment. The key is composed of 8 segments.

C. Decryption phase

The process of decryption involves obtaining the key that is generated and the shares. These shares are identified by comparing the information in the key with the watermark. Once the identification process is done the permutation information and the random number from the key is obtained to implement the inverse of the permutations to reveal the secret.

2.2.5 REVIEW ON IMAGE ENCRYPTION TECHNIQUES

K.Brindha et al.[3] proposed image encryption with the DES algorithm. The resultant final encrypted output image is similar to the input image with no loss and transmitted with more security. It contains three steps: Initially, the byte array is obtained by converting the input image and then the string is obtained by converting the byte array and then it is passed in DES for encryption. Finally, an encrypted image is obtained at the output which is the same as the input image.

Dr.P.Mahajan et al.[12] have surveyed and analysed experiments for AES, DES and RSA algorithms and their performance are compared. The performances of these algorithms are determined based on the stimulated time. This stimulated time is analysed at the time of both encryption and decryption.

K.Saraf et al.[23] have proposed image and text encryption and decryption using advanced encryption standard (AES) algorithm. Same encryption and decryption technique cannot be used for all types of data. If the images differ by its size, then different algorithms are used. With this variation in AES algorithm the image as well as text can be protected.

Q.A.Keste[9] focused on a new technique of encryption which is based on the RGB pixel shuffling and transposition. This method proved that it provides more security than other methods. After shifting of the RGB components, the swapping of RGB values will take place. This swapping gives more security for images against all attacks.

A.Kaur et al.[8] have implemented different chaotic maps for image encryption. The chaotic map includes sine map, Arnold cat map, tent map, logistic map. Image compression and image encryption is one of the applications of the chaotic systems. For efficient encryption two maps are combined. By the combination of cryptography and chaos theory, a high level of security can be achieved.

2.3 SURVEY ON COMPRESSION TECHNIQUES

Consider an application scenario in which a content owner Alice wants to securely and efficiently transmit an image I to a recipient Bob, via an untrusted channel provider Charlie. Conventionally, this could be done as follows. Alice first compresses I into B, then encrypts B into Ie using an encryption function $E_K(\cdot)$, where K denotes the secret key, as illustrated in Fig. 2.2. The encrypted data Ie is then passed to Charlie, who simply forwards it to Bob. Upon receiving Ie, Bob sequentially performs decryption and decompression to get a reconstructed image I.

Even though the above Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive to compress her data, and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when Alice uses a resource-deprived mobile device. In contrast, the channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Charlie, who typically has abundant computational resources. A big challenge within such Encryption-then- Compression framework is that compression has to be conducted in the encrypted domain, as Charlie does not access the secret key K. This type of system is demonstrated in Fig. 2.3.

The possibility of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years. At the first glance, it seems to be infeasible for Charlie to compress the encrypted data, since no signal structure can be exploited to enable a traditional compressor. Although counter- intuitive, Johnson et al showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency or the information-theoretic security. In addition to the theoretical findings, also proposed practical algorithms to lossless compress the encrypted binary images. Schonberg et. al later investigated the problem of compressing encrypted images when the underlying source statistics is unknown and the sources have memory. By applying LDPC codes in various bit-planes and exploiting the inter intra-correlation, Lazzeretti and Barni presented several

methods for lossless compression of encrypted grayscale/color images. Furthermore, Kumar and Makur applied the approach of to the prediction error domain and achieved better lossless compression performance on the encrypted grayscale/color images. Aided by rate-compatible punctured turbo codes, Liu et al developed a progressive method to losslessly compress stream cipher encrypted grayscale/color images. More recently, Klinc et al, extended Johnson's framework to the case of compressing block cipher encrypted data.

To achieve higher compression ratios, lossy compression of encrypted data was also studied. Zhang et. Al proposed a scalable lossy coding framework of encrypted images via a multi-resolution construction, compressive sensing (CS) mechanism was utilized to compress encrypted images resulting from linear encryption. A modified basis pursuit algorithm can then be applied to estimate the original image from the compressed and encrypted data. Another CS-based approach for encrypting compressed images was reported. Furthermore, Zhang designed an image encryption scheme via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently compressed by discarding the excessively rough and fine information of coefficients in the transform domain. Recently, Zhang et. al suggested a new compression approach for encrypted images through multi-layer decomposition. Extensions to blind compression of encrypted videos were developed.

Despite extensive efforts in recent years, existing systems still fall significantly short in the compression performance, compared with the state-of- the-art lossless/lossy image and video coders that require unencrypted inputs. The primary focus of this work is on the practical design of a pair of image encryption and compression schemes, in such a way that compressing the encrypted images is almost equally efficient as compressing their original, unencrypted counterparts. Meanwhile, a reasonably high level of security

needs to be ensured. If not otherwise specified, 8-bit grayscale images are assumed. Both lossless and lossy compression of encrypted images will be considered. Specifically, we propose a permutation- based image encryption approach conducted over the prediction error domain. A context-adaptive arithmetic coding (AC) is then shown to be able to efficiently compress the encrypted data. Thanks to the nearly i.i.d property of the prediction error sequence, negligible compression penalty (< 0.1% coding loss for lossless case) will be introduced. Furthermore, due to the high sensitivity of prediction error sequence against disturbances, a reasonably high level of security could be retained.

