DATA HIDING TECHNIQUE USING SECURE SPREAD-SPECTRUM AND DISCRETE WAVELET TRANSFORM

Enrollment No. - 101318
Name of Student - Vishal Aery
Name of supervisor - Mr. Amit kumar Singh

MAY-2014

Submitted in partial fulfillment of the Degree of
Bachelor of Technology

DEPARTMENT OF COMPUTER SCIENCE
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TABLE OF CONTENTS

Chapter No	Topics	Page No.
	Certificate from the Supervisor	iii
	Acknowledgement	iv
	Summary	v
Chapter-1	1.0 Digital watermarking	1
	1.1 History of water marking	5
	1.2 Defining watermarking	7
	1.3 Need of data hiding	7
	1.4 Types of watermarking	8
	1.4.1 Visible Watermarking	8
	1.4.2 Invisible Watermarking	8
	1.5 Principle of watermarking	9
	1.6 Characteristics of digital watermarking	10
	1.6.1 Robustness	11
	1.6.2 Tamper resistance	11
	1.6.3 Fidelity	13
	1.6.4 Computational cost	13
	1.6.5 False positive rate	14
	1.7 Requirements	15
	1.7.1 Security	15
	1.7.2 Imperceptibility	15
	1.7.3 Robustness	15
	1.7.4 Capacity or data load	16
	1.8 Applications of watermarking	16
	1.8.1 Copyright protection	16
	1.8.2 Authentication	16
	1.8.3 Broadcast monitoring	17
	1.8.4 Content labeling	17
	1.8.5 Tamper detection	17
	1.8.6 Digital fingerprinting	17
	1.8.7 Content protection	17
	1.9 Techniques or schemes of watermarking	17
	1.9.1 Spatial domain technique	17
	1.9.1.1 Least significant bit coding	17
	1.9.1.2 Predictive coding schemes	18
	1.9.1.3 Correlation-based techniques	18
	1.9.2 Frequency domain technique	18
	1.9.2.1 Discrete cosine transform(DCT) based technique	19
	1.9.2.2 Wavelet transform based watermarking	24

TABLE OF CONTENTS

Chapter No	Topics	Page No.
	1.10 Factors affecting digital watermark strength	24
	1.10.1 Image variation/randomness	25
	1.10.2 Image size	26
	1.10.3 Compression	26
	1.10.4 Randomness of image data	26
	1.11 Attacks	27
	1.11.1 Basic	27
	1.11.2 Robustness	27
	1.11.3 Presentation	27
	1.11.4 Interpretation	28
	1.11.5 Implementation	28
	1.11.6 Removal	28
	1.11.7 Geometrical	29
	1.11.8 Cryptographic	30
	1.11.9 Protocol	30
	1.11.10Active & Passive	31
	1.11.11Collusion	31
	1.11.12Distortive	31
Chapter-2	2.0 Literature Review	32
Chapter-3	Proposed Method for Image Watermarking	37
	3.0 About technique	37
	3.0.1 Spread spectrum watermarking	37
	3.0.2 Spread spectrum watermarking principle	38
	3.1 Proposed algorithm	38
	3.1.1 Embedding process	39
	3.1.2 Extraction process	40
Chapter-4	Experiments and Results	42
	4.0 Results	42
	4.1 Performance analysis	44
	4.2 Conclusion	47
	Appendix	48
	Reference	57

CERTIFICATE

This is to certify that the work titled "**Data Hiding Technique Using Secure Spread-Spectrum And Discrete Wavelet Transform"** submitted by **"Vishal Aery"** in partial fulfillment for the award of degree of B.Tech of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ……………………..
Name of Supervisor Mr. Amit Kumar Singh
Designation Assistant Professor
Date ……………………..

ACKNOWLEDGEMENT

First of all I would like to acknowledge the almighty god for bestowing his good wishes and giving me the strength at every moment of despair to complete this project.

It’s incumbent on my part to thank my project guide **Mr. Amit Kumar Singh** Dept. of Computer Science and Information Technology, Jaypee University of Information Technology, Waknaghat, Solan (H.P.) who has been a great support and guided us throughout the completion of my project.

Last but not the least I express my warm thanks to my respected parents and all my friends for their support and their constructive suggestions, which enabled me to bring improvements in my project.

Signature of the student ……………………..
Name of Student Vishal Aery
Date ……………………..

SUMMARY

This project focuses on implementing various techniques of watermarking as nowadays chunks of data are being embedded on digital media or distributed over the internet. Digital watermarking is the process of hiding a message related to digital signals in different forms like an image, song, video within the signal itself. The data which is distributed can be replicated easily without error, putting the rights of their owners at risk. When encrypted for distribution, the information can easily be decrypted and copied. The best way to discourage illegal copying is to insert information known as watermark, into the important data in such a way that it is impossible to separate the watermark from the data.

In this project, a secure spread-spectrum watermarking algorithm for the digital images is implemented using discrete wavelet transform (DWT). The algorithm applied is such that the watermark i.e, the message to be inserted in the form of logo is being embedding into the host cover image. In this, the watermark is spread over many different frequency bins so that each bin contains very little amount of energy and certainly undetectable. Robustness and image quality of the proposed method is calculated by *Normalized Correlation* (NC) and Peak Signal to Noise Ratio (PSNR). The performance of the proposed algorithm has been tested against various signal processing attacks. We found that the method is robust against different attacks.

-------------------------	---------------------------
Signature of Student	Signature of Supervisor
Name:	Name:
Date:	Date:

CHAPTER 1

DIGITAL IMAGE WATERMARKING

1.0 INTRODUCTION DATA HIDING

In computer science, data or information masking is the principle of separation of the design decisions in a computer program that are most likely to alter, thus protecting other parts of the program from widespread modification if the design decision is changed. Various methods like cryptography or steganography have been applied to ensure reliability, robustness, safety & security of the data hidden. Since now-a-days, many multinational companies & organizations, various artists want to have private right over their products, hence the necessity for a method that ensures authencity of their product has increases & so originates various data hiding techniques for this purpose. Therefore term encapsulation is often used conversely with information hiding.

Data hiding is a very prehistoric art such as Caesar Cipher, Vignere Cipher etc. In modern times, data hiding is associated with digital forms such as Cryptography, Steganography Cryptography & Watermarking. Reason behind data hiding is to hide personal, sensitive or private data; to avoid misuse of data. Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

The history of watermark dates back to the 13th century. Watermarks were used to indicate the paper brand and the mill that produced it in Italy. By the 18th century watermarks began to be used as anti- counterfeiting measures on money and other documents and in 1995 interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms. Throughout this report some of these techniques are discussed and one such technique is implemented. As many advances are made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods are designed to offer better security than what cryptography can offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Figure 1 explains how watermarking is derived from steganography[4].

