A Hybrid Approach for Image Security by Combining Watermarking with Encryption

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology

in

Information Security

Submitted By

Pushpak Yadav

Roll No. 801333019

Under the supervision of:

Ms. Maggi Bansal

Lecturer

CSE Department

Mr. Sumit Miglani

Lecturer

CSE Department

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

May 2015

ACKNOWLEDGEMENT

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life.

This work would not have been possible without the encouragement and able guidance of my supervisor's **Ms. Maggi Bansal** and **Mr. Sumit Miglani**. I thank my supervisor's for their time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable.

I am equally grateful to **Dr. Deepak Garg**, Associate Professor and Head, Computer Science & Engineering Department, a nice person, an excellent teacher and a well – credited researcher, who always encouraged me to keep going with work and always advised me with his invaluable suggestions.

I will be failing in my duty if I don't express my gratitude to **Dr. S.S. Bhatia,** Senior Professor and Dean of Academic Affairs, Thapar University, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my family whom I dearly miss and without whose blessings none of this would have been possible. To my parents, I own thanks for their wonderful love and encouragement. I would also like to thank my brother, since he insisted that I should do so. I would also like to thank my close friends for their constant support.

Date: July, 2015
Place: Thapar University, Patiala

(Pushpak Yadav)

ACKNOWLEDGEMENT

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life.

This work would not have been possible without the encouragement and able guidance of my supervisor's **Ms. Maggi Bansal** and **Mr. Sumit Miglani**. I thank my supervisor's for their time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable.

I am equally grateful to **Dr. Deepak Garg**, Associate Professor and Head, Computer Science & Engineering Department, a nice person, an excellent teacher and a well – credited researcher, who always encouraged me to keep going with work and always advised me with his invaluable suggestions.

I will be failing in my duty if I don't express my gratitude to **Dr. S.S. Bhatia,** Senior Professor and Dean of Academic Affairs, Thapar University, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my family whom I dearly miss and without whose blessings none of this would have been possible. To my parents, I own thanks for their wonderful love and encouragement. I would also like to thank my brother, since he insisted that I should do so. I would also like to thank my close friends for their constant support.

Date: July, 2015
Place: Thapar University, Patiala

(Pushpak Yadav)

ABSTRACT

In todays networked world, security of digital data is of uttermost importance. Digital data are extensively used throughout the world in almost every field. Banking, social media, hospitals, hotels, theaters are some of the areas where security of digital data is very important. The need for securing the data increases, as they need to travel over the network vulnerable. Thus, before sending digital data over the insecure network,

The sender must take some measures to ensure protection of the sensitive data. For this, the sender may choose various techniques such as watermarking, cryptography or steganography. These techniques ensure different aspects of security. Watermarking ensures data authentication and copyright protection, whereas cryptography and steganography both ensures confidentiality and integrity. For very sensitive data any one of these techniques is not sufficient, thus a hybrid approach is recommended to ensure multi-dimensional security.

In this thesis, a hybrid approach for securing images using watermarking and encryption is presented to improve the overall security of images. This approach ensures the integrity, authenticity, copyright protection, confidentiality of images. Here security of digital data is ensured twice. First using encryption, it is encrypted and then it is hide in cover image using watermarking. Watermarking is also applied in edges of cover image, due to which visual quality of the image is maintained. Using this approach overall security of the image is improved. Experimental results show that quality of image after watermarking is improved. Results were compared on PSNR and MSE metrics.

Table of Contents

S. No. **Topic Name** **Page No.**

List of Figures

Figure No. Figure Name **Page No.**

List of Tables

Table No. **Table Name** **Page No.**

Chapter 1

Introduction

1.1 Digital Image Processing

An image can be defined as a two variable function f (x, y), where y and x are the coordinates of the plane and f is a function which defines the intensity or gray level at some random point (x, y) on plane in the image. For an image to be digital, values of f and x, y must be discrete and finite, and if we can process an image which is digital in nature using digital computer than it is called as digital image processing.

Image processing was first used in newspaper industries, initially at that time images were sent over countries via submarine cables, which takes even more than a week, and also a lot of quality degradation is noticed, so to improve tonal quality and resolution image processing come in picture [1].

The main objective of processing image is either to increase the quality of the image so that more data can be taken from it to process or understood by humans, or we can play with its components to make it comfortable to store or transfer. For different purposes, we apply different techniques, as per the requirement. We can either apply image processing to make it easy for human readers by decreasing noise in it, or enhance its quality such as colour , contrast, brightness etc, or we can make it useful for machines so that they can use the information given in the image for further processing, for example in target detection, face recognition ,fingerprint matching etc.

1.2 Types of Image Processing:

Mostly consider the three types of processing low-level, mid-level, high-level processes.

1.2.1 Low Level Processes:

Low level image processing consists of pre-processing the image for enhancing its features, for example, reducing noise, enhancing contrast, sharpening etc. In low-level processing both input and output of processing are images.

1.2.2 Mid-level Processes:

This type of processing involves operations in which components of image were extracted, for example segmentation (breaking the image into regions or objects) and classifying individual region. In mid-level processing, consider that input is an image, but output may or may not be an image, as it could be a component of image such as edges, contour etc.

1.2.3 High Level Processing:

In high-level processing, the main objective is making sense of extracted region or objects, as in image analysis, and processing. From high level processing data is being extracted from an image which is then further used in different fields like machine vision applications, automated detection, recognition of fingerprint, tracking targets, weather forecasting etc.

1.3 Fundamental Stages in Digital Image Processing:

Fundamental steps used in digital image processing are shown below in figure 6.

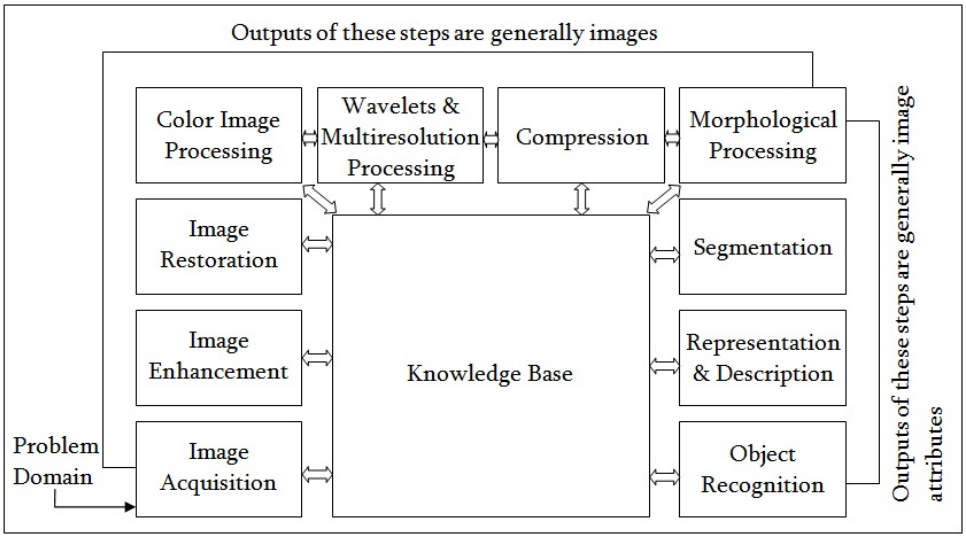


Figure 1.1: Fundamental stages of Digital Image Processing

Image acquisition, image enhancement, Image restoration, morphological processing, Segmentation, object recognition, representation and description, image compression, colour image processing [1].