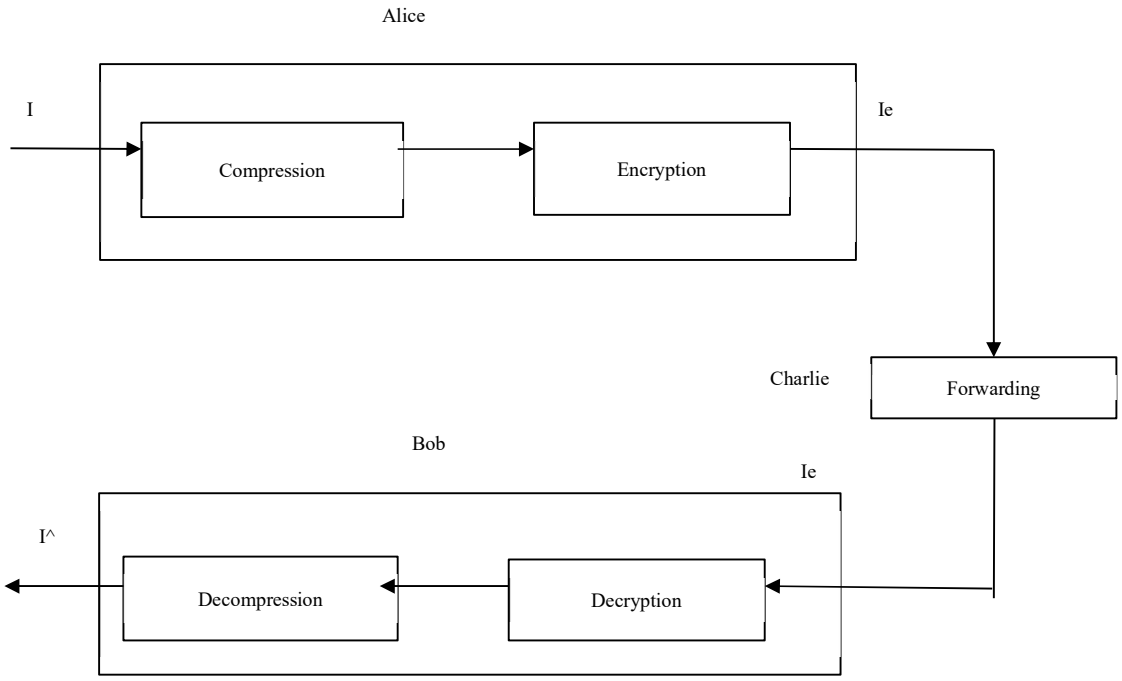

Figure 2.2: Traditional Compression-then-Encryption system

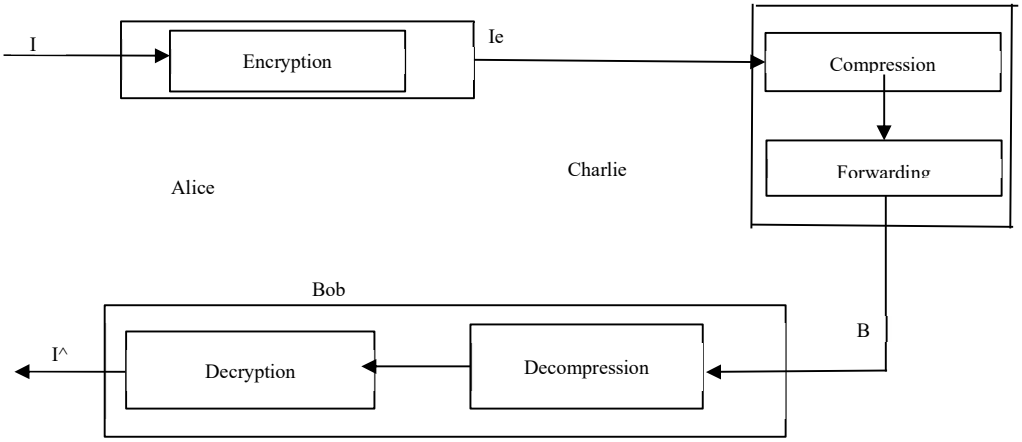

Figure 2.3: Encryption-then-Compression system.

2.3.1 IMAGE COMPRESSION TECHNIQUES

There are two types of compression algorithm

1. Lossless compression.
2. Lossy compression.

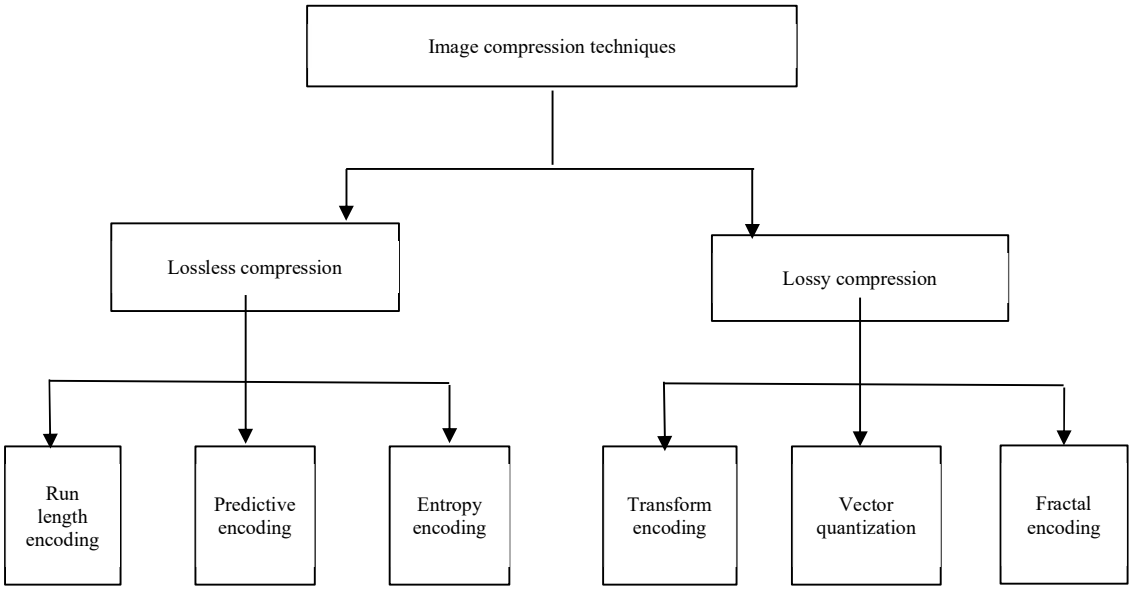

Figure 2.4: Classification of compression techniques

Figure 2.4 shows the broad classification of digital image compression techniques and the brief notes about each technique are discussed below.

A. Lossless Compression:

In the lossless compression the compressed image is totally a replica of the original input image, there is not any amount of loss present in the image. It includes

a. Run Length Encoding

b. Entropy encoding

c. Predictive Coding

a. Run Length Encoding

Run length Encoding (RLE) is one of the simplest image compression techniques. It consists of replacing a sequence (run) of identical symbols by a pair containing the symbol and the nin length. It is used as the primary compression technique in the 1-D CCITT Group 3 fax standard and in conjunction with other techniques in the JPEG image compression standard.

b. Entropy encoding

Entropy encoding is a lossless data compression scheme that is Independent of the specific characteristics of the medium. One of the main types of entropy coding creates and assigns a unique prefix-free code to each unique symbol that occurs in the input. These entropy encoders then compress data by replacing each fixed-length input symbol with the corresponding variable length prefix-free output codeword. The length of each codeword is approximately proportional to the negative logarithm of the probability. Therefore, the most common symbols use the shortest codes.

c. Predictive Coding

Predictive Coding Technique constitutes another example of exploration of intermixed redundancy, in which the basic idea is to encode only the new information in each pixel. This new information is usually defined as the difference between the actual and the predicted value of the pixel. The predictor's output is rounded to the nearest integer and compared with the actual pixel value: the difference between the two-called prediction errors. This error can be encoded by a Variable Length Coding (VLC). The distinctive feature of this method lies in the paradigm used to describe the images. The images are modelled as non-causal random fields.

B. Lossy Compression

In lossy compression the compressed image is not the same as the input image, there is some amount of loss present in the image. It includes

a. Transform encoding

b. Vector Quantization

c. Fractal Coding

a. Transform encoding

Transform coding is a type of data compression for "natural" data like audio signals or photographic images. The transformation is typically lossy, resulting in a lower quality copy of the original input. In transform coding, knowledge of the application is used to choose information to discard, thereby lowering its bandwidth. The remaining information can then be compressed via a variety of methods. When the Output is decoded, the result may not be identical to the original input.

b. Vector Quantization

Vector quantization (VQ) technique is the extension of Scalar quantization in multiple dimensions. This technique develops a dictionary of fixed-size vectors which are called code vectors. A given image again partitioned into non-overlapping blocks called image vectors. Then for each image vector, the closest matching vector in the dictionary is determined and its index in the dictionary is used as the encoding of the original image vector.

c. Fractal Coding

Fractal Coding decomposes the image into segments by using standard image processing techniques such as edge detection, colour separation, and spectrum and texture analysis. Then each segment is looked up in a library of fractals. The library actually contains codes called iterated function system (IFS) codes, which are compact sets of numbers. Using a systematic procedure, a set of codes for a given image are determined, such that when the IFS codes are applied to a suitable set of image blocks yield an image that is a very close approximation of the original.

2.3.2 REVIEW ON IMAGE COMPRESSION TECHNIQUES

M. Mozammel Hoque Chowdhury[13] suggests an image compression scheme based on discrete wavelet transformation. This reduced the redundancy of the image data in order to be able to store or transmit data in an efficient form. It was noted that discrete wavelet transform offers less computational complexity without any sacrifice in image quality. First the image is decomposed into sub- hands and then the resulting coefficients are compared with a threshold. Coefficients below the threshold are taken as zero. Finally, the coefficients above the threshold value are selected and encoded with a loss less compression technique. He also noted that wavelets are well

suited to time-limited data and wavelet based image compression technique maintains better image quality with less errors.