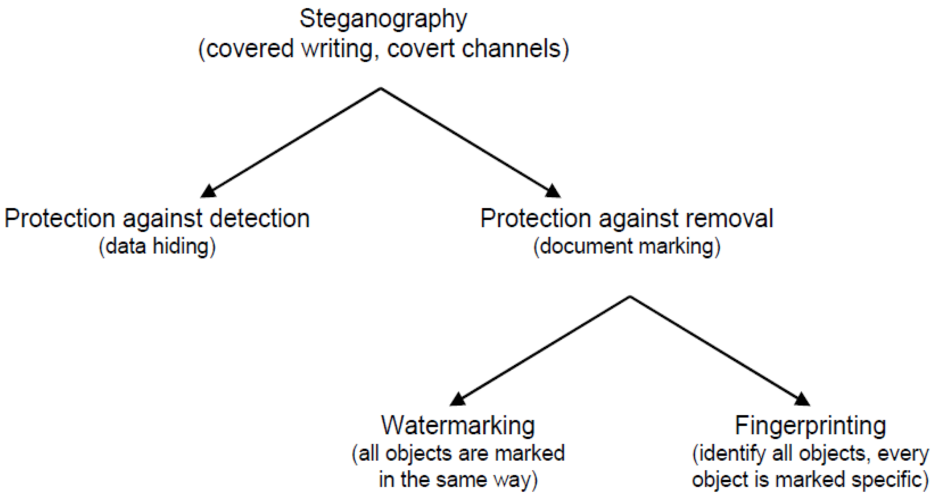

Steganography
(covered writing, covert channels)
Protection against detection
(data hiding)
Protection against removal
(document marking)
Watermarking
(all objects are marked in the same way)
Fingerprinting
(identify all objects, every object is marked specific)

Fig.1 Types of Steganography [4]

Steganography comes from the combination of the Greek words Stegano means sealed and Graphy referring to writing which means secret writing. Steganography is a very old art of embedding personal information into other data by using some rules and techniques. As a result, unauthorized users are not able to see and recognize the embedded information. Steganography is managing a secret path for sending information invisibly. Figure1 shows two general directions of steganography: protection against detection and protection against removal. Protection against detection uses some ways to embed information invisibly that does not degrade the quality of the original data. Protection against removal supposes that the method should be able to resist to common digital signal processing and noises. Removing the hidden data will definitely reduce the object's quality and its performance will not be functional.

There is an increased emphasis on the use of digital techniques in all aspects of human life today. Broadcast radio and television, cellular phone services, consumer and entertainment electronics etc are increasingly using digital signal processing techniques to improve the quality of service. Transmission and storage of documentation and images pertaining to patient records cannot remain an exception to this global trend. Hence, patient records (text and image information) are increasingly stored and processed in digital form. Currently, text and image information, which constitute two separate pieces of data are handled as different files. Thus, there is a possibility of the text and message information, pertaining to different patients, being interchanged and thus mishandled. This can be avoided by merging text and image information in such a manner that the two can be separated without perceptible damage to information contained in either file. Digital watermarking techniques can be used to interleave patient information with medical images.

Digital image watermarking is solitary such technology that has been made to protect digital images from illicit manipulations. It is a concept intimately related to steganography, in that they both hide a message inside a digital signal. Watermarking tries to hide a message related to the actual content of the digital signal, but in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking is used for providing a kind of security for various type of data(it may be image, audio, video, etc.). Watermarkin*g* is the process of embedding a message on a host signal.

Watermarking, as different to steganography, has the extra requirement of robustness against possible attacks. A watermark can be either visible or invisible. Using digital watermarking, copyright information can be implanted into the multimedia data. This is implemented by using some algorithms. Information such as number, images or text with special implication can be embedded. The purpose of this information can be for copyright protection, covert communication, authenticity distinguish of data file, etc.

TABLE1 Difference between Cryptography, Steganography and watermarking[20]

	Cryptography	**Steganography**	**Watermarking**
Techniques	Transposition, Substitution, RSA	LSB, Spatial Domain, steg, Out guess	compensated prediction, DCT
Naked eye Identification	Yes, as message is convert in Other way, which sough something is hidden	No, as message is Hide within other carrier (cover image)	Yes, as actual message is hiding by some watermark.
Capacity	Capacity is so high, but as message is long it chances to be decrypt	Differs as different Technology usually low hiding capacity	Capacity depends on the size of hidden data.
Detection	Not easy to detect ,depend on technology used to generate	Not easy to detect because to find steganographic image is hard.	Not easy to detect
Strength	Hide message by altering the message by assigning key	High	Extend information and become an attribute of the cover image
Imperceptibility	High	High	High

Applicability	Universally	Universally	Universally
Robust	Yes	Yes	Yes

1.1 HISTORY OF DATA HIDING

The idea of communicating secretly is as old as communication itself. Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in law. The second story also came from Herodotus, which claims that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece. Back then, the writing medium was written on wax-covered tablet. Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected[8].

Information hiding serves as an effective criterion for dividing any piece of equipment, software or hardware, into modules of functionality. For instance a car is a complex piece of equipment. In order to make the design, manufacturing, and maintenance of a car reasonable, the complex piece of equipment is divided into modules with particular interfaces hiding design decisions. By designing a car in this fashion, a car manufacturer can also offer various options while still having a vehicle which is economical to manufacture. For instance, a car manufacturer may have a luxury version of the car as well as a standard version. The luxury version comes with a more powerful engine than the standard version. The engineers designing the two different car engines, one for the luxury version and one for the standard version, provide the same interface for both engines. Both engines fit into the engine bay of the car which is the same between both versions. Both engines fit the same transmission, the same engine mounts, and the same controls. The differences in the engines are that the more powerful luxury version has a larger displacement with a fuel injection system that is programmed to provide the fuel air mixture that the larger displacement engine requires.

In addition to the more powerful engine, the luxury version may also offer other options such as a better radio with CD player, more comfortable seats, a better suspension system with wider tires, and different paint colors. With all of these changes, most of the car is the same between the standard version and the luxury version. The radio with CD player is a module which replaces the standard radio, also a module, in the luxury model. The more comfortable seats are installed into the same seat mounts as the standard types of seats. Whether the seats are leather or plastic, or offer lumbar support or not, doesn't matter. The engineers design the car by dividing the task up into pieces of work which are assigned to teams. Each team then designs their component to a particular standard or interface which allows the sub-team flexibility in the design of the component while at the same time ensuring that all of the components will fit together.

Motor vehicle manufacturers frequently use the same core structure for several different models, in part as a cost-control measure. Such a "platform" also provides an example of information hiding, since the floor pan can be built without knowing whether it is to be used in a sedan or a hatchback. As can be seen by this example, information hiding provides flexibility. This flexibility allows a programmer to modify functionality of a computer program during normal evolution as the computer program is changed to better fit the needs of users. When a computer program is well designed decomposing the source code solution into modules using the principle of information hiding, evolutionary changes are much easier because the changes typically are local rather than global changes. Cars provide another example of this in how they interface with drivers. They present a standard interface (pedals, wheel, shifter, signals, gauges, etc.) on which people are trained and licensed. Thus, people only have to learn to drive a car; they don't need to learn a completely different way of driving every time they drive a new model. (Granted, there are manual and automatic transmissions and other such differences, but on the whole cars maintain a unified interface.)

1.2 DEFINING WATERMARKING

Digital watermarking focuses mainly on the protection of intellectual property rights and the authentication of digital media. Similar to steganographic methods, digital watermarking methods hide information in digital media. The difference consists in the purpose of the hidden information – it pertains to the digital medium itself and contains information about its author, its buyer, the integrity of the content, etc. Digital watermarking methods help keeping track of the quick and inexpensive distribution of digital information over the Internet. They provide new ways of ensuring the adequate protection of copyright holders in the intellectual property distribution process. Using digital watermarking, copyright information can be embedded into the multimedia data. This is done by using some algorithms. Information such the serial number, images or text with special significance can be embedded. The function of this information can be for copyright protection, secret communication, authenticity distinguish of data file, etc.

1.3 NEED OF DATA HIDING

Data hiding bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models

Creating a watermark, for your digital images, is a great way to discourage people from copying photos that you may have on a website. While still allowing the image to be seen, most people will probably not want the picture as it is with the watermark on it. Creating a watermark and placing it on photos that you plan to post on the web will identify them as your own work and discourage people from copying them or claiming them as their own.

1.4 TYPES OF WATERMARKING

This is sub-divided into visible watermarks and invisible watermarks.