In today's world, most of the data which travels on the internet is in digital form. In every field such as banking, medical, e-commerce etc digital data is being used very extensively. Therefore, its security is also becoming a major issue of concern, as in

today's network world every data need to go on network for sharing, which is very suitable place for all the hackers or malicious users to attack on it, therefore it needs security very much. Data in digital form become vulnerable to copyright attack, illegal distribution and authentication problems. To overcome such security issues researchers were working in the field of watermarking, steganography and cryptography.

1.4 Watermarking

Watermarking is a technique of hiding information of signals into signals itself to protect it from being copied thus preserving its authentication. It is a special version to steganography as here too we hide a message, but here the message is something related to signal which we hide it. Here the signal is generally either image, video or audio i.e. digital signals, watermarking is applied commonly on digital signals as in today's network world every data need to go on network for sharing, or because of increasing growth of network its security is at much higher risk, it also became the suitable place for all the hackers or malicious users to take it, so it needs security very much therefore we generally provide watermarking on digital data. Watermarking tries to hide information which is somehow related to signal itself and help to know the generator of information to track or to know the users of that data, while in steganography the information may or may not be related to carrier signal, as in steganography we hide data which is not related to the signal, even here we try to take some signal as a carrier which are innocent/nowhere related to that data.

1.4.1 Types of Watermarks:

Majorly there are two types of watermarks, we can embed into image.

1.4.1.1 Pseudo-Random Gaussian Sequence:

A Pseudo random Gaussian sequence watermark contains a sequence of numbers containing 1 and -1 and these sequences of equal number of 1's and -1's are considered as watermark. These watermarks are considered for original data detection based on correlation measure.

1.4.1.2 Binary Image or Gray Scale Image Watermarking:

Unlike Pseudo random Gaussian sequence watermarking, some methods embed digital data or meaningful data like image. These algorithms are considered as a binary image watermark or grayscale image watermarking. They are used for original

data detection. Based on the type of watermark we embed, a suitable decoder must be chosen to detect the existence of watermark.

1.4.2 Watermarking applications:

1.4.2.1 Broadcast Monitoring:

The technique of cross verifying the content that needs to be broadcasted, is actually broadcasted or not on TV or radio. It is used to monitor broadcasting, as suppose a advertising agency want to monitor whether their advertise is being aired for the time they paid or not, so they simply watermark their advertisement video to monitor it.

1.4.2.2 Copyright Protection:

One of its use is to prevent copy infringement, for example a producer will embed different watermarks in all the legal copies of his movies or book, now if it's being illegally copied then it's easy for him to detect that from where its being leaked or from which legal copy its being copied so that he can trace the person.

Copy controlling application of watermarking is very promising as there are watermarking compatible cd dvds in the market, which won't allow to copy the content on cd's as they are not original which help in reducing piracy up to a large extent.

Figure 1.2: Application in Copyright

1.4.2.3 Content Archiving :

Watermarking can also be used to add digital object identifier or serial number in

digital contents like images, videos, audios while archiving them. With the help of this we can also classify and organise digital data. Normally they can be detected by their names, but with this method we can even change the file name without any problem, hence embedding identifier in object itself reduces the chances of tempering[2].

Figure 1.3: Application in Content Archiving

1.4.2.4 Metadata Insertion:

Metadata is the data that describes data, we can label the images with their contents and can be used in search engines to optimize their results. For example, the audio file can also carry the singers name or lyrics along with audio. You can search the news through the image of incident, etc. [2].

1.4.2.5 Temper Detection:

Watermarking can be used to detect any type of temper in digital data by embedding fragile watermarks. It detects the presence of temper and hence we can decide whether to trust the data or not. Temper detection is very use full in court of laws for verifying the truthfulness of digital evidences [2].

1.4.2.6 Digital Fingerprinting:

To detect the owner of the digital data, this technique is used, as fingerprints are unique to the owner of the digital data [2].

Figure 1.4: Application in Digital Fingerprinting

Watermarking can be of two types either visible which were generally applied on images or videos, but they actually spoil their beauty. So we can use invisible watermarking they are hidden from attacker so become more difficult to forge, and also does not spoil the beauty of image or video.

Invisible watermarking can be done mainly in two domains spatial and transformation domain.

1.5 Types of Watermarking:

Based on the domain in which we insert watermarks, we classified watermarking as spatial domain and transform domain based watermarking. To implement spatial domain based watermarking, the simplest way is to insert the watermark in least significant bits (LSB) [3]. These methods are less used these days as here the capacity of data is although god but they are not very much secure and robust against various kinds of attacks for example, they can be easily cracked and found that data is hidden in their LSB because of two reasons, firstly they are a very common form of watermarking so anyone can guess the algorithm, secondly they somehow reduce the quality of the image so, by seeing the image any well experienced person can know it. On the other hand transform domain based techniques are quite new and less known also they are popular today and mostly used because of their high level of security and robustness, they ensure robustness because of they hide data not directly on LSB's but at some finer level of pixels. The most popular transform domain are frequency domain via DFT (discrete Fourier transform) [4], SVD (singular value decomposition) etc. Other variants are DWT (discrete wavelet transform) etc. Generally, these methods were used majorly or their variants for secure and robust watermarking.

1.5.1 DCT Based:

DCT stands for discrete cosine transform, these types of watermarking are robust enough to handle attacks than spatial domain based watermarking. They can survive against attacks on low pass filter, brightness and contrast tempering etc.

But they have some issues related to them due to which they are not widely used everywhere which are as:

They are costlier in terms of computation than other methods.

They are not as much easier to implement as spatial domain based are.

They don't stand strong against geometrical attacks like scaling, rotation cropping etc. [5].

1.5.2 DWT Based:

DWT stands for discrete wavelet transform, in this type of methodology we divide our image matrix into 3 spatial domains i.e. Vertical, diagonal and horizontal.

The magnitude of coefficient is more in lowest band (LL) than any other one (HL, LH, HH). This division into sub bands is more appropriate in showing HVS properties. It is also called as multi resolution display/description of image as an image shows different levels from low to high level of resolution. They perform finer processing specially in terms of visual artifacts as compared to DCT as they broke the image matrix into blocks and then process it [5].

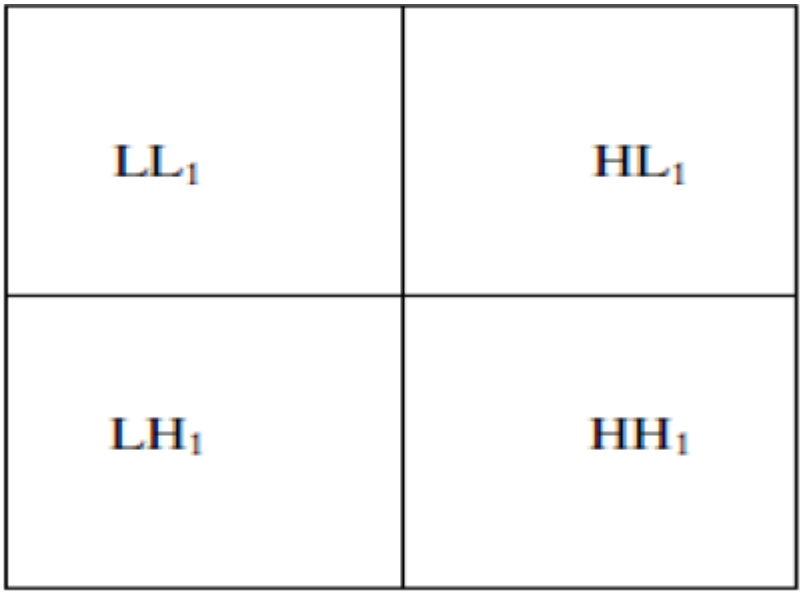


Figure 1.5: Single Level Decomposition Using DWT

1.5.3 DFT Based:

DFT stands for discrete frequency transform, it provides better security against geometric tempering as scaling translation cropping rotation etc. They are resistant to cropping attack as any change in size (cropping) leads to quality degradation of image.