Security can be given to the image along with effective compression. Oh Naveen[15] in his paper discussed the role of E2W in providing additional security to images along with its main function of compression.

The process starts by providing image security with compressing the image using EZW. This will generate four different data vectors must of which one is coded son. The coded sequences are taken and convert it Into 2D sequence, On the 2D data chaos based scrambling method is applied using two initial conditions keys for row and column respectively. The user must provide the same key at the time of descrambling and reconstruction of image. To reconstruct the Image using coding process, the encoded bit stream in the same order as at the time of generation is required. This helps in making the algorithm more robust.

Dalvir Kaur et al.[4]proposed a compression technique using the two Je methodologies Huffman coding and Lempel Ziv Welch coding to compress images. First the image is compressed with Huffman coding resulting in the Huffman tree and Huffman Code words. After that Huffman code words are connected together and then compressed by using Lempel Ziv Welch coding. Filly Retinex algorithm is used on compressed images to enhance the contrast of image and improve the quality of image. The amount of compression achieved depends upon the characteristics of the source to a great extent. It was noted that the higher data redundancy helps to achieve more compression. Reproduced image and the original image are equal in quality by using Retinex Algorithm, as it enhances the image contrast using MSR

Mridul Kumar Mathur et al.[14]suggested a lossless image compression based on the Huffman algorithm is presented. The image is converted into an

array using Delphi image control tool. Huffman coding method is used to move redundant codes from the image and compress a BMP image file.. This image compression scheme is well suited for gray scale (black and white) bitmap images. Huffman coding suffers from the fact that the decompressed needs to have some knowledge about the probabilities of the symbols in the compressed files. It needs more bits to encode the file if this information is unavailable.

Set partitioning in hierarchical trees (SPIHT) is a wavelet based algorithm which is computationally very fast and offers a good compression ratio. [16, 21] It is an extension of embedded zero tree wavelet (EZW) coding method. It is based on spatial orientation trees and makes use of a set partitioning sorting algorithm. SPIHT defines parent-children relationships between similar sub bands to establish spatial orientation trees. The SPIHT algorithm encodes the image file using three lists such as LIP, LIS and LSP. The LIP list contains the individual coefficients that have magnitudes smaller than the threshold values. LIS list contains the overall wavelet coefficients that are defined in tree structure with magnitudes smaller than the threshold values. LSP is the set of pixels having magnitude greater than threshold value. Sorting process and refinement process is carried out to select the coefficients that are important. Precise rate control is an important characteristic of the SPIHT algorithm.

CHAPTER 3

EFFICIENT IMAGE WATERMARKING AND ENCRYPTION WITH LOSsLESS COMPRESION (WELC) FOR WIRELESS COMMUNICATION

3.1 METHODOLOGY

There is rapid development in multimedia and network technology where privacy and security become the Important is in multimedia which is transmitted openly over the network. In this work, we design and Implement huge encryption and compression system, in which lossy compression is considered. The proposed system operated scheme for image encryption with a permutation method which is shown to provide reasonably high level of security. Here a new image compression algorithm is implemented using the 2D 3 LEVEL Wavelet Transform that can be used to efficiently compress the encrypted image. More notably, the approach applied for compensation to encrypted images proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). In this work, we design and implement an image with a watermarking, encryption and compression system, in which the lossless compression is considered. Hiding the secret image in the cover image is known as Watermarking. For enhancing the security of the image, encryption is done. Encryption is defined as converting the embedded image into a noisy image. After encrypting an image, compression is performed. And then the image is transmitted using OFDM technique. At the receiver, decompression then decryption and reverse

Watermarking process is done. As a, the secret image will get extracted from the cover image as shown in Figure 3.1.

1. Algorithm for Image Watermarking Image

Watermarking using 2D-3 Level Wavelet Transform

2. Algorithm for Image Encryption

Image Encryption using 64-bits Blowfish Algorithm

3. Algorithm for Image Compression

Image Compression using Vector Scanning SPIHT (Set Partitioning in Hierarchical Tree) algorithm