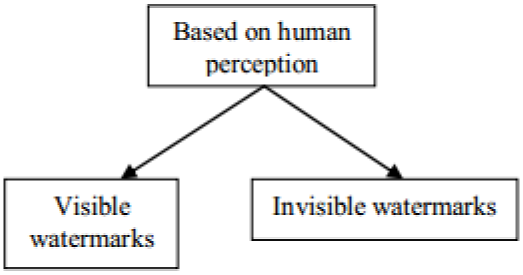


Fig.2 Classification of Watermarking[9]

1.4.1 VISIBLE WATERMARKS

These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal. The watermarked signal is different from the original signal.

1.4.2 INVISIBLE WATERMARKING

Invisible watermarking refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily. Invisible watermark can be further divided into three types,

Robust Watermarks

Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

Fragile Watermarks

They are designed with very low robustness. They are used to check the integrity of objects.

Public and Private Watermark

They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non-blind watermark or a private watermark.

1.5 PRINCIPLE OF WATERMARKING

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 3 shows the basic block diagram of watermarking process.

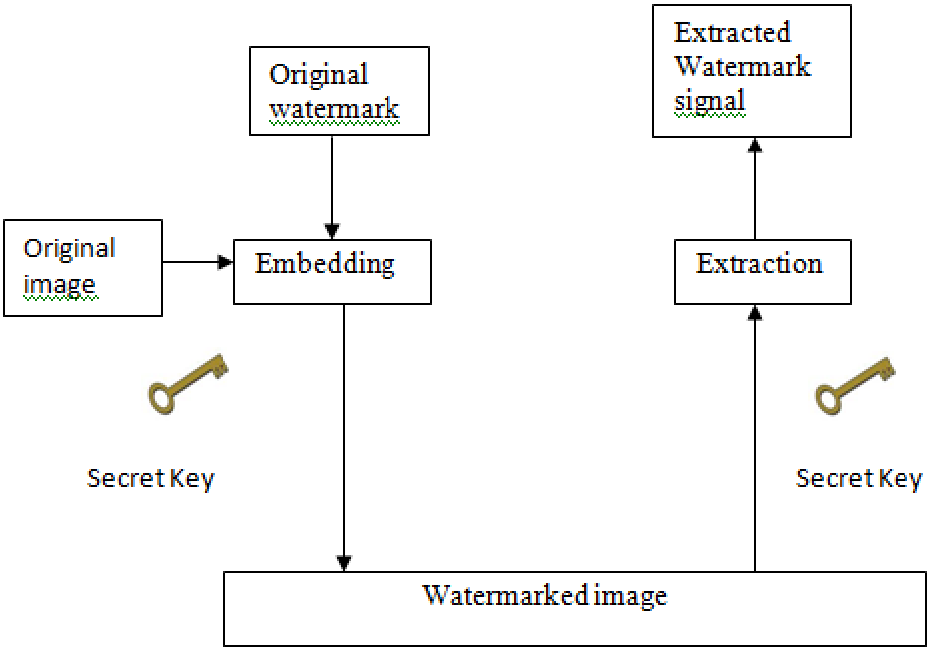


Fig.3 Watermarking block diagram

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

1.6 CHARACTERISTICS OF DIGITAL WATERMARKS

There are a number of papers that have discussed the characteristics of watermarks. Some of the properties discussed are robustness, tamper resistance, fidelity, computational cost, and false positive rate. In practice, it is probably impossible to design a watermarking system that excels at all of these. Thus, it is necessary to make tradeoffs between them, and those tradeoffs must be chosen with careful analysis of the application. In addition, the application can affect the very definition of a property. In the following subsections, we look at each of the five properties listed above, and discuss how its importance and definition varies with application.[15]

1.6.1 ROBUSTNESS

A watermark is said to be robust if it survives common signal processing operations such as digital-to analog-to digital conversions and lossy compression. More recently, there has been an increased concern that video and still image watermarks also be robust to geometric transformations. Robustness is often thought of as a single-dimensional value, but this is incorrect. A watermark that is robust against one process may be very fragile against another. In many applications, robustness to all possible processing is excessive and unnecessary. Usually, a watermark must survive common signal processing only between the time of embedding and the time of detection. For example, in television and radio broadcast monitoring, the watermark need only survive the transmission process. For television, this means lossy compression, analog transmission, and some small amount of horizontal and vertical translation. It need not survive rotation, scaling, high-pass filtering, or any of a wide variety of distortions that do not occur during broadcast. In some cases, robustness may be completely irrelevant, or even undesirable. Watermarks used for covert communication need not be robust at all, if the cover media will be transmitted digitally without compression. A watermark for simple authentication, which just indicates whether the media has been altered, should be fragile. On the other hand, when the signal processing between embedding and detection is unpredictable, the watermark may need to be robust to every conceivable distortion. This is the case for owner identification, proof of ownership, fingerprinting, and copy control. It is also true for any application in which hackers might want to remove the watermark.

1.6.2 TAMPER RESISTANCE

Tamper resistance refers to a watermarking system's resistance to hostile attacks. There are several types of tamper resistance. Depending on the application, certain types of attacks are more important than others. In fact, there are several applications in which the watermark has no hostile enemies, and tamper resistance is irrelevant. Some basic types of attack are

- ✓ Active attacks. Here the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting, and copy control, in which the purpose of the mark is defeated when it cannot be detected. However, it is not a serious problem for authentication or covert communication.

✓ Passive attacks. In this case, the hacker is not trying to remove the watermark, but is simply trying to determine whether a mark is present, i.e. is trying to identify a covert communication. Most of the scenarios above are not concerned with this type of attack. In fact, we might even advertise the presence of the mark so that it can serve as a deterrent. But for covert communication, our primary interest is to prevent the watermark from being observed.

✓ Collusion attacks. These are a special case of active attacks, in which the hacker uses several copies of one piece of media, each with a different watermark, to construct a copy with no watermark. Resistance to collusion attacks can be critical in a fingerprinting application, which entails putting a different mark in each copy of a piece of media. However, the number of copies that we can expect the hacker to obtain varies greatly from application to application. For example, in the DiVX application, a hacker can buy any number of DiVX players, and play one movie on all of them to obtain any number of differently-watermarked copies. On the other hand, in the film-studio dailies application, each employee can only obtain one copy of the watermarked material. A collusion attack would require that several employees conspire to steal the material, which is an unlikely prospect.

✓ Forgery attacks. Here, the hacker tries to embed a valid watermark, rather than remove one. These are our main security concern in authentication applications, since, if hackers can embed valid authentication marks, they can cause the watermark detector to accept bogus or modified media.

1.6.3 FIDELITY

A watermark is said to have high fidelity if the degredation it causes is very difficult for a viewer to perceive. However, it only needs to be imperceptible at the time that the media is viewed. If we can be certain that the media will be seriously degraded before it is viewed, we can rely on that degradation to help mask the watermark. Such a case occurs when we watermark video that will be transmitted over NTSC, or audio that will be transmitted over AM radio. The quality of these broadcast technologies is so low that our initial fidelity need not be very good. Conversely, in HDTV and DVD video and audio, the signals are very high quality, and require much higher fidelity watermarks (though, of course, the quality of the content remains the same - a bad movie is a bad movie whether on VHS or DVD). In some applications, we can accept mildly perceptible watermarks in exchange for higher robustness or lower cost. For example, Hollywood dailies are not finished products. They are usually the results of poor transfers from film to video.[16] Their only purpose is to show those involved in a film production the raw material that has been shot so far. A small visible distortion caused by a watermark will not diminish their value.