Image scaling can amplify the retrieved pixels and can be detected. Similarly rotation will cyclically shift the signals so can also be detected in exhaustive search. [5]

J.R. Hernandez et. Al. [6] Proposed in his research that if we embed our watermarking image in MSB portion (low frequency) then it will become more robust than the one with embedding in LSB. But at the same time it will more difficult to hide it now.

While on the other hand, if we hide our watermark image in LSB (high frequency) then it will no more resistant to attacks but can be hidden more prominently.

1.5.4 SVD Based:

Singular Value Decomposition (SVD) is a linear algebra based on a numeric analysis, which is extensively used in image processing based applications. It is used to decompose a matrix based on equation (1)

$$A=USV^{T} \qquad (1)$$

These singular values of SVD are very stable, which is an important factor in making this approach very suitable for watermarking, because of this stability SVD is very robust and resistant against various kinds of attacks. SVD is very powerful method for robust watermarking, their SV's are stable, therefore it remains undisturbed from disturbance in the image. It also preserves some of the properties which are not preserved with DCT or DFT. It shows intrinsic algebraic properties of images.

1.6 Properties of Watermarking:

There are 3 major properties of digital watermarking.

1.6.1 Fidelity or Transparency:

Digital watermarking should not disturb the original quality of the image. After embedding there should not be any sign of embedding, no difference should be visible in image after and before embedding, no visible distortion should be introduced otherwise its commercial value is depreciated[2].

1.6.2 Robustness:

A watermark is called as robust if embedded information is detected reliably from watermarked signals, even if some transformations are used to degrade it. Most common degradations are JPEG compression, cropping, rotation, noise, etc. For video signals MPEG compression and temporal modification are also included.

1.6.3 Fragility:

A watermark is said to be fragile if it fails to be detected even after modifications (attacks). These types of watermarks are used for tamper detection (integrity proof). And a semi fragile watermark is those which resist against benign transformation, but fails under higher degree attacks.

1.6.4 Perceptibility:

A watermark is called imperceptible if the cover image (before watermarking) and watermarked image (image after watermarking) are indistinguishable. On the other hand a digital watermark is known as perceptible if its presence is noticeable on marked signal image, best example of perceptible watermarking are visible watermarking.

1.6.5 Capacity:

This property shows the amount of data that can be embedded as watermark in a signal to be successfully detected during extraction. A watermark should content that much information which is enough to detect the uniqueness of the image. Different applications need different size of data or payload [7].

1.7 Cryptography:

Cryptography deals with the security of data through encryption and decryption. Cryptography has existed since 4000 years majorly used by Egyptians.

The rapid growth and modernization leads to the higher exchange rate data over network day by day. In every field data is being stored or shared digitally over network in many forms, therefore it becomes more vulnerable to different types of attacks like duplicating data and modification, etc. by hackers hence before transmitting data it is important to make sure that it is protected, for example, information like credit card details, passwords, personal data, banking information etc. Need extra care, to achieve this we use encryption. Many encryption techniques were existing which were used to protect against information theft. In the recent era of

wireless communication, encryption plays a vital role in securing data in online transactions. Encryption is a very common and used technique in securing digital data. Its evolution is moving towards endless possibilities. Every day some new work in this field is introduced. Image encryption, video encryption and chaos based method of encryption has applications in many fields like internet communication, medical imaging, tele-medicine and military operations or communication etc.

1.7.1 Objectives of Cryptography:

The main objectives fulfilled by cryptography are discussed below:

1.7.1.1. Confidentiality:

Only the intended audience of data should be able to understand it. No one else should understand the data.

1.7.1.2. Data Integrity:

It is maintaining the accuracy, originality, consistency of data throughout its life time, the intended recipient should be able to cross check, whether the message was changed/modified accidentally or deliberately during its transmission. No one should be able to replace the original message with the false one or modify it or part of it.

1.7.1.3. Authentication:

It is an act of confirming the origin of a message or data. No one should send a message signing it as someone else. Before initializing connection, both the parties must check the authentication of each other by identifying each other.

1.7.1.4. Non-Repudiation:

A sender should not be able to deny from the fact that he or she doesn't send a particular message after sending one. Similarly recipient must not be refused from accepting the message or data after requesting it.

1.8. Encryption and Decryption:

Encryption is a process of encoding a message or data into cipher text, which is a form unreadable without a key to decode it, which will prevent it from reading by unintended user. Decryption is a reverse process of encryption in which we get the message or data again into readable form while received, i.e. Plain text.

Key in cryptography is a sequence of bits long enough is used for encryption and decryption. As shown in the fig. The algorithm takes a key and message as input and

produce a same length coded message called as cipher text. Likewise for the decryption reverse procedure is applied, encrypted message and key is taken as input and plain text is reproduced from it.

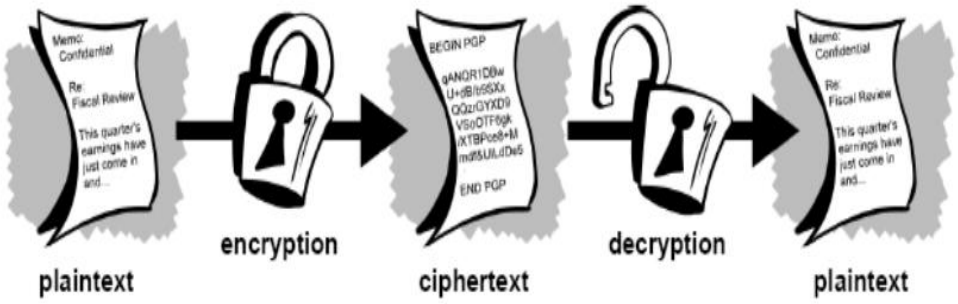


Figure 1.6: Cryptography [8]

1.8.1. Types of cryptography:

There are various ways of classifying cryptography algorithms. Main classification is based on the number of keys indulge to perform encryption and decryption.

1.8.1.1. Secret Key Cryptography (Private Key Cryptography):

In Private Key cryptography, only one key is used for both encrypting and decrypting the message. Here sender will apply this common key to the message before sending it and convert the plain text into cipher text. On receiving the cipher text, the receiver will apply the same private key again on that cipher text to convert it into plain text again. In this way the same key is used for both the purposes'. This type of encryption is also called as symmetric key cryptography[9].

In this type of cryptography, both sender and receiver must have the possession of the key, therefore the main challenge is to distribute the key securely among both sender and receiver, so that it will remain unknown to the world.

1.8.1.2. Public Key Cryptography*:*

This type of cryptography is also known as asymmetric key cryptography. This is the most common since the beginning. In public key cryptography, two parties were involved in communication over an insecure channel without sharing key. Here both the keys were mathematically related to each other, in other words, both were compliments of each other. One is used to encrypt the message while the complement

of that key is used to decrypt the message and convert it from cipher text to plain text. Here both keys play an important role and indeed in the process.

Chapter 2

Literature Review

In this chapter, we will discuss the work done by many researchers in the field of security of images. Security of digital data is achieved by applying watermarking, cryptography. New techniques were proposed in this area.