3.2 OVERVIEW OF PROPOSED SYSTEM

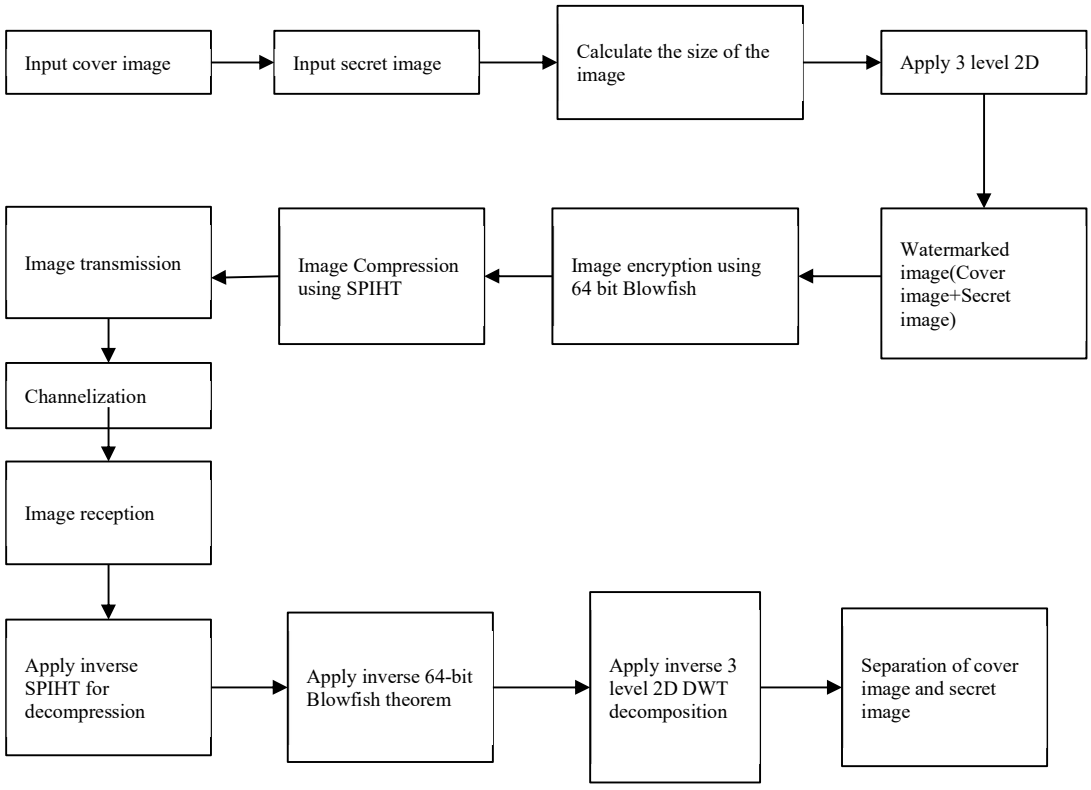

figure 3.1: Overview of proposed system

3.3 IMAGE WATERMARKING USING 2D-3 LEVEL WAVELET TRANSFORM

A. WATERMARK EMBEDDING ALGORITION

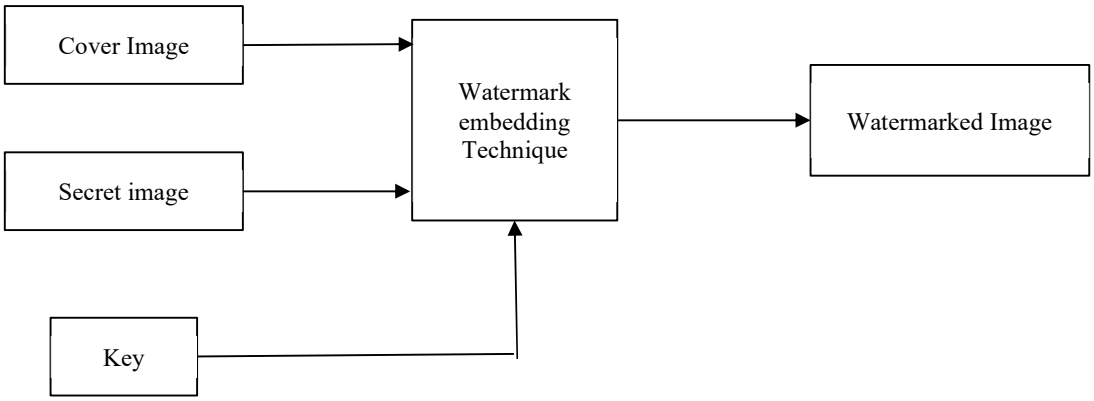

Figure 3.2: Block diagram of Watermark embedding

In case of two-dimensional image, after a DWT transform, the image is divided into four comers, upper left comer of the original image, lower left corner of the vertical details, upper right corner of the horizontal details, lower right corner of the component of the original image detail (high frequency). You can then continue to the low frequency components of the same upper left comer of the 2nd, 3rd inferior wavelet transforms. On the basis of such considerations, the algorithm uses a different colour image multiplied by the weighting coefficients of different ways to solve the visual distortion, and by embedding the watermark, wavelet coefficients of many ways, enhance the robustness of the watermark. The process of watermark embedding is shown in figure 3.2.

After that we select the ordered coefficient from to N to get N coefficient. The formulae of watermark embedding are as follows.

Where the parameter a is called embedding intensity and their effect of validity of the algorithm directly is applied after this process, after that apply the inverse wavelet transform to the image for finding out watermark image.

ALGORITHM OF EMBEDDING SECRET IMAGE USING HAAR WAVELET:

Step 1: Image Acquisition for Cover Image (Ic)

Step 2: Determine size of Cover image (Ic)

Step 3: Image Acquisition for Secret Image (Im)

Step 4: Read the Secret image (Im)

Step 5: Prepare Im as message vector

Step 6: Image Acquisition for Key Image

Step 7: Read the key image

Step 8: Decompose the Ic by using HAAR-Wavelet transform

Step 9: Generate pseudo-random number (Pn)

Step 10: Modify detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding On when message bit = 0.

Step 11: Compute IDWT in 2D to get the watermarked image

Step 12: Filter Gaussian and random noise

Step 13: Prepare filtered watermarked image to display

B. WATERMARK EXTRACTION ALGORITHM

The extraction algorithm process is the inverse of the embedding process. The operation of channel separation is applied on the watermarked color image to generate its sub images, and then 2-level discrete wavelet transform is applied on the sub images to generate the approximate coefficients and detail coefficients. For this purpose the following formulae is used W(i) = (Yw(i)+Yo(i))/a.

After this Execution the Inverse 2-level discrete wavelet transform is applied on watermark data to generate three watermark images extracted.

ALGORITHM OF EXTRACTING SECRET IMAGE USING HAAR WAVELET:

Step 1: Read the decrypted watermarked image (Is)

Step 2: Decompose the Ic and Is by using HAAR-Wavelet

Step 3: Generate message vector of all ones transform

Step 4: Find the correlation between the original and modified coefficients

Step 5: Turn the message vector bit to 0 if the correlation value is greater than mean correlation value

Step 6: Prepare message vector to display secret image

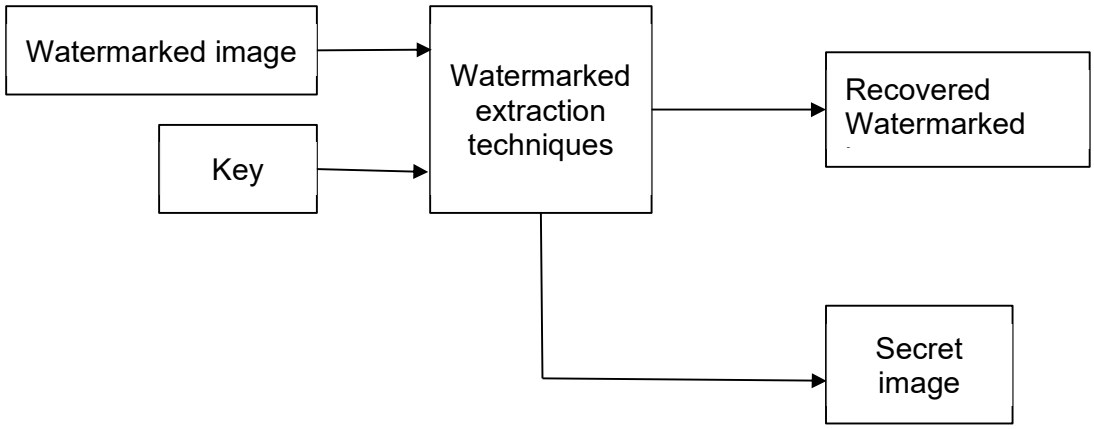

Figure 3.3: Block diagram of Watermark extraction technique

3.4 IMAGE ENCRYPTION USING 64 BLOWFISH ALGORITHM.

We propose a new image encryption Algorithm based on the 64-bits Blowfish Algorithm. Our algorithm consists of two replacement approaches; to change the value of the pixel without shuffling the image itself. To do that, we suggest using a Pixel Mapping Table (PMT) with the random shifting value to increase the ty of the image. After that, we modified the pixel value by using the w and columns replacement approach.

Algorithm for Encryption Process

Step 1: Read the watermarked image,

Step 2: Calculate the size of the watermarked image,

Step 3: Generate a pseudo random sequence with respect to row and column.

Step 4: Add the pseudo random sequence as noise to the watermarked image.

Step 5: Display the encrypted image.

Algorithm for Decryption Process

Step 1: Read the decompressed image

Step 2: Apply inverse 64 blowfish algorithm.

Step 3: Display the decrypted image.

CASE	INPUT IMAGE SIZE	ENCRYPTED IMAGE SIZE
COVER 1	24.8 KB	452 KB
COVER 2	48.7 KB	403 KB
COVER 3	97.4 KB	576 KB
COVER 4	54.5 KB	536 KB

Table 3.1. Compression of size of both the input and encrypted output image

As shown in table 3.1 the encrypted image is large in size such that the size of the scenery image is 288 KB and for the person image is 505.9KB when compared to the input size such that the scenery image is 31.1KB and for the person is 249 KB. Hence there is a lot of loss in the bandwidth. Therefore the encrypted image has to be compressed before transmission.