1.6.4 COMPUTATIONAL COST

Different applications require the embedders and detectors to work at different speeds. In broadcast monitoring, both embedders and detectors must work in (at least) real time. The embedders must not slow down the media production schedule, and the detectors must keep up with real time broadcasts. On the other hand, a detector for proof of ownership will be valuable even if it takes days to find a watermark. Such a detector will only be used during ownership disputes, which are rare, and its conclusion about whether the watermark is present is important enough that the user will be willing to wait. Furthermore, different applications require different numbers of embedders and detectors. Broadcast monitoring typically requires a few embedders and perhaps several hundred detectors at different geographic locations. Copy control applications may need only a handful of embedders but millions of detectors. Conversely, in the fingerprinting application implemented by DiVX, in which each player embeds a distinct watermark, there would be millions of embedders and only a handful of detectors. In general, the more numerous a device needs to be for a given application, the less it must cost. The wide variation in dollar cost and in speed requirements means that there is a wide variation in the required computational efficiency of watermark embedders and detectors.

1.6.5 FALSE POSITIVE RATE

A false positive is a detection of a watermark in a piece of media that does not actually contain that watermark. When we talk of the false positive rate, we refer to the number of false positives we expect to occur in a given number of runs of the detector. Equivalently, we can discuss the probability that a false positive will occur in any given detector run. There are two subtly different ways to define this probability that are often confused in the literature. They differ in whether the watermark or the media is considered to be the random variable. In the first definition, the probability of a false positive is the probability that, given a fixed piece of media and a randomly-selected watermark, the detector will report that the watermark is in the media. The watermarks are drawn from a distribution that is defined by the design of a watermark generation system.

Typically, watermarks are generated by either a bit-encoding algorithm or by a Gaussian, independent random number generator. In many cases, probability of false positives, according to this first definition is actually independent of the piece of media, and depends only on the method of watermark generation. In the second definition, the probability of a false positive is the probability that, given a fixed watermark and a randomly-selected piece of media, the detector will detect the watermark in the media. The media is chosen from the distribution of natural media, which is defined by either nature or Hollywood, depending on the application. This distribution is very different from that defined by the watermark generation system, and thus probabilities based on this definition can be quite different from those based on the first definition. In most applications, we are more interested in the second definition of false positive probability than in the first. However, in a few cases, the first definition is also important, such as in the case of fingerprinting, where the detection of a random watermark in a given image might lead to a false accusation of theft. The probability of false positives that is required depends on the application. In the case of proof of ownership, the detector is used so rarely that a probability of 10−6 should suffice to make false positives unheard of. On the other hand, in the copy control application, millions of watermark detectors are constantly being run on millions of pieces of media all over the world.

If one piece of un-watermarked media consistently generates false positives, it could cause serious trouble. For this reason, the false positive rate should be infinitesimal. For example, the general consensus is that watermark detectors for DVD video should have a false positive rate of 1 in 1012 frames.

1.7 REQUIREMENTS

The major requirements of digital watermarking are:

1.7.1 Security: The security requirement of a watermarking system can differ slightly depending on the application. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks.

1.7.2 Imperceptibility: The imperceptibility refers to the perceptual transparency of the watermark. Ideally, no perceptible difference between the watermarked and original signal should exist. A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal. However, this makes it easy for an attacker to alter the watermark information without being noticed.

1.7.3 Robustness: This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. Watermark robustness accounts for the capability of the watermark to survive signal manipulations. Apart from malicious attacks, common signal processing operations can pose a threat to the detection of watermark, thus making it desirable to design a watermark that can survive those operations. For example, a good strategy to robustly embed a watermark into an image is to insert it into perceptually significant parts of the image. Therefore, robustness is guaranteed when we consider the case of lossy compression which usually discards perceptually insignificant data, thus data hidden in perceptual significant portions is likely to survive lossy compression operation. However, as this portion of the host signal is more sensitive to alterations, watermarking may produce visible distortions in the host signal. The exact level of robustness an algorithm must possess cannot be specified without considering the application scenario. Not all watermarking applications require a watermark to be robust enough to survive all attacks and signal processing operations. Indeed, a watermark needs only to survive the attacks and those signal processing operations that are likely to occur during the period when the watermarked signal is in communication channel. In an extreme case, robustness may be completely irrelevant in some case where fragility is desirable.

1.7.4 Capacity or Data Load: This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the water during extraction. Watermarking capacity normally refers to the amount of information that can be embedded into a host signal. Generally speaking, capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness. A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.[17]

1.8 APPLICATIONS OF WATERMARKING

1.8.1 Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

1.8.2 Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

1.8.3 Broadcast Monitoring: As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

1.8.4 Content Labeling: Watermarks can be used to give more information about the cover object. This process is named content labeling.

1.8.5 Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

1.8.6 Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

1.8.7 Content protection: In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

1.9 TECHNIQUES OR SCHEMES OF WATERMARKING

1.9.1 Spatial Domain Techniques

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression.

1.9.1.1 Least Significant Bit Coding (LSB)

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

1.9.1.2 Predictive Coding Schemes

Predictive coding scheme was proposed by Matsui and Tanaka for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.[18]

1.9.1.3 Correlation-Based Techniques

In this method a pseudo random noise (PN) with a pattern W(x, y) is added to an image, according to the equation where,

Iw(x,y) = Watermarked image.

I(x,y)=Original image

k=gain factor

Increasing *k* increases the robustness of the watermark at the expense of the quality of the watermarked image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

1.9.2 Frequency Domain techniques

All signals have a frequency domain representation and in 1822, Baron Jean Baptiste Fourier detailed the theory that any real world waveform can be generated by the addition of sinusoidal waves.

1.9.2.1 Discrete cosine transform (DCT) based technique:

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforms from this class are “sinusoidal“, which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum. Therefore one speaks about transformation to the frequency domain. The most popular member of this class is the Discrete Fourier Transformation (DFT).The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry DCT and DFT are equivalent. There are eight different variants of DCT. There is a very slight modification between these eight variants.

DCT –I

In JPEG compression the input data are two-dimensional, presented in 8x8 blocks. There's a need of using two-dimensional DCT. Since each dimension can be handled separately, the two-dimensional DCT follows straightforward form the one-dimensional DCT. A one-dimensional DCT is performed along the row and then along the columns, or vice-versa.

The formula used for one-dimensional DCT:

$$F(u)=C(u)\sum_{x=0}^{N-1} f(x)\cos[\frac{\pi(2x+1)u}{2N}]$$

$$where\ u=0,1,\ldots N-1$$

$$C(u)=\sqrt{\frac{1}{N}}\ \ when\ u=0\quad C(u)=\sqrt{\frac{2}{N}}\ \ when\ u\neq 0$$

DCT –II

The formula used for two-dimensional DCT:

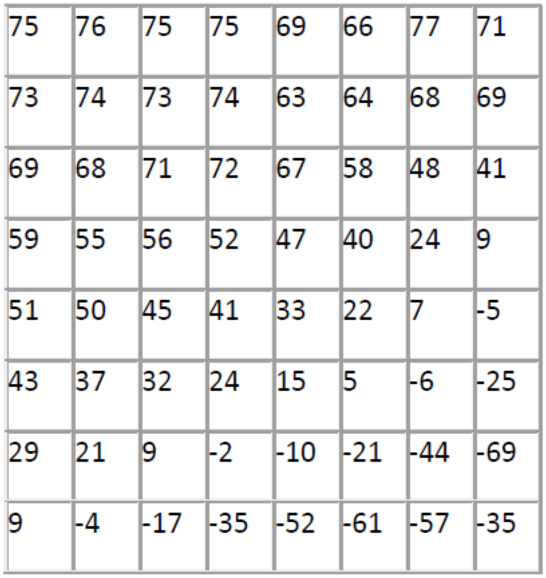
$$F(u,v)=C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\cos[\frac{\pi(2x+1)u}{2N}]\cos[\frac{\pi(2y+1)v}{2N}]$$

$$where\, u=0,1,\ldots N-1 \quad v=0,1,\ldots M-1$$

$$C(u),C(v)=\sqrt{\frac{1}{N}} \; when\, u,v=0 \quad C(u),C(v)=\sqrt{\frac{2}{N}} \; when\, u,v\neq 0$$

Applying these formulas directly requires much computational resources therefore an implementation in hardware can be very efficient.