Chang-Tsun Li et.al. [10] proposed a method of using the feature map of the image as a watermark, then partition it into a block, then send it to the other end where it will be again compared with the original watermark calculated, which ensure us about the integrity of data. Previously in watermarking the sender use some numbers or logical patterns as a watermark, which is also difficult for receiver to handle and proper care of it is also needed as every data has its own watermark so they have to create a database which will store them[26], also there are some chances that this watermark may get copied during transfer from sender to receiver, and there is also some overhead of sending this watermark to receiver separately before data is being send as he need it to compare with the data coming from sender. As here we have to access to the database so many times and also every time watermark has to be taken separately from channel, which will increase unnecessary overhead and excessive channel utilization. To see whether there is some alteration is done in channel, knowledge about the image is necessary i.e. We need to access database again. Therefore, in [10] Chang-Tsun Li et.al. Advised about using image features itself as a watermark so that no extra information is needed to be preserved thereby decreases channel utilization and overhead. This will help both the communication parties as they are now free from maintaining database as it will use feature map which is already present inside the image and its not new and therefore not needed to be send and maintained separately. There is no need of watermark to be sent so now there is less chances of it to behold in between by an intruder. Also now information about the image is needed by the receiver as previously needed to detect any tampering with it. And the security

is also enhanced as channel utilization is decreased and less data about the image or watermark is now travelling through the channel.

Biometric data are most often used for identification and authorization these days, which involve more security threats as they are unique and provide excellent in authentication, but they are not hidden also, as they can be easily taken or copied by anyone. Therefore, before using them as an authentication tool against traditional ones we need to secure them first, their security has become a more challenging task.

Anil K. Jain et al. [11] proposed a watermarking scheme in which he uses amplitude based modulation. Where he tries to conceal biometric data in various images, which will increase the security of both, the data as well as image, this method will guarantee high accuracy. Biometric based identification technique uses biometric features as a key become more popular than conventional ones example id card, password, etc. The main reason behind their popularity is that they can easily distinguish the person from others. Among all the techniques available in the field of biometrics as face geometry, fingerprint retina, iris etc, finger print is most widely used one, as they are easy to practically implement and also cheaper in execution. As they are more secure, reliable but they have some bottleneck in implementation as they are more crucial to secure, and need extra efforts to do so, for example, if we came to know that our biometric image is being stolen, then we have no option like replacing them, in that case, what we can do is either replace the type of data (like use retina if previous fingerprint is used) which is not practically feasible as it need a whole system to be changed. Schneier [12] has also quoted that biometrics based Verification system works properly only if the verifier system can guarantee that the biometric data came from the legitimate person at the time of enrollment. Ratha et al. [13] observed eight types of attacks. As biometric provide inquests but fails to provide reliability so we have to focus more on securing them before using them as an authentication tool, for that purpose, either use encryption, watermarking or steganography, encryption is good to be applied, but we are not sure about the security if they were decrypted in between, watermarking provide copyright protection as we can use our personal signature as watermark to copyright it, steganography will simply try to conceal the data, so we can say that steganography sounds more reliable for securing biometric data, or we can apply encryption on it before hiding it. Or we can use different permutations of all these methods. Anil. K.

Jain et.al. [11] Describe the method of securing one type of data while using another type of biometric data which will increase the overall security. So it can be said that encryption, steganography, and watermarking will fulfill our requirement of security of biometric data.

Jaspal Kaur Saini et. al.[14] has proposed a hybrid method for securing data, where they first applied encryption on the image, first they encrypt the image using advanced AES algorithm then which then being concealed under the cover image in this way they applied both encryption as well as steganography to increase the security level. Cryptography allows the data to be converted into a form which is not understandable by normal users[28], i.e. It needs to be again regenerate into original form by applying key. Here he first encrypt the message and place it on the channel, on the other hand, the recipient will take it and regenerate the actual message by decipher it. Here they first applied encryption on image by dividing it into small blocks and applied modified AES algorithm, which convert the original image in encrypted one which can't be decoded without decryption keys. Now during sending it may be captured by an intruder and he may somehow decode it, then it's impossible to save the message. So they applied steganography on data to hide the existence of image so no one can detect it and it become more complicated for intruder to read or fetch the original image. They use a cover image which is used to hide the message encrypted image in it. For steganography they choose the least significant bits (lsb) of pixels to hide the image so that more capacity can be offered or more than one image can also be saved in the same cover image. Here new version of AES algorithm is used which help in providing better security, they first encrypted it using this algorithm and then applied steganography, which provide better results than using them individually.

Swanirbhar Majumder et.al. [15] has proposed one another method to secure digital data where they raise the issue regarding security of digital data as they were not very secure and being copied so easily, there is an enormous way of making pirated copies of these data, so he suggested the method of applying watermarks to safeguard them, here he used biometric data as a watermark as they are more secure and appropriate to use instead of other traditional watermark schemes, iris image is used in biometric data as they were more secure than fingerprints and face, and also provide equivalent security after retina. They take the images of iris and then extract the discrete cosine

values of these templates or images which was then converted to binary streams. Now calculate the singular value of image's coefficients through wavelet transform and embed this data into these singular values. This algorithm is tested on various attack vectors. Here he interrelate the biometric with the watermarking scheme as to enhance the overall security of the system. Although he tried to make the algorithm very simple, still by using both SVD and DWT will provide more robustness and reliability to the algorithm[29,30].

Wang Na et.al. [16] has proposed a method, where they used steganography based security mechanism to protect biometric data, he first encrypt the data by applying logistic maps. Using logistic maps he generated two pseudorandom sequences which were used to encrypt the data before hiding. JPEG and JND (just noticeable difference) are used for applying steganography, as using them an efficient algorithm can be designed which is more robust and transparent. Peak signal to noise ratio (PSNR) is used here to measure the invisibility of watermark, and normalized correlation is employed to detect the similarity of original code and extracted one, comparing both the codes we can conclude whether tempering is done or not.

The PSNR ratio of images should be high in order to reduce the chances of being caught by an intruder.

FAR (False Accept Rate) and FRR(False Refuse Rate) for representing the recognition performance, is utilized to measure the effects after stegonagraphy.

An another method suggested by Yang Ren-er et.al. [17] where he suggested to use steganography along with DES algorithm. He first uses the DES algorithm to encrypt the image so that it will not be detected even after being caught, and then apply steganography to hide it. For steganography they used LSB bit manipulation, i.e. They will insert the image data at lbs of each byte. Now in this manner it will be easier to increase the robustness as even if someone is able to unhide the image still he won't be able to decipher it as its in encoded form, experiments show that cumulatively applying DES encryption and steganography, will increase the security level then using steganography alone. Cumulatively applying these both methods will enhance the security as DES will change the basic characteristics and LSB based steganography help to conceal this hidden data.

According to John N. Ellinas, and Panagiotis Kenterlis[18], the quality of your algorithm of watermarking depends on the quality of visual information after watermarking. To attain this they advised an algorithm in which watermarking employs wavelet transform upto forth level of decomposition and then involve Human Visual System characteristics. To achieve this DWT up to fourth level is applied and then find the edges of the cover image and use those edge pixels to hide the watermark image. According to proposed algorithm, embedding watermark in edges will merely affect the quality of the image as distortions are not much more noticeable here.

To achieve watermarking on binary images V.J Subashini [19] et.al coined an algorithm. Now a days biometric based systems are intensively used for security of data in every field, for example in commercial, forensics and governments etc. From all the biometric treats of human, finger prints are most commonly used as they are very common, because of this a huge number of fingerprint images are needed to be stored securely, as applications where biometric based security is increasing so do database rapidly, the size of these databases may reduce if the size of the image reduced, to achieve this, we can use binary images instead of grayscale or colored images. The main purpose of watermarking is to provide security with lesser visual changes. In this proposed algorithm, watermarking is embedded based on the generated run length of pixels patterns in binary biometric images, this approach make the hiding efficient and invisible. According to algorithm the carrier image is transformed in one dimensional array of pixels, then compute their run lengths. This run length vector is then split into three overlapping vectors among these, the middle one is used for embedding of watermark.