3.5 IMAGE COMPRESSION USING VECTOR SCANNING SPIHT (SET PARTITIONING IN HIERARCHICAL TREE) ALGORITHM

In recent years there has been an astronomical increase in the usage of computers for a variety of tasks. With the advent of digital cameras, one of the most common uses has been the storage, manipulation, and transfer of digital images. The files that comprise these images, however, can be quite large and can quickly take up precious memory space on the computer's hard drive. In multimedia application, most of the images are in color and color images contain data redundancy and require a large amount of storage space. Set partitioning Hierarchical Trees (SPIHT) is wavelet based computationally very fast and among the best image compression based transmission algorithm that offers good compression ratios, fast execution time and good image quality. We will obtain a bit stream with increasing accuracy from EZW algorithm because of basing on progressive encoding to compress an image

Modified SPIHT is a widely used compression algorithm for wavelet transformed images. Though Modified SPIHT is much simpler and efficient than many existing compression techniques as it's a fully embedded codec, provides good image quality, high PSNR, optimized for progressive image transmission, efficient combination with error protection, sort information on demand and hence requirement of powerful error correction decreases from

beginning to end but still it has some drawbacks which need to be removed for its better use so since its evolution it has undergone many changes in its original version.

This project presents MODIFIED SPIHT implementation because these are the lossy techniques and also introduce Huffman encoding technique which is lossless MODIFIED SPIHT codes the individual bits of the image wavelet transform coefficients following a bit-plane sequence. Thus, it is capable of recovering the image perfectly (every single bit of it) by coding all bits of the transform. However, the wavelet transform yields perfect reconstruction only if its numbers are stored as infinite-precision numbers. In practice it is frequently possible to recover the image perfectly using rounding after recovery, but this is not the most efficient approach. For lossless compression we proposed an integer multiresolution transformation, similar to the wavelet transform, which we called S+P transform. It solves the finite-precision problem by carefully truncating the transform coefficients during the transformation (instead of after).

Algorithm for Compression Process

Step 1: Read the encrypted image

Step 2: Apply SPIHT algorithm to compress the image

Step 3: Display the compressed image and transmit the compressed image

Algorithm for Decompression Process

Step 1: Read the received compressed image

Step 2: Apply the inverse SPIHT algorithm to decompress the image.

Step 3: Display the decompressed image.

CASE	INPUT IMAGE SIZE	ENCRYPTED IMAGE SIZE	COMPRESSED IMAGE SIZE
COVER 1	24.8 KB	452 KB	623 KB
COVER 2	48.7 KB	403 KB	621 KB
COVER 3	97.4 KB	576 KB	623 KB
COVER 4	54.5 KB	536 KB	624 KB

Table 3.2: Compression of size of the image for input, encrypted and compressed images

As shown in **table 3.2** the encrypted image of scenery and person with sizes 288 KB and 505.9KB respectively is compressed to the size of 58.4KB and 276.3KB respectively. Hence the encrypted image is compressed to a desired level. This compressed image is considered as the image to be transmitted over a wireless channel. This compressed image is of high security since the watermarked image is encrypted to a greater level by generating random noise and adding the noise to the watermarked image.

3.6 ADVANTAGES OF PROPOSED SYSTEM

MODIFIED SPIHT algorithm is the lossless compression algorithm that reduces file size with no loss in image quality. When the file is saved it is compressed, when it is decompressed (opened) the original data is retrieved. The file data is only temporarily thrown away, so that the file can be transferred. This type of compression can be applied not just to graphics but to any kind of computer data such as spreadsheets, text documents and software applications. If you need to send files as an email attachment, then you may be best to compress it first.

A common format which is used to do this is the compressed format. If you've downloaded a software program from the Internet it may have been in this or another compressed format. When you open the file up all the original data is retrieved.

Steps involved during transmission of compressed image

Step 1: Compressed image is transmitted using OFDM technique.

Step 2: Initialize PSK modulation.

Step 3: Forward error correction is done.

Step 4: Convert column matrix into m x n Matrix.

Step 6: Convert frequency domain into time domain using IFFT.

Step 7: Cancel ICI and ISI using cyclic prefix.

Steps involved during reception of compression image

Step 1: Apply inverse SPIHT to decompress the received Image using OFDM

Step 2: Decrypt the decompressed image using inverse 64 blowfish algorithm.

Step 3: Apply inverse 3 level 2D DWT decomposition.

Step 4: Recover the cover image.

Step 5: Recover the secret image.

3.7 RESULTS AND DISCUSSION

In our proposed system we consider two cover images as input with different dimensions. In the first case based on the database a common scenery image is taken from the internet with dimensions 384 256(31.1KB) as shown in figure 3.4. In the second case a real time image of a person is taken with dimensions 1380*256(249 KB) as shown in figure 3.4.

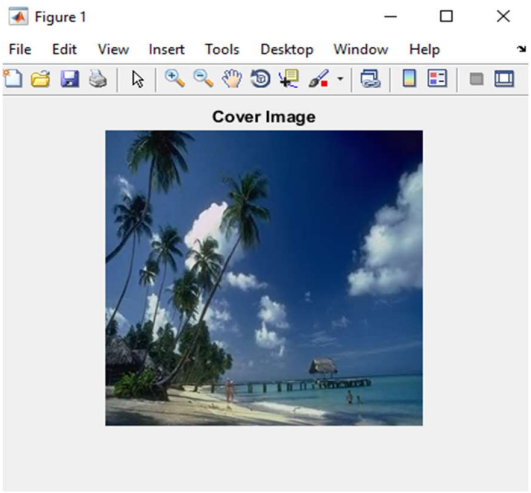

Figure 3.4: Cover Image

Then two secret images with different dimensions are taken to embed in the cover image in an invisible manner to hide and transmit it in the wireless channel. In the first case the secret image with message 'Embedding of dimensions 50*20(222 bytes as shown in figure 3.5 is used to hide in the cover image of scenery. In the second case the secret image with message 'stego-key' of dimensions 5719(214 bytes) as shown in figure 3.5 is used to hide in the cover image of a person

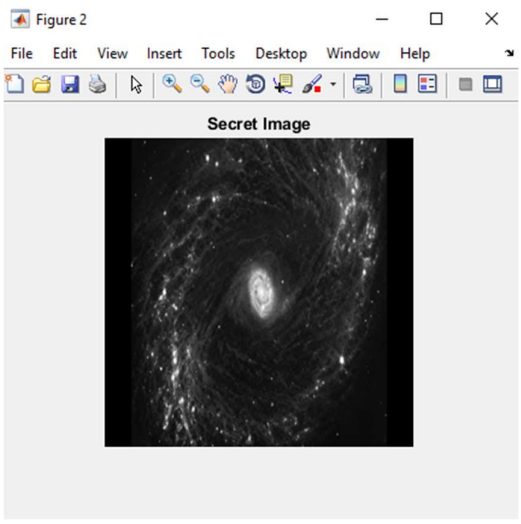

Figure 3. 5: Secret Image

In order to hide the secret image into the cover image it is necessary to convert the image from spatial domain to frequency domain and to decompose the cover image by using HAAR wavelet transform and image coefficients is obtained as shown figure 3.6

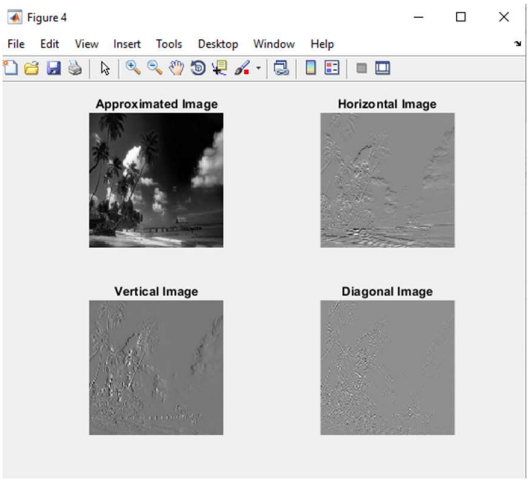

Fig 3.6 Image Co-efficients

After applying HAAR wavelet transform, the secret image is embedded in the first layer of the decomposed cover image and the embedded image is obtained as shown in figures 3.7.