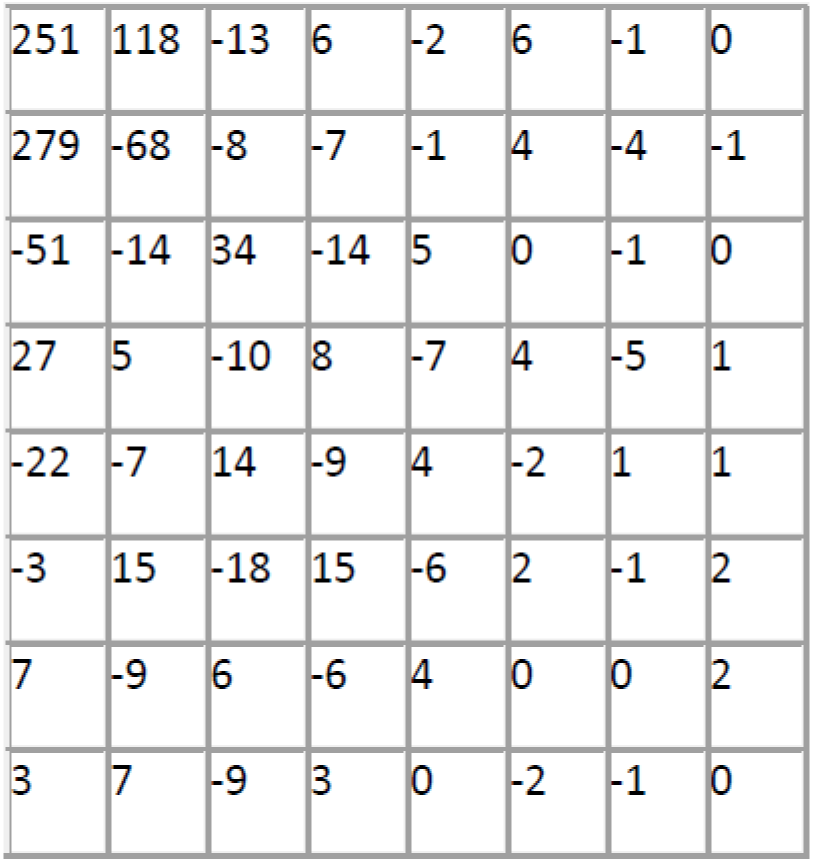
The figure below shows example of 8x8 blocks before DCT.



75	76	75	75	69	66	77	71
73	74	73	74	63	64	68	69
69	68	71	72	67	58	48	41
59	55	56	52	47	40	24	9
51	50	45	41	33	22	7	-5
43	37	32	24	15	5	-6	-25
29	21	9	-2	-10	-21	-44	-69
9	-4	-17	-35	-52	-61	-57	-35

Fig.4 8X8 example block before DCT

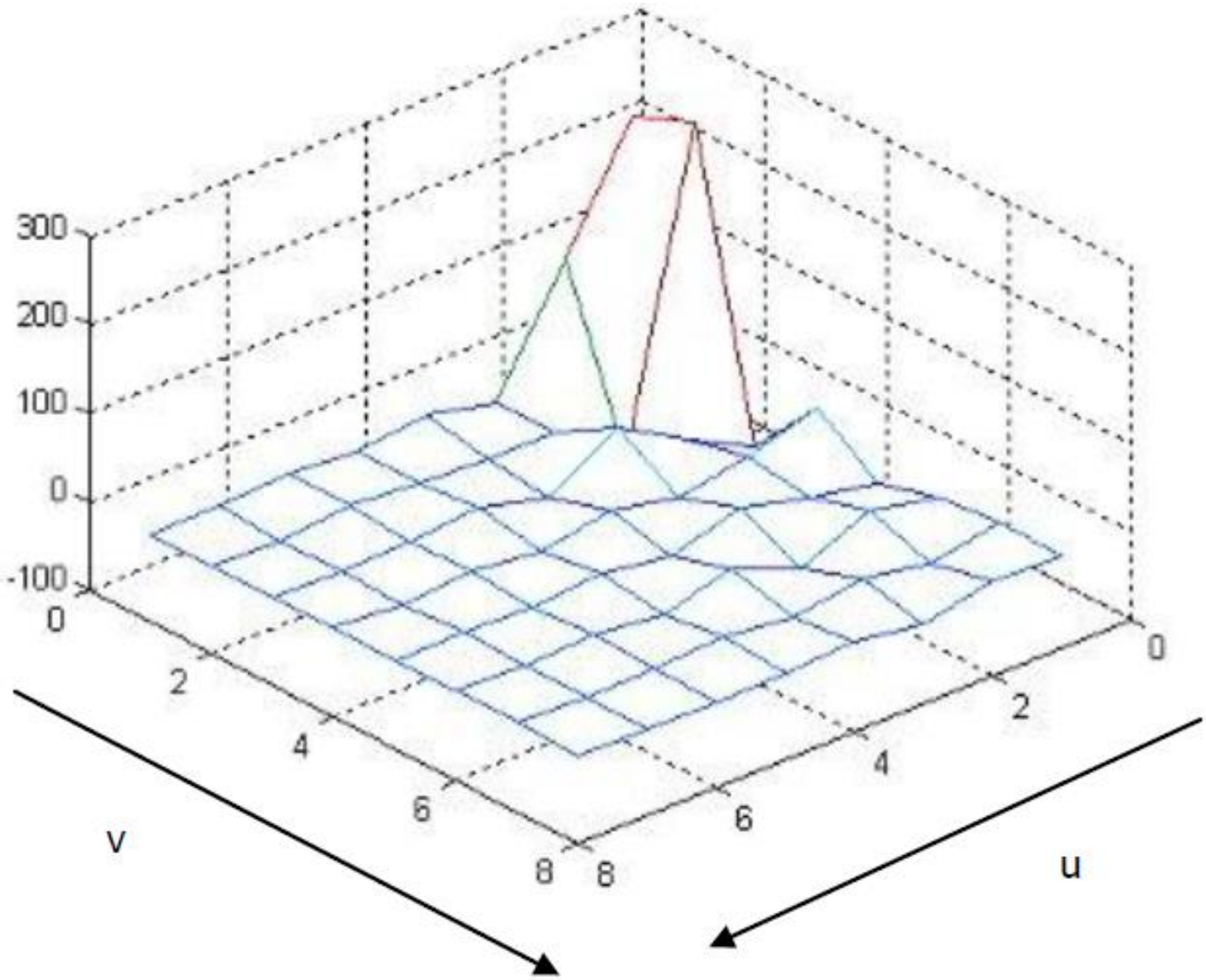
After Discrete Cosine Transform the block has following values:



251	118	-13	6	-2	6	-1	0
279	-68	-8	-7	-1	4	-4	-1
-51	-14	34	-14	5	0	-1	0
27	5	-10	8	-7	4	-5	1
-22	-7	14	-9	4	-2	1	1
-3	15	-18	15	-6	2	-1	2
7	-9	6	-6	4	0	0	2
3	7	-9	3	0	-2	-1	0

Fig.5   After 2D-DCT of the 8X8 block shown in Fig.4

As it can be seen higher values of transform coefficients are concentrated on the top left corner. In the frequency domain it looks like low frequency has advantage over high frequency. It is shown on the figure 6



As you can see only small amount of low frequency elements dominates over the rest of the coefficients. It allows reducing data during next stages of JPEG compression.