Khalil zebbiche et.al [20] proposed an algorithm for robust watermarking. Robust watermarking technique is among the most important technique in securing visual data, authorized access and ensuring copyright protection. But the two main characteristics in robust watermarking were conflicting each other which are imperceptibility and robustness. So the algorithm must be coined which make a proper balance among them, i.e in enhancing one characteristic, one must provide acceptable performance in another. Therefore, in this proposed algorithm, robust watermarking which will also provide acceptable performance in imperceptibility as they use the HVS (human visual system) behavior. This algorithm used an efficient

just perceptual weighting (JPW) model which exploits three human visual system characteristics, which are: texture masking, spatial frequency sensitivity and local brightness masking. Using these characteristics each wavelet coefficient's weight is calculated. This weight is used as a threshold for controlling the amplitudes of watermark inserted. The main motivation behind this approach is the use of fingerprint images, which is different in perceptual from normal image and the use of the JPW model for such image will further enhance the robustness.

Vineet Mehan et al.[21] proposed a unique method of watermarking combined with fingerprint image for colored images applied to double DCT domain. This approach helps in copyright protection and identify the traitor in digital media. Mid frequency coefficients if altered are analyzed by forward DCT transform applied. Second DCT is applied for the précised determination of blocks where data is embedded. By applying DCT twice enhance the embedding capacity in the image as in a particular block, we chose more than one coefficient. By some simulations it can be predicted that the watermarking is immune to compression attack, median filter and noise. Quality of image after watermarking is also not degraded much.

A. V. Subramanyam et al. [22] also proposed a scheme of robust watermarking compressed image which is encrypted first. Where JPEG2000 is used for compressing the image for storing in the database. Digital asset management system stores data by compressing the encrypted data[32-35]. To secure these data more, watermarking is sometimes necessary. As these data are compressed and encrypted, it is very difficult to watermark them, as here by compressing the media it will pack the raw bits in a lower number of bits and then encrypting them will randomize those packed bits. Applying watermarking of such media is crucial as a little degradation on randomized bits will drastically degrade the image quality. Thus, it is utter most important to choose the encryption technique very wisely, as it should be secure enough and also allow watermarking to be reasonable. The author chose a stream cipher technique for encryption. Author chooses to embed watermark in compressed encryption domain, therefore the extraction of watermark is applied in decryption domain. The proposed method will enhance the embedding capacity, robustness, security and perceptual quality.

The method suggested by Roli Bansal et al. [23] In which NN-PSO based approach to secure a person's identity is used. Where a person’s fingerprint is secured by watermarking them their own facial image and demographic information. The input image of finger print is first divided into blocks which then feed to the feed forward neural network to calculate the number of number of bytes to embed in each block of the image. PSO is applied on image to find optimum wavelet coefficient, this procedure is applied in such a way that the quality of fingerprint image must be preserved. This procedure is applied to gray scale image of fingerprint of human which provide security and authentication. As we know DWT is much closer to the human visual system than DCT, As it split the image in blocks or bands and we can apply watermarks to them individually.

Chapter 3

Problem Statement

In this chapter, we will analyze the gap and weakness in existing techniques, Problem statement on which we were writing this thesis, and objective which we want to achieve are discussed below.

3.1 Gap Analysis

In the literature review chapter we have discussed some methods of watermarking, which are the latest in the research domain of watermarking. This review shows some gaps exist which are as:

1) Either plain text data or simple image is used generally as watermark. The problem with them is, intruders can easily guess the watermark and re- generate watermarked content. Thus, advance method is needed so that it can't be re-generated easily without legitimate user.

2) The intruder may breach the watermarking algorithm and get the possession of watermark data and spoof the data.Therefore a approach is needed where intruder even after breaching the watermarking algorithm can't get the watermark data.

3) Watermarking alone only fulfill some aspect of security like authentication, copyright protection, piracy control, etc. which is not sufficient for overall security of sensitive data. Nowadays just ensuring these aspects doesn't secure sensitive data over insecure network. Therefore, an approach must cover all the aspects of security too, and provide overall security of data.

3.2 Problem Statement

Various methods for image watermarking were presented in previous years and improve the security of image while sending them over the network or for protecting their copyright protection. Some were proposed their method for providing authentication to images so that they can be used for authentication purposes, some were dealing with integrity of the image through watermarking. Some algorithms were working for protecting copyright protection etc. But the problem with them is that they were not dealing with these issues simultaneously. If some method provides

authentication, then it may not provide integrity or copyright protection or confidentiality. If some provide integrity, then may fail in dealing with others. In improving one security aspect other may be ignored or reduced. As in growing digital networking world, to secure our digital data, we have to use 3 dimensional approach which will not just work in one direction but also in others.

In order to withstand in a digital networked world with secured digital data an algorithm is needed which will help in securing our digital data fully, as only watermarking is not providing overall security to images so it must be enhanced somehow so that overall security is achieved like authentication, integrity, confidentiality, copyright protection etc.

3.3 Objectives

1) To study the existing techniques in the field of watermarking.
2) To propose a hybrid watermarking method which enhance security.
3) To implement the proposed method.
4) To test and validate the results of our approach through different comparison matrices.

Chapter 4

Implementation Details

In this chapter, the proposed method of watermarking for security of images is discussed. A hybrid approach is used for securing digital data. For the implementation purpose, we have used MATLAB R2013a. which is also compatible with the previous versions, but it was the latest version and have some features and tools which were not present in previous versions. MATLAB provides an easy environment for implementation, and is also an efficient way for implementation.

As we have discussed most of the watermarking algorithms were not covered all the aspects of security. In most of the watermarking algorithms, either text data or simple image is used as a watermark, which intruder may capture and regenerate. Therefore, in proposed method, we used a biometric image so that it can't be generated by another person except the originator. In proposed method we implemented invisible watermarking on the image pre processed with DES encryption which further provide security to watermark as even if intruder get the watermark, its confidentiality is preserved. Invisible watermarking can also be implemented either in spatial domain or transform domain, we used transform domain to apply watermarking in images, so that the copyright of the image holder can be protected, therefore, to ensure this we used the fingerprint image as our watermark which we will be embedding in the cover image. To accomplish this we used DWT, edge detection techniques, DES encryption.

4.1 Overview of MATLAB

MATLAB is a tool used to bridge the gap between theoretical knowledge and practical implementation of theoretical concepts. It is a high level language for the implementation of numerical computational work, visualization, using this we can create models, implement algorithms, analyze data. It provides various toolboxes, in built functions for different kind of computational works, by which we can reach our results[24].

MATLAB can be used in various fields as, in control systems, image processing, video processing, channel and signal processing, communication, test and measurement, biological computation etc.

It provides a different specialized tool box for the processing of images, which include various functions, and methods to be used in image processing, which will make processing very easy and less complex up to an extent.

MATLAB stands for matrix laboratory, developed by linear system package and Eigen system package projects [31]. It is a computational tool preferred widely in research works basically for development and analysis. It has a image processing toolbox, which has a collection of various functions used in processing or implementing any image processing based algorithm [24].

4.2 Various Techniques used in proposed method

4.2.1 DES Encryption

DES is a block cipher approach which applies encryption on a block or stream of data not on a bit, it is a iterative block cipher which is known as Feistel approach, which is a symmetric structure used for constructing block ciphers. It is a symmetric key encryption algorithm. It uses the same key for both encrypting as well as decrypting a message, therefore both sender and receiver knows and uses the same key. For encrypting the data it will group the data in 64 bit chunks which is then applied by 64-bit key to produce 64 bits of cipher text. Deciphering is completely reverse of the ciphering process, all the steps are applied in reverse order to decrypt the message again from cipher text [25]. In this approach encryption on black and white finger print images is applied, which is further used as a watermark to increase its security. As in fingerprint image no colour information is present therefore even on converting it into black and white no information is lost. Then encrypt the image, chunk by chunk of 64 bits each. After which merge the chunks and convert them into image matrix form again.