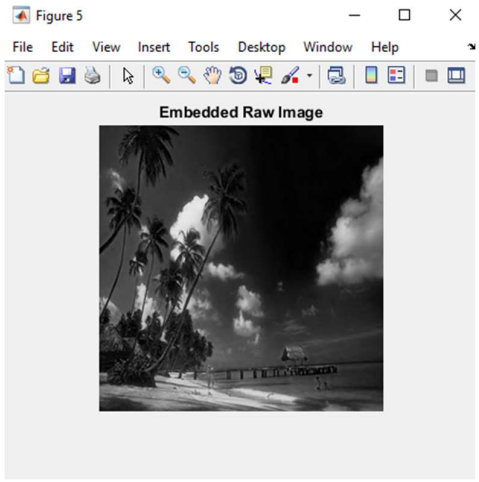

Figure 3.7: Embedded raw image

As the embedded raw image is obtained, it is found that the image is obtained with some noise and so the embedded image is filtered to get noise free embedded image then gaussian noise is filtered as shown in figures 3.8.

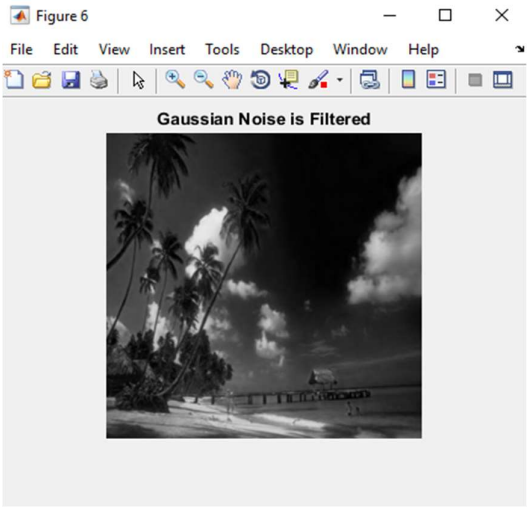

Figure 3.8: Gaussian noise filtered image

Once the Gaussian noise is filtered the random noise is also filtered and the filtered image is obtained as shown in figures 3.9.

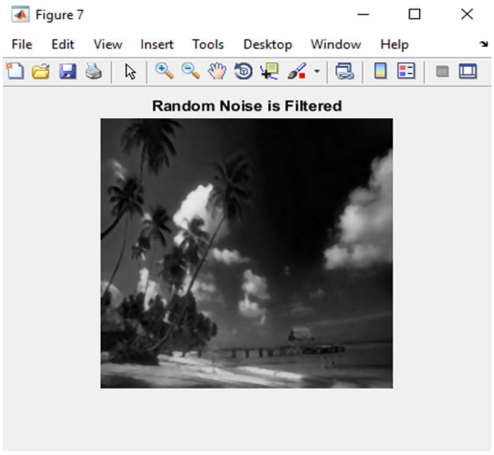

Figure 3.9: Random noise filtered image

After the filtration process to eliminate the Gaussian noise and random noise in the embedded raw image, the filtered watermarked image is obtained as shown in figures 3.10 which has the secret image hidden inside the given cover images.

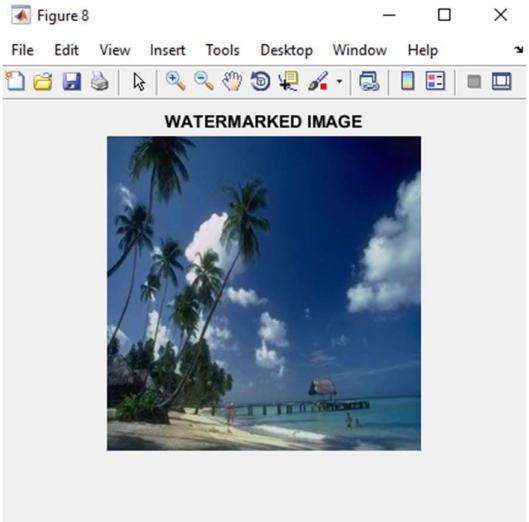

Figure 3.10: Watermarked image

In order to enhance the security level of the secret image pseudo random sequence is generated with respect to the number of rows and columns of the watermarked image and added as a noise-to-signal to the watermarked image and the encrypted image is obtained as shown in figures 3.11.

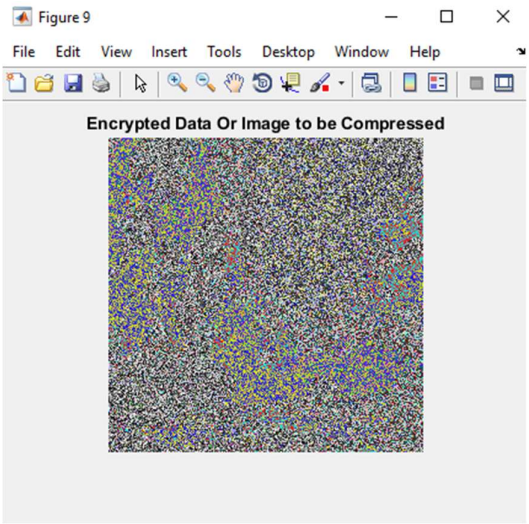

Figure 3.11: Encrypted image

The encrypted image thus obtained will have the size larger than the input image and hence the encrypted image should be compressed using SPIHT and the compressed image is obtained as shown in figures 3.12.

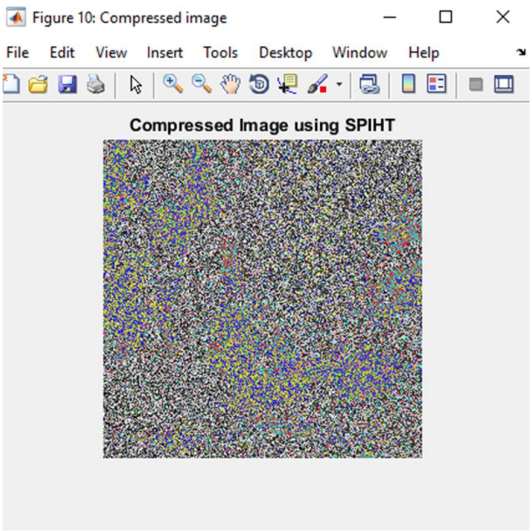

Figure 3.12: Compressed image

The compressed image thus obtained is transmitted using OFDM and the compressed transmitted image is as shown in figures 3.13.

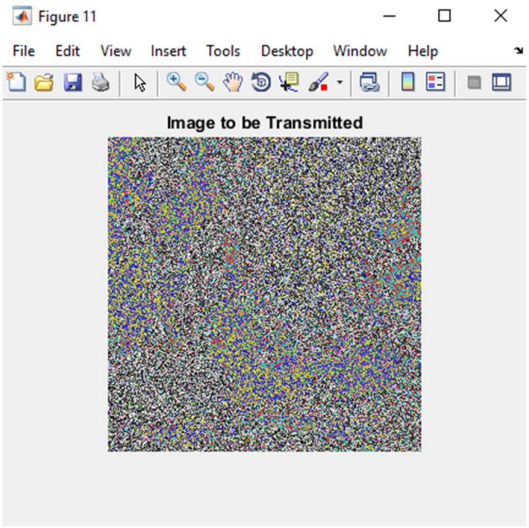

Figure 3.13: Images to be transmitted

The transmitted image is thus sent through the wireless channel using OFDM technique obtained as shown in figures 3.14 which is the received image. The transmitted image does not occupy more bandwidth since the encrypted image is compressed using SPIHT which greatly reduces the size of the image when compared to the size of the encrypted image.