The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. Most of the energy in the DCT domain is concentrated in the low frequencies. As is known low frequencies are perceived very well by human eye, hence the chances of the watermark being perceptible is high where as high frequencies are prone to attacks such as compression and scaling. So, a tradeoff has to be made.

Basic Steps:

1. The image is segmented into non-overlapping blocks of 8x8.
2. Forward DCT is applied to each of the block.
3. Selection criteria are then applied.
4. This is followed by applying coefficient selection criteria.
5. Embed watermark by modifying the selected coefficients.
6. Inverse DCT is applied to obtain the final watermarked image.

Block Diagram:

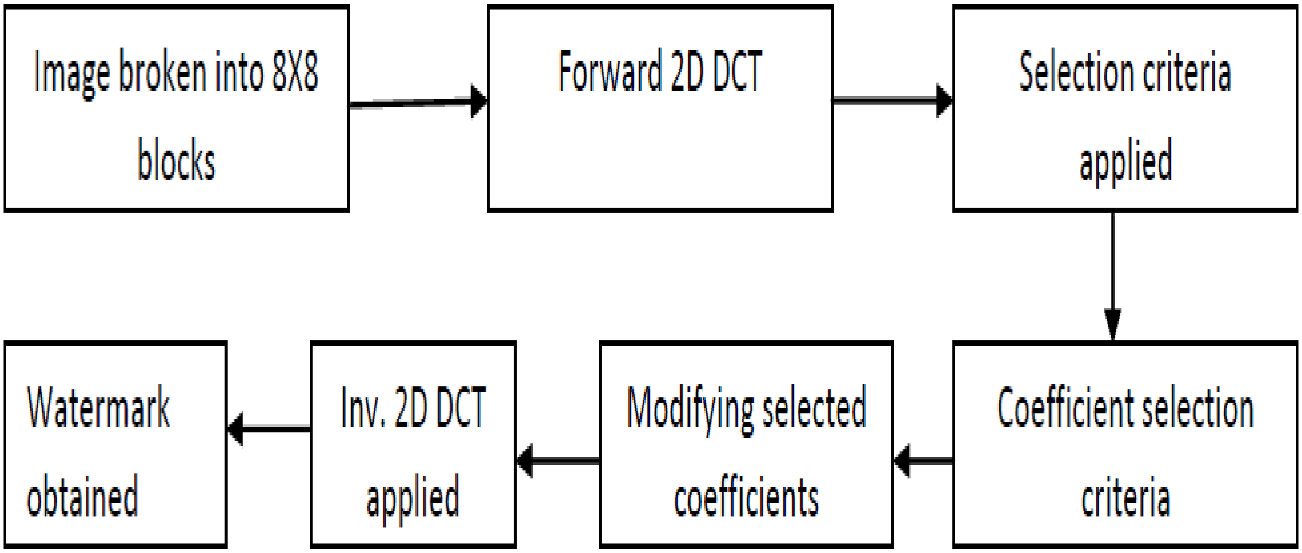


Image broken into 8X8 blocks
Forward 2D DCT
Selection criteria applied
Coefficient selection criteria
Modifying selected coefficients
Inv. 2D DCT applied
Watermark obtained

Fig.7 Block diagram of watermarking steps using DCT[13]

1.9.2.2 Wavelet Transform based Watermarking

The Fourier transform is an analysis of global frequency content in the signal. There are applications in digital image processing wherein we need the localized frequency components. This can be done by using the Short Time Fourier Transform . This is similar to the concept of using windowing functions. The windowed transform is given as

$$F(\omega,\alpha) = \int_{-\infty}^{\infty} f(x)g(x-\alpha)\, e^{-j\omega x}dx$$

Where ‘w’ denotes the frequency and ‘alpha’ denotes the position of the window. This equation transforms the signal f(x) in a small window around ‘alpha’. The STFT is then performed on the signal and local information is extracted. The wavelet transform based watermarking technique divides the image into four sidebands – a low Resolution approximation of the tile component and the component’s horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform.

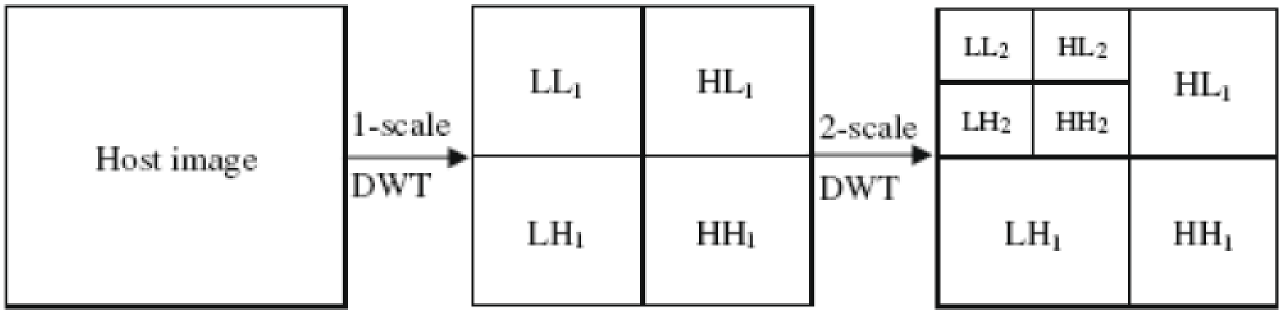


Fig.8 Wavelet based transforms

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the human visual system (HVS) as compared to the DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. One of the most straightforward techniques is to use embedding technique similar to that used in the DCT,

$$I_{W\,u,v} = \begin{cases} W_i + \alpha \left| W_i \right| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases}$$

In the Wavelet Domain where   denotes the coefficient of the transformed image, i the bit of the watermark to be embedded, and α a scaling factor. To detect the watermark the same process as that used in DCT is implemented. Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients.

1.10 FACTORS AFFECTING DIGITAL WATERMARK STRENGTH

Along with the intensity setting that you choose when embedding a watermark, the strength of a digital watermark is also affected by the following factors:

1.10.1 Image variations/randomness: The successful embedding of a digital watermark is dependent on the variation and randomness present in the pixels making up the image. For example, if you are working with an image that contains more flat color regions than detailed areas, you may want to choose a higher digital watermark strength so that the watermark will overcome the limitations of the specific image. This may result in a more visible digital watermark, but in some situations that is an acceptable trade-off.

1.10.2 Image size: As far as possible the Watermarks should be immune to Image size.

1.10.3 Compression: Saving the watermarked image in a compressed format may affect the durability of the digital watermark. The following factors will influence the impact that lossy compression has on digital watermark survival:

- **Level of image compression:** Lossy compression degrades the image to some extent, depending upon the quality setting chosen when saving in compressed format; most digital watermarks will survive as long as a moderate level of compression is used.

- **Visibility/durability setting used when embedding a digital watermark:** The higher the intensity setting, the better the chances the digital watermark will survive compression. Again, a higher-intensity digital watermark provides more data-to-survive compression. Since the visual quality of compressed images is often somewhat compromised anyway, generally a higher watermark intensity setting yields quite acceptable results.

- **Image size:** The greater the number of pixels in the image, the more the digital watermark can be repeated throughout it; the recommended minimum size for an image that will be compressed is 256 x 256 pixels. The larger the image, the better the digital watermark will survive compression.

1.10.4 Randomness of image data: As discussed in the earlier section "Image variations/randomness," the more randomness and/or color variation in an image, the better; a flat color space with little gradation may not survive well, while an image with more detail and contrast will fare better. Since a digital watermark is applied more strongly within areas of high contrast or variation, an image that contains more contrast and/or variation than others will contain more digital watermark data and thus stand a better chance of surviving compression.