For decrypting the image apply DES on encrypted chunks, and merge them all to show the original image.

4.2.2 DWT

In this type of methodology we divide our image matrix into 3 spatial domains i.e. Vertical, diagonal and horizontal.

The magnitude of coefficient is more in lowest band than any other one (HL, LH, HH). This division into sub bands is more appropriate in showing HVS properties. It is also called as multi resolution display/description of image as an image shows different levels from low to high level of resolution.

4.2.3 Edge Detector

An edge of an image is a portion across which image brightness changes abruptly.

Edge detection is an important image processing task, which is used in pattern recognition, scene analysis and segmentation of images. It is a high pass filter which is applied to point out the edge points of image [1].

4.3 Architecture of proposed method

The proposed method is comprised of 5 steps. The methodology we are using in our implementation is shown in brief in figure 12

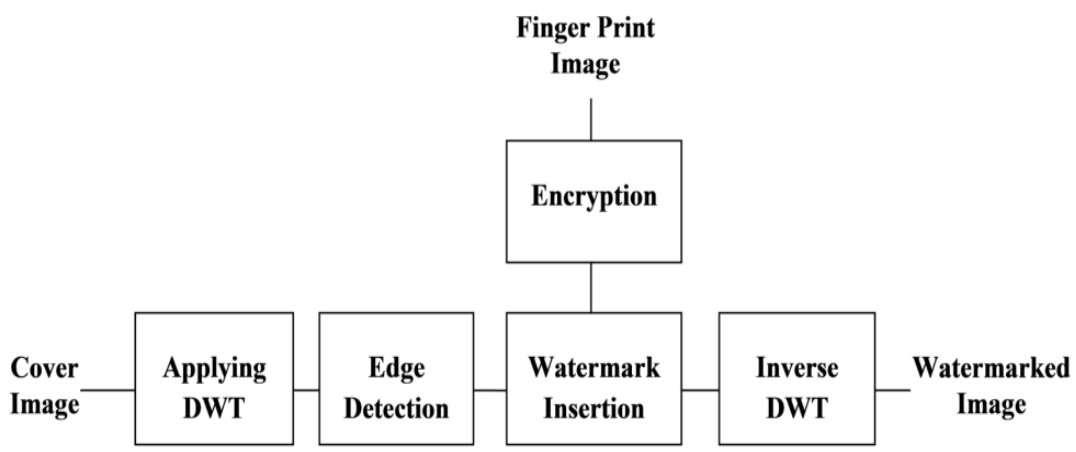


Figure 4.1: Architecture of the Proposed Method

4.3.1 Embedding Algorithm

For the embedding of watermark which is a fingerprint image into a cover image, we use the following algorithm

Step 1: Read the cover image OI

Step 2: Convert the image in grayscale G_OI

Step 3: Repeat step 4 four times

Step 4: Decompose the image using DWT

Step 5: Calculate edges of decomposed OI image

Step 6:Read watermark image FI

Step 7: Convert the watermark image into binary image BF

Step 8: Convert the image in blocks of 64 size each

Step 9: For each block apply DES encryption algorithm

Step 10: Convert the image in singular matrix of size 1*10000 i.e F

Step 11: Insert encrypted pixels in edges of cover image to form WI

Step 12: Repeat step 4 four times

Using leena.png as OI and finger.jpg as FI we shows the working of proposed algorithm below:

- Take Leena.png and convert it into grayscale

Figure 4.2: Conversion of Colored Image to Grayscale Image

- Apply DWT on cover image up to 4 levels of decomposition using HAAR wavelet.
- **STEP 3**: Take fingerprint image called finger.png and convert it to grayscale.

(a) Colored Image **(b) Black and White Image**

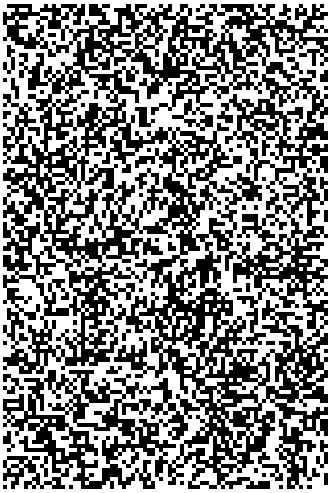
Figure 4.3: Conversion of Colored Image into Binary Image

- Encrypt the finger.png using the DES encryption algorithm.

(a) Fingerprint Image **(b) Encrypted Fingerprint Image**

Fig. 4.4: Encryption of Fingerprint Image

- Convert the finger.png into a single dimension array.



(a). Encrypted Finger Image of Size 100*100

(b) Encrypted Finger Image of Size 1*10000

Figure.4.5: Reshaped Finger Images

- Calculate the edge pixels in the cover image (Leena.png).

(a) (b)

Figure.4.6: Significant (edge) Pixels of Image

- Insert the watermark image (finger.png) in place of those edge pixels.

The fingerprint image is decomposed into a singular array of pixels and embedded at the significant pixels of cover image's sub bands, using equation (2)

$$WI_{x,y=}OI_{x,y} + \alpha.abs(OI_{x,y}).F_x \quad (2)$$

Where $WI_{x,y}$ =watermarked image pixel

$OI_{x,y}$=Original image pixel

$abs(OI_{x,y})$ = absolute of original image pixel

$F_{x,y}$= fingerprint images pixel

α = scaling factor

- Apply IDWT to regain the watermarked image.

Figure.4.7: Watermarked Image

4.3.2 Extraction Algorithm

Algorithms to implement watermark extraction from the watermarked image is as follows :

Step 1: Read the watermarked image WI

Step 2: Repeat step 3 four times

Step 3: Decompose image using DWT

Step 4: Remove encrypted pixels from edges of watermarked image WI

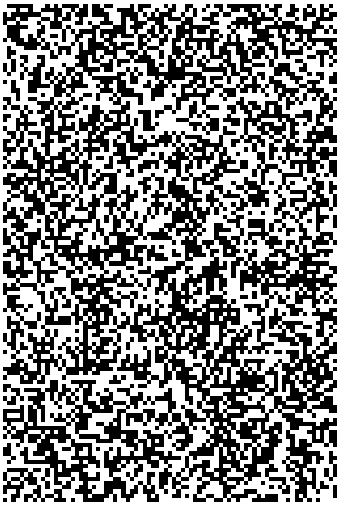
Step 5: Create 2D matrix of size 100*100 SF

Step 6: For each block of 64 bites of SF, apply DES algorithm

- Perform DWT on watermarked image upto fourth level of decomposition.
- Remove pixels of the original sub band from watermarked image.
- Convert singular matrix of pixels of fingerprint image to 2D.

Figure 4.8 shows conversion of fingerprint image from singular matrix to 2 dimensional matrix of size 100*100.

(a). Finger Image of Size 1*10000



(b). Finger Image of Size 100*100

Figure.4.8: Extracted Fingerprint Image

- Decrypt the singular matrix again to gain original pixels.

(a) Encrypted Fingerprint Image **(b) Fingerprint Image**

Figure 4.9: Extraction of Fingerprint Image

Chapter 5

Experiments and Results

The result of the experiment shows watermarked images, which were obtained by applying our proposed method of hybrid watermarking on different images. In this chapter, experimental results of method on four different images were shown, which shows the complete step by step implementation on them, and final result obtained from this method. Each step is shown from conversion of the image to encrypting it to embedding of watermark. Also, we have compared the obtained results from the result obtained by applying the base paper technique. We have compared the results with a base technique based on the comparison metrics like PSNR, MSE in table 1.