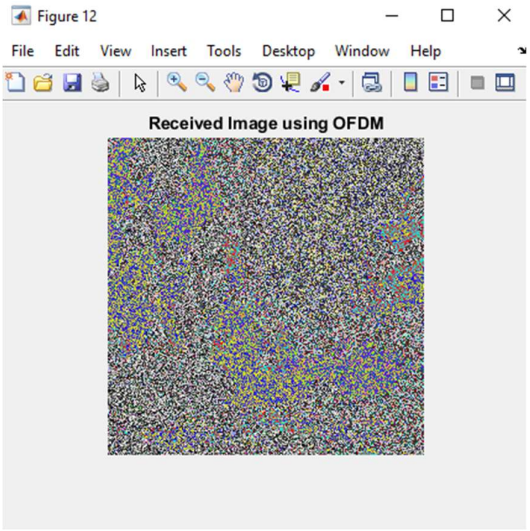

Figure 3.14: Received image

At the receiver side the image is decompressed and decrypted and the image is obtained as shown in figure 3.15.

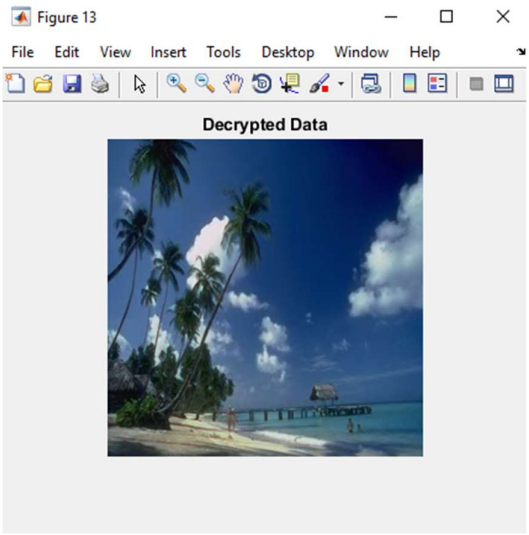

Figure 3.15: Decrypted image

Then after applying inverse 2D 3 level HAAR wavelet transform the secret image is recovered as shown in figures 3.16.

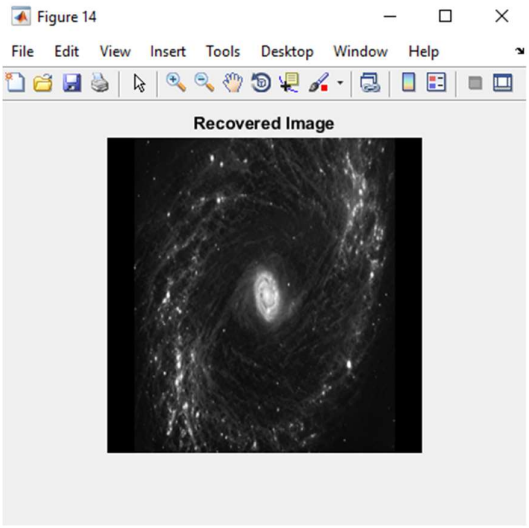

Figure 3.16: Recovered secret image

3.8. PERFORMANCE ANALYSIS

Our proposed system is subjected to various performance analyses such as PSNR, MSE and Compression ratio for each case. The PSNR, MSE and Compression Ratio can be calculated using the following formulae and the results are tabulated in table 3.3.

The PSNR is calculated by applying the formula is,

$$\textbf{Peak Signal to noise Ratio} = 10 * \log_{10}\left(\frac{255^2}{mse}\right) \textbf{ in dB}$$

$$\textbf{mse} = \frac{1}{I} * \frac{1}{J} \sum_{i=1}^{I} * \sum_{j=1}^{J} [x(i,j) - x(i,j)]^2$$

The compression ratio can be obtained by using the formula,

- K = Scaling factor
- Ib = k.Width*k.Height*k.BitDepth/8;
- cb = k.FileSize;
- Compression Ratio = (ib/cb)*2;

Cover Images used:

Figure 3.17: Cover image 1

Figure 3.18: Cover image 2

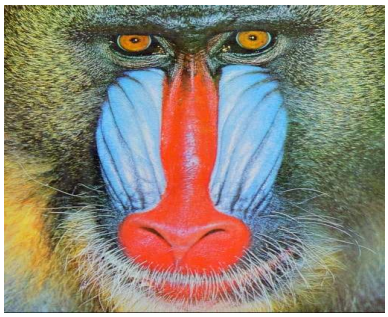

Figure 3.19: Cover image 3

Figure 3.20: Cover image 4

INPUT IMAGE USED	TIMES TAKEN TO HIDE	TIME TAKEN TO RECOVERY	MSE	PSNR	COMPRESSION RATIO
COVER 1	140.7656	270.5156	0.0288	68	9.8389
COVER 2	443.7031	508.1230	0.0256	69	10.1295
COVER 3	232.7188	452.5469	0.0289	68	10.0142
COVER 4	228.1719	454.4219	0.0290	68	10.3884

Table 3.3 Performance analysis for proposed system For hicet image

Different sets of cover images are used to hide secret image. For hicet (secret image) cover image 2 has high Peak signal-to-noise ratio(PSNR) compared to other cover images.

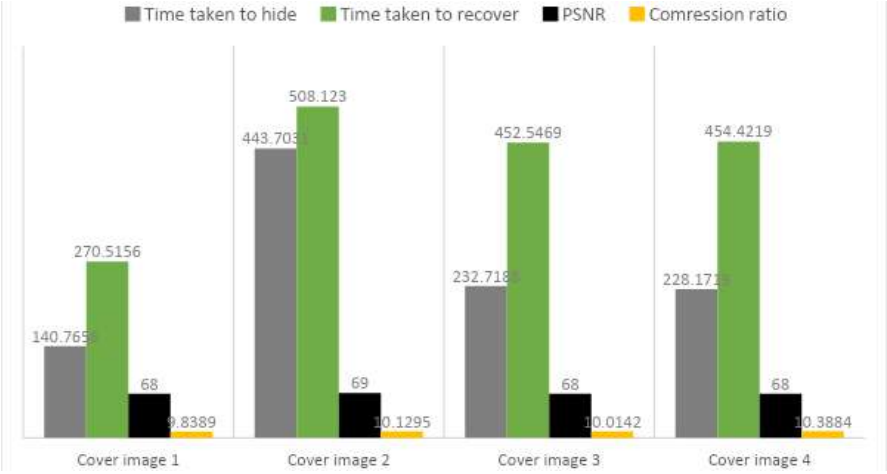

Figure 3.21: Performance analysis for hicet image

INPUT IMAGE USED	TIMES TAKEN TO HIDE	TIME TAKEN TO RECOVERY	MSE	PSNR	COMPRESSION RATIO
COVER 1	138.6875	277.2813	0	Inf	9.8610
COVER 2	121.7500	219.7188	5.8542	21	9.9996
COVER 3	124.2031	225.3438	6.4767	21	9.8400
COVER 4	121.7969	218.7344	0.5126	20	10.0223

Table 3.4 Performance analysis for proposed system For galaxy image

Different sets of cover images are used to hide secret image. For galaxy (secret image), cover image 1 has a high Peak signal-to-noise ratio(PSNR) compared to other images. The cover image 1 has mean square error equal to zero, PSNR equals to infinity, which results in no degradation in recovered secret image.