1.11 ATTACKS

“Digital watermarking is not as secure as date encryption. Therefore, digital watermarking is not immune to hacker attacks” . Watermarking attacks are broadly divided into the following categories:

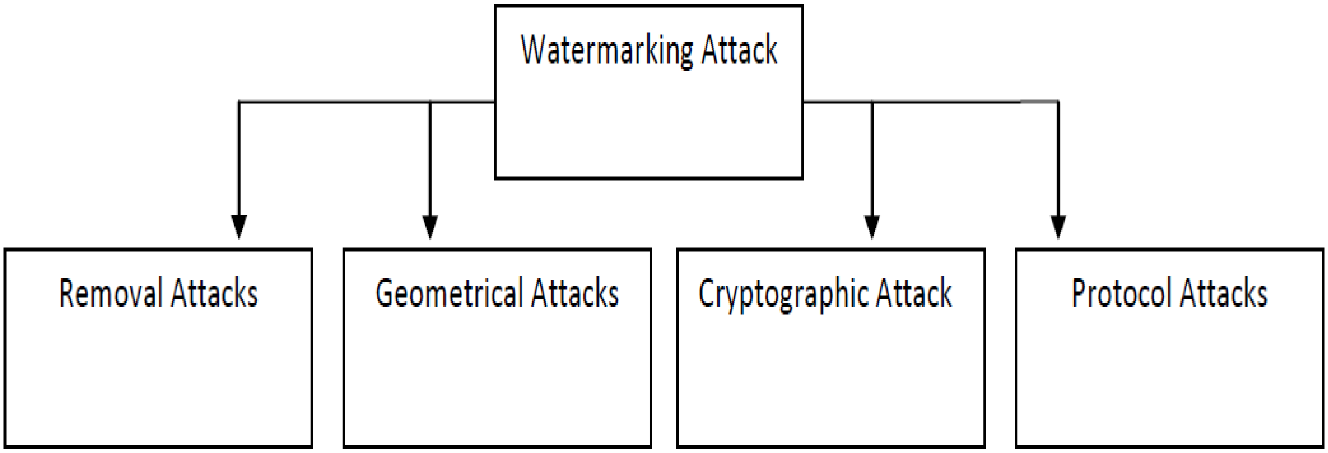


Fig 9 Types of Watermark Attacks[18]

1.11.1 Basic

In basic attack, the attacker takes advantage of the limitations in design of the embedding technique. As the name suggests the attack is very basic and can be easily resolved.

1.11.2 Robustness

This may include removal attacks where the attacker aims at removal of the watermark from the cover data. Also the attacker may try to diminish the data.

1.11.3 Presentation

These attacks modify the content of the file in order to prevent the detection of the watermark. The mosaic attack takes advantage of size requirements for embedding a watermark. By splitting the marked file into small sections, the mark detection can be confused. Many web browsers will draw images together with no visible split enabling the full image to be effectively restored while hiding the mark. If the minimum size for embedding the mark is small enough the mosaic attack is not practical. This attack can defeat web crawlers which download pictures from the Internet and check them for the presence of a watermark.

1.11.4 Interpretation

These attacks find a situation where ownership certification is prevented. They rely on misinterpretation the data to comply with ownership certification

1.11.5 Implementation

This method Attacks the detection software. A marking system can provide more opportunities for attack than the marking technique itself. If the mark detection software is vulnerable it may be possible for attackers to deceive it.

1.11.6 Removal

Removal Attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding). That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., for compression), remodulation, and collusion attacks. Not all of these methods always come close *to* their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly. Sophisticated removal attacks try to optimize operations like denoising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, statistical models for the watermark and the original data are exploited within the optimization process. Collusion attacks are applicable when many copies of a given data set, each signed with a key

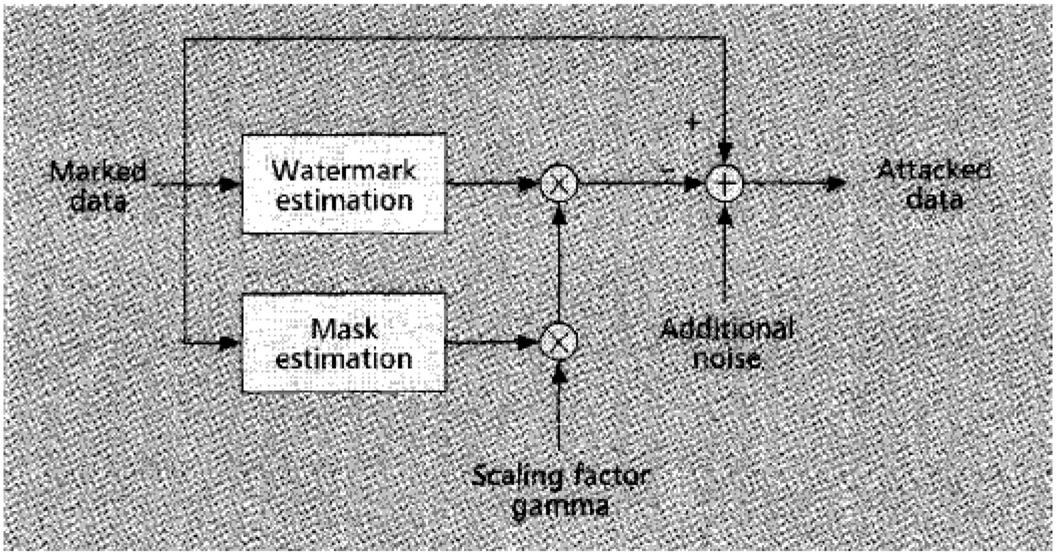


Figure10. A perceptual demodulation attack[18]

or different watermark, can be obtained by an attacker or a group of attackers. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy.

1.11.7 Geometrical

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform-invariant domain (Fourier-Melline) or an additional template, or specially designed periodic watermarks whose auto-covariance function (ACF) allows estimation of the geometric distortions. However, as discussed below, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is more or less a solved issue. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist this attack.

1.11.8 Cryptographic

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.

1.11.9 Protocol

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks**.** The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be noninvertible. The requirement of non-invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document.

A solution to this problem might be to make watermarks signal-dependent by using one-way functions. Another protocol attack is the copy attack. In this case, the goal **is** not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant to the copy attack.

1.11.10 Active & Passive

Attacker removes or spoils the watermark. Attacker just identifies the watermark and does not damage it.

1.11.11 Collusion

Attacker decodes different copies with different watermarks and joins them to make one single watermark.

1.11.12 Distortive

Attacker applies distortive transformation to make the watermark undetectable by any other person & making it unreadable by the end receiver.

Formula used

Peak Signal to Noise Ratio (PSNR) - The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. When comparing compression codec, PSNR is an approximation to human perception of reconstruction quality. A higher PSNR generally indicates that the reconstruction is of higher quality and vice versa. PSNR is most easily defined via the mean squared error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K,MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

$$PSNR = 10 * \log(10) (MAX_i^2/MSE)$$

Normalized Coefficient – Normalized correlation is a standard method of estimating the degree to which two series are correlated. Consider two series x(i) and y(i) where i=0,1,2...N-1. Cross

$$r = \frac{\sum_i [(x(i) - mx) * (y(i-d) - my)]}{\sqrt{\sum_i [(x(i) - mx) * (x(i) - mx)]}\sqrt{\sum_i [(y(i-d) - my) * (y(i-d) - my)]}}$$

correlation r at delay d is defined as Where mx and my are the means of the corresponding series. If the above is computed for all delays d=0, 1, 2,...N-1 then it results in a cross correlation series of twice the length as the original series.