5.1 Result of pushpak.jpg image

Pushpak.jpg is taken and converted into gray scale. Both image and its gray scale image are shown in figure.5.1

(a) (b)

Figure 5.1: Conversion of Colored Image into Grayscale image

Take fingerprint image called finger.png and convert it to grayscale. Figure.5.2 shows the output of this step.

(a) colored image (b) gray scale image

Figure 5.2: Conversion of Colored Image to Grayscale

Figure 5.3 shows encrypted finger print image of black and white image.

(a) Fingerprint Image **(b) Encrypted Fingerprint Image**

Figure 5.3: Encryption of Fingerprint Image

Figure. 5.4: Shows the Results of Resize Fingerprint Image.

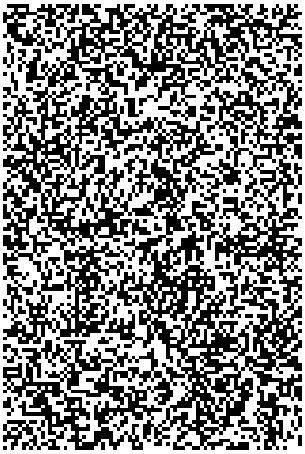


Figure 5.4: Resized Fingerprint Image 100*100

Now convert this fingerprint image into singular matrix, shown in figure 5.5

Figure 5.5: Fingerprint Image of Size 1*10000

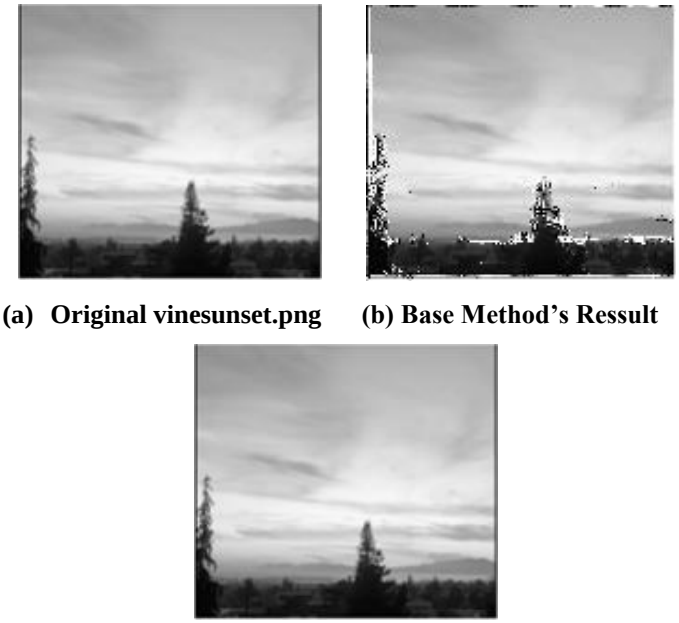
Now this fingerprint image is embedded in edges of the cover image. Shown in figure 5.6

Figure 5.6: Watermarked Image

5.2 Results of Different Images

The results of different images used for experiment are shown below. We applied all the steps on these images of our proposed method. Final watermarked image after applying our proposed method are compared with the method proposed by John N. Ellinas, and Panagiotis Kenterlis[18] which is our base method.

- **Experimental result of vinesunset.png is shown in figure 5.7.**



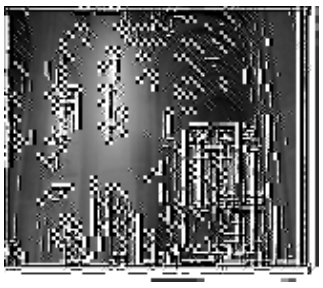
(a) Original vinesunset.png **(b) Base Method's Ressult**

(c) **Propose Method's Result**

Figure 5.7: Experimental Result of vinesunset.png

- **Experimental result of nave.png image is shown in figure 5.8:-**

(a) Original nave.png



(b) Base Method's Ressult

(c) Propose Method's Result

Figure 5.8: Experimental Result of nave.png

- **Experimental result of auto.png is shown in figure 5.9:-**

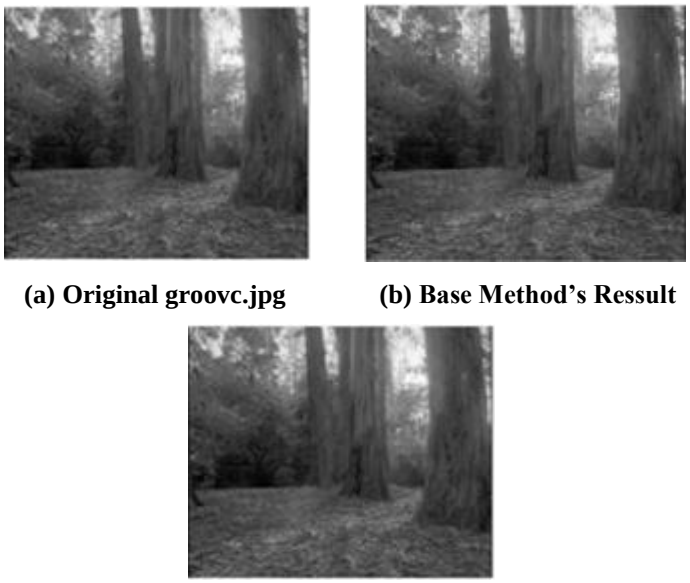
(a) Original auto.jpg

(b) Base Method's Ressult

(c) Propose Method's Result

Figure.5.9. Experimental results on auto.jpg

- **Experimental result of groovc.jpg shown in figure 5.10**



(a) Original groovc.jpg **(b) Base Method's Ressult**

(c) Propose Method's Result

Figure.5.10 Experimental results on groovc.jpg

From the experimental results shown above produced by our propose technique, it is clear that the visual quality of images was not degraded even after embedding watermark in the edges of the cover image. The visual qualities of image which can be detected by human eye were not affected. By viewing the images, we can't predict that the image is tempered or any kind of information is embedded in it. In table 1 we have shown the performance of the proposed technique by comparing it with base technique suggested in [18]. In table 1 comparison is done based on PSNR and MSE metrics on 6 images.

S. No.	Image Name	Matrices	Base paper watermarking	Proposed watermarking
1	**leena.jpg**	PSNR	78.9292	80.1593
		MSE	1.2796e-08	9.6398e-09
2	**pushpak.jpg**	PSNR	74.5022	75.7745
		MSE	3.554e-08	2.649e-08
3	**vinesunset.png**	PSNR	11.0234	78.5823
		MSE	0.0790	1.411e-08
4	**nave.png**	PSNR	11.127	28.5823
		MSE	0.041	1.11e-05
5	**auto.jpg**	PSNR	13.278	14.419
		MSE	3.579e-06	2.349e-06
6	**groovc.jpg**	PSNR	11.2315	14.1716
		MSE	0.097	1.23e-03

Table 1. Experimental Results on Different Images

Chapter 6

Conclusion and Future Work

6.1 Conclusion:

A hybrid approach for watermarking preprocessed with encryption for dual security of digital data is presented. Where DWT is used for decomposing the image in sub bands, which provides a fine discrete band of frequencies which hold the properties of the image. A watermark is embedded in edge pixels of detailed sub bands of the decomposed image. Before embedding, a watermark is preprocessed and encrypted using the DES algorithm. Encrypting the watermark before embedding and using edges for embedding make this approach different and unique. This will make it difficult to detect the watermark. Experimental results show that this approach produces better results than the approach suggested by aliens, John N. et.al. [18]. This approach is easy to implement as well as effective in providing robust non visible watermarked image. The following objectives are achieved by this approach:

- Dual security of data is achieved through encryption and watermarking.
- The visual quality of the image is maintained.
- It provides the robustness against copy infringement, authentication, confidentiality, etc.