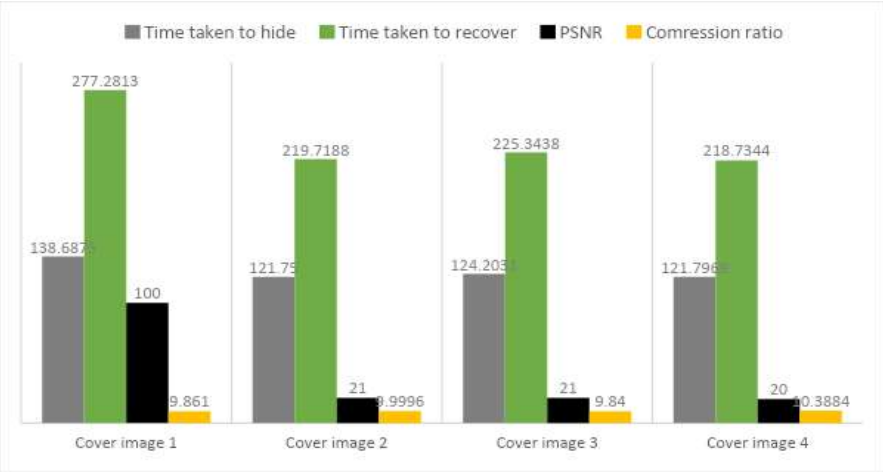

Figure 3.22: Performance analysis for galaxy image

CHAPTER 4

CONCLUSION AND FUTURE SCOPE

4.1 CONCLUSION

2D modified SPIHT algorithm can be used for any image size. When the size of the colour image increases, the time required for compression and reconstruction of the image also increases. The algorithm was tested using two colour image datasets. The results show that we obtained improvement using the 2D SPIHT Huffman algorithm in terms of compression ratio, mean-squared error, and Peak signal to noise ratio. This benchmark suite includes medical, natural, and man-made images. Our method employs motion estimation and obtained better compression than competing wavelet-based lossless compression methods on all images in our benchmark suite.

4.2 FUTURE SCOPE

The proposed system can be implemented for 3D images. The compression ratio between encrypted and compressed images can be increased to a greater level in order to save the bandwidth as it will be very much useful in the field of military applications. The size of the secret image can be increased to a greater level. The PSNR value can also be increased to a greater level in the future systems. 3D images can also be encrypted with higher security.

REFERENCES

[1]Barni M, Bartolini F, Piva, (2001) "An Improved Wavelet Based Watermarking Through Pixel Wise Masking", IEEE transactions on image processing, Vol. 10, pp.783791.

[2]Bo Chen, Hong Shen, (2009) "A New Robust-Fragile Double Image Watermarking Algorithm", Third IEEE International Conference on Multimedia and Ubiquitous Engineering, pp. 153-157

[3]Brindha, R. Sharma, and S. Saini,(2014) "Use of Symmetric Algorithm for Image Encryption," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, Issue 5, pp. 44014407, May.

[4]Dalvir Kaur, Kamaljit Kaur, (2013)"Huffman Based LZW Lossless Image Compression Using Retinex Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August

[5]Hina Lala, (2017) "Digital Image Watermarking using Discrete Wavelet Transform", International Research Journal of Engineering and Technology(IRJET), Volume: 04 Issue: 01 Jan,pp1682

[6]Jamo Mielikainen and Bormin Huang (2012)" Lossless Compression of Hyperspectral Images Using Clustered Linear Prediction With Adaptive Prediction Length "IEEE GEOSCIENCE AND REMOTE SENSING LETTERS, VOL.9,NO.6,NOVEMBER

[7]Kaewkamnerd.N and K.R. Rao,(2000) "Wavelet Based Image Adaptive Watermarking Scheme", IEEE Electronic Letters, Vol. 36,Feb., pp.312-313.

[8]Kaur (2014) "A Review of ImageEncryption Schemes Based on the Chaotic Map," International Journal of Computer Technology & Applications, vol. 5, Issue. 1, PP. 144-149.

[9]Keste, "Image Encryption based on the RGB PIXEL Transposition and Shuffling, "(2013) I. J. Computer Network and Information Security, 7, in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijenis.2013.07.05, pp.43-50, Published Online June 201

[10]Lu, W., Lu, H. and Chung, F.L. (2006) "Robust digital image watermarking based on subsampling" Applied Mathematics and Computation, vol. 181, pp. 886- 893.

[11]Maha Senior Member Sharkas, Dahlia ElShafie, and Nadder Hamdy,(2005) IEEE, "A Dual Digital-Image Watermarking Technique" World Academy of Science, Engineering and Technology 5, pp. 136-139.

[12]Mahajan, A. Sachdeva (2013) "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security (GJCSTNWS), vo, 13 Issue. 15 Version 1.0 Year.

[13]Mozammel Hoque Chowdhury, Amina Khatun (2012) "Image Compression Using Discrete Wavelet Transform", International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July.

[14]Mridul Kumar Mathur, Seema Loonker, Dr. Dheeraj Saxena,(2012) "Lossless Huffman Coding Technique For Image Compression And Reconstruction Using Binary Trees", IJCTA, Vol 3, Jan-Feb.

[15]Naveen, T Venkata Sainath Gupta, V.R. Satpute, A.S Gandhi,(2015) "A Simple and Efficient Approach for Medical Image Security Using Chaos on EZW", IEEE

[16]NirmalRaj,(2015) "SPIHT: A Set Partitioning in Hierarchical Trees Algorithm for Image Compression", Contemporary Engineering Sciences, Vol. 8.

[17]Peng Liu, Zhizhong Ding (2009) "A Blind Image Watermarking Scheme Based on Wavelet tree Quantization", Second IEEE International Symposium on Electronic Commerce and Security, pp. 218-222.

[18]Preeti Gupta, (2012) "Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September,1 ISSN 22295518, pp. 1-4.

[19]Ramana Reddy, Munaga. V.N.K. Prasad, D. Sreenivasa Rao,(2009) "Robust Digital Watermarking of Color Images under Noise Attacks" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May, pp. 334-338.

[20]Ran Tao and Xiang-Yi Meng (2010) "Image Encryption with multi orders of fractional fourier transform" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER.

[21]Ritu Chourasiya, Prof. Ajit Shrivastava, (2012)"A Study of Image Compression Based Transmission Algorithm Using SPIHT for Low Bit Rate Application", Advanced Computing: An International Journal (ACIJ), Vol.3, No.6, November.

[22]Sadreazami,(2016) Student Member, IEEE, M. Omair Ahmad, Fellow, IEEE, and M. N. S. Swamy, Fellow, IEEE "A Robust Multiplicative Watermark Detector for Color Images in Sparse Domain "IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 7, JULY.

[23]Saraf, V. P. Jagtap, and A. K. Mishra,(2014) Text and Image Encryption Decryption Using Advanced Encryption Standard," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, Issue 3, pp. 118-126, May-June.

[24]Seyun Kim (2015). Student Member, IEEE, and Nam Ik Cho, Senior Member, IEEE "Hierarchical Prediction and Context Adaptive Coding for Lossless Color Image Compression "IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 1, JANUARY.

[25]Vinita Gupta, Atul Barve,(2014) "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes, International Journal of Computer Applications (0975-8887)Volume 100-No.14, August.

[26]Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce, (1997) "A Multiresolution Watermark for Digital Images" Proc. IEEE Int. Conf. on Image Processing, Oct., vol. 1, pp. 548-551.