CHAPTER 2

LITERATURE REVIEW

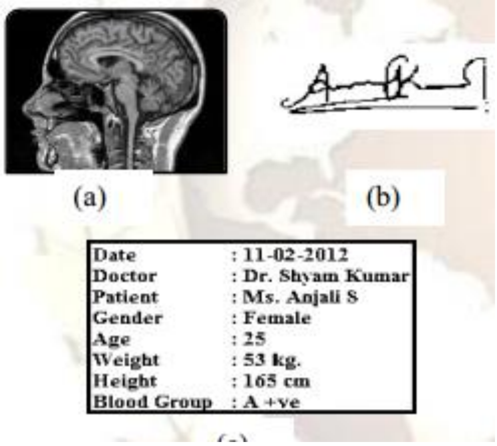
2.0 LITERATURE SURVEY

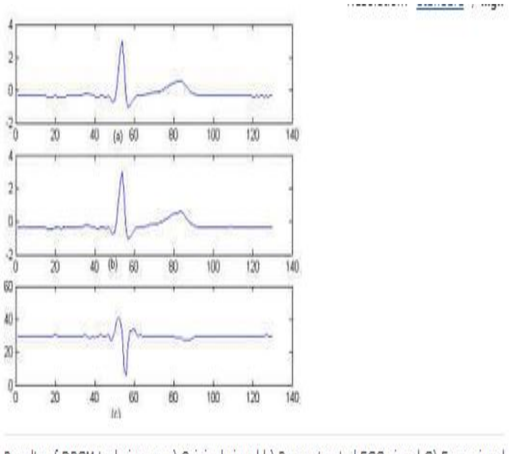
Before getting into the details of the secure spread spectrum technique variety of researchers and scholars have proposed their working research materials on watermarking that employees different techniques such as techniques like Singular Value Decomposition, Discrete Cosine Transform, Discrete Wavelet Transform and a combination of spatial domain and transform domain techniques etc. The researches on various techniques by different researchers are briefly described below.

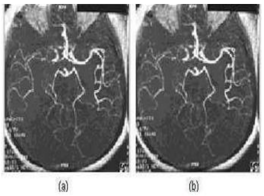
Singh et al. [1] has discussed steganography approach for hiding image in DCT domain watermarking algorithm for digital images: the method, which operates in the frequency domain and embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After they proposed embedding, the watermark is adapted to the image by exploiting the characteristics of the human visual system, thus ensuring the watermark invisibility. By exploiting the statistical properties of the embedded sequence, the watermark can be extracted without resorting to the original uncorrupted image. The watermark has been tested using various types of noise such as Gaussian and Salt & Pepper. DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. Elizabeth Philip et al. [2] proposed a technique based on Telemedicine Applications. This watermarking algorithm is used for embedding watermark like patient's history and doctor's signature in binary image format into host's medical image for telemedicine applications. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality as this may cause a misdiagnosis. This kind of a system requires a high level of security, which can be ensured by using digital watermarking techniques. This imposes three mandatory characteristics: robustness, capacity and imperceptibility. There are different methods that has been using for medical image watermarking. The watermark can directly be embedded in the LSB also. Security of medical information, derived from strict ethics and governmental rules, gives rights to the patient and duties to the health professionals. This imposes three compulsory characteristics: robustness, imperceptibility, capacity. Robustness is defined as the ability of watermark to resist against both lawful and illicit attacks. One of the stringent requirements of the image watermarking is the imperceptibility. Imperceptibility means that watermark embedded in the image must be invisible to the human eye. In watermarking of medical images, all the information necessary for physician such as identification of patient, diagnosis report, origin identification (who created the image) are embedded. This information is further increased when the image is sent to other physician for second opinion. Therefore, capacity for embedding the payload must be high. Nayak et al. [3] has proposed Digital watermarking is a technique of hiding specific identification data for copyright authentication. This technique is adapted here for interleaving patient information with medical images, to reduce storage and transmission overheads.

In this patient information is encrypted before interleaving with images to ensure greater security. The bio-signals are compressed and subsequently interleaved with the image. This interleaving is carried out in the spatial domain and Frequency domain. The performance of interleaving in the spatial, Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) coefficients is studied. Differential pulse code modulation (DPCM) is employed for data compression as well as encryption . The Differential Pulse Code Modulation (DPCM) technique is extensively used to reduce the dynamic range of the signal. The DPCM is used here for encrypting the ECG signal. The ASCII code of the encrypted text is swapped with the least significant bit of the pixels in the image. Each bit in the ASCII code of the text is placed at last bit of the pixels in the image. This procedure is repeated for all the ASCII codes of given text. It can be seen that one ASCII code can be hidden in eight pixels of the given image. Similarly the graphic files of bio-signals are also interleaved in the pixels using above said procedure. The graphic file is encrypted using DPCM. In this study ECG is used as a bio-signal which is encrypted. For interleaving the LSB of each DCT coefficient is replaced by the text data. Reddy et al. [8] has discussed LSB Steganography and its Evaluation for Various files Formats. They explains the steganography which refers to the science of “invisible” communication. For hiding secret information in various file formats, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. The Least Significant Bit (LSB) embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format. This paper explains the LSB Embedding technique and Presents the evaluation for various file formats.

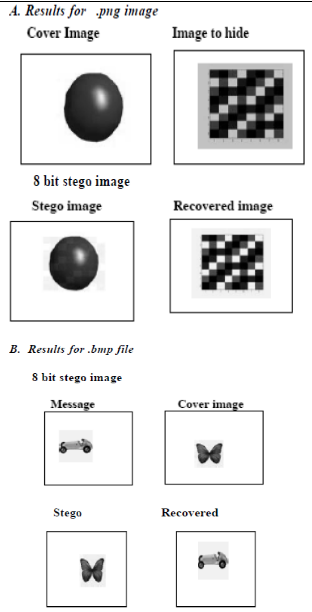
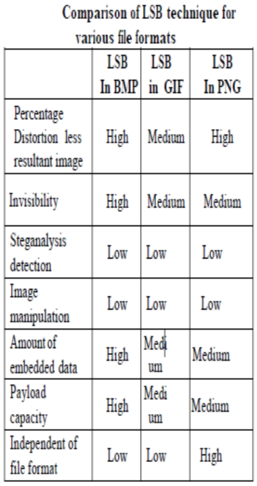
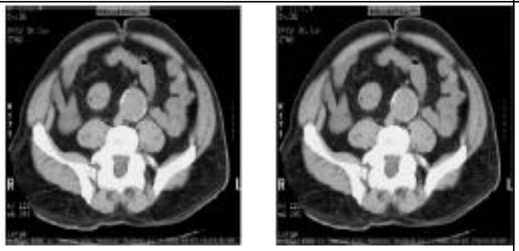
There are many steganographic algorithms available. Steganographic algorithms chosen must be such that it overcomes such manipulation and the steganographic data reaches the destination in the required format. Kumar et al. [17] presents a secure spread-spectrum watermarking algorithm for digital images in discrete wavelet transform (DWT) domain. The algorithm is applied for embedding watermarks like patient identification/source identification or doctors signature in binary image format into host digital radiological image for potential telemedicine applications. Performance of the algorithm is analysed by varying the gain factor, sub-band decomposition levels, size of watermark, wavelet filters and medical image modalities. Simulation results show that the proposed method achieves higher security and robustness against various attacks. W.N Cheung [19] reviews both spatial and frequency domain watermark embedding schemes for single-frame images. It focuses on the application of quantum distributed private keys in the concealment of data in images. Simple examples are used to illustrate the approach. In the spatial domain, differential PCM is used to detect the edge regions of the image so that data can be hidden on those pixels of the image when the differential signal is larger than