6.2 Future Scope:

There are multiple approaches for secure watermarking. Many of them were using a single approach like encryption, watermarking and steganography. In this approach, encryption is used before watermarking, to secure watermark. But in recent times different combinations of these methods are used. In future,watermarked image can be encrypted to provide confidentiality of the cover image, or research can be done for further improving the security of digital data, travelling through a network.

References

[1] Gonzalez, Rafael C. *Digital image processing*. Pearson Education India, 2009.

[2] Gupta, Vinita, and A. Barve. "A review on image watermarking and its techniques." *International Journal of Advanced Research in Computer Science and Software Engineering* 4.1 (2014): 92-97.

[3] Podilchuk, Christine, and Edward J. Delp. "Digital watermarking: algorithms and applications." *Signal Processing Magazine, IEEE* 18.4 (2001): 33-46.

[4] C.Hsieh, P. Tsou, "Blind Cepstrum Domain Audio Watermarking Based on Time Energy Features", 4th International Conference on Digital Signal Processing, pp.,705-708, 2004

[5] Singh, Y. Shantikumar, B. Pushpa Devi, and Kh Manglem Singh. "A Review of Different Techniques on Digital Image Watermarking Scheme." *IJER Volume* 2: 193-199.

[6] Hernandez, Juan R., Martin Amado, and Fernando Perez-Gonzalez. "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure." *Image Processing, IEEE Transactions on* 9.1 (2000): 55-68.I.J.Cox, M.L.Miller, J.A.Bloom, "Digital Watermarking", Morgan Kaufmann Publisher, San Francisco, CA, USA 2002.

[7] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126. A. M. Elshamy, A. N. Z. Rashed, A. E. A. Mohamed et al., "Optical image encryption based on chaotic baker map and double random phase encoding," Journal of LightwaveTechnology, vol., no., pp., 31, 15, 2533–2539, 2013.

[8] Li, Chang-Tsun, Der-Chyuan Lou, and Tsung-Hsu Chen. "Image authentication and integrity verification via content-based watermarks and a public key cryptosystem." *Image Processing, 2000. Proceedings. 2000 International Conference on*. Vol. 3. IEEE, 2000.

[9] Jain, Anil K., and Umut Uludag. "Hiding biometric data." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 25.11 (2003): 1494-1498.

[10] Schneier, Bruce. "Biometrics: uses and abuses." *Communications of the ACM* 42.8 (1999): 58.

[11] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "An analysis of minutiae matching strength." *Audio-and Video-Based Biometric Person Authentication*. Springer Berlin Heidelberg, 2001.

[12] Saini, Jaspal Kaur, and Harsh K. Verma. "A hybrid approach for image security by combining encryption and steganography." *Image Information Processing (ICIIP), 2013 IEEE Second International Conference on*. IEEE, 2013.

[13] Majumder, Subhashis, Kharibam Jilenkumari Devi, and Subir Kumar Sarkar. "Singular value decomposition and wavelet-based iris biometric watermarking." *Biometrics, IET* 2.1 (2013): 21-27.

[14] Na, Wang, et al. "Enhancing iris-feature security with steganography." *Industrial Electronics and Applications (ICIEA), 2010 the 5th IEEE Conference on*. IEEE, 2010.

[15] Ren-Er, Yang, et al. "Image Steganography Combined with DES Encryption Pre-processing." *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*. IEEE, 2014.

[16] Ellinas, John N., and Panagiotis Kenterlis. "A wavelet-based watermarking method exploiting the contrast sensitivity function." *International Journal of Signal Processing* 3.4 (2006): 266-272.

[17] Subashini, V. J., S. Poornachandra, and M. Ramakrishnan. "A fragile watermarking technique for fingerprint protection." *Intelligent Computational Systems (RAICS), 2013 IEEE Recent Advances in*. IEEE, 2013.

[18] Zebbiche, Khalil, and Fouad Khelifi. "Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking." *IET Image Processing* 8.1 (2014): 23-32.

[19] Mehan, Vineet, Renu Dhir, and Yadwinder Singh Brar. "Joint watermarking and fingerprinting approach for colored digital images in double DCT domain." *Signal Processing, Computing and Control (ISPCC), 2013 IEEE International Conference on*. IEEE, 2013.

[20] Subramanyam, A. V., Sabu Emmanuel, and Mohan S. Kankanhalli. "Robust watermarking of compressed and encrypted JPEG2000 images." *Multimedia, IEEE Transactions on* 14.3 (2012): 703-716.

[21] Bansal, Rajeev, Priti Sehgal, and Punam Bedi. "Intelligent wavelet domain watermarking of fingerprint images." *Hybrid Intelligent Systems (HIS), 2012 12th International Conference on*. IEEE, 2012.

[22] Tian, Qiyuan, Jiang Duan, and Guoping Qiu. "Gpu-accelerated local tone-mapping for high dynamic range images." *Image Processing (ICIP), 2012 19th IEEE International Conference on*. IEEE, 2012.

[23] Wolfgang, Raymond B., Christine Podilchuk, and Edward J. Delp. "Perceptual watermarks for digital images and video." *Proceedings of the IEEE* 87.7 (1999): 1108-1126.

[24] Wong, Ping Wah. "A watermark for image integrity and ownership verification." *IS AND TS PICS CONFERENCE*. SOCIETY FOR IMAGING SCIENCE & TECHNOLOGY, 1998.

[25] Li, Yongzhong, et al. "An Adaptive Blind Watermarking Algorithm Based on DCT and Modified Watson's Visual Model." *Electronic Commerce and Security, 2008 International Symposium on*. IEEE, 2008.

[26] Stallings, William. "CryptographyandNetworkSecurity: PrinciplesandPractice." (2011).

[27] Mallat, Stephane G. "A theory for multiresolution signal decomposition: the wavelet representation." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 11.7 (1989): 674-693.

[28] Zhu, Xinzhong, Jianmin Zhao, and Huiying Xu. "A digital watermarking algorithm and implementation based on improved SVD." *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*. Vol. 3. IEEE, 2006.

[29] Jie, Sun Yaoyao Liu. "Realization of Similarity Based on Embedded MATLAB Function Blocks [J]." *Computer & Digital Engineering* 2 (2010): 008.

[30] Hwang, Seong Oun, et al. "Modeling and implementation of digital rights." *Journal of Systems and Software* 73.3 (2004): 533-549.

[31] Sachan, Amit, et al. "Privacy preserving multiparty multilevel DRM architecture." *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*. IEEE, 2009.

[32] Thomas, Tony, et al. "Joint watermarking scheme for multiparty multilevel DRM architecture." *Information Forensics and Security, IEEE Transactions on* 4.4 (2009): 758-767.

[33] Subramanyam, A. V., Sabu Emmanuel, and Mohan S. Kankanhalli. "Compressed-encrypted domain JPEG2000 image watermarking." *Multimedia and Expo (ICME), 2010 IEEE International Conference on*. IEEE, 2010.

List of Publications

Communicated:

1. Pushpak yadav, Maggi Bansal and Sumit Miglani " A Hybrid Approach for Image Security by Combining Watermarking with Encryption" 8th International Conference on Contemporary Computing(IC3), Noida, IEEE, 2015

Video URL:

https://www.youtube.com/watch?v=ndKRFFroW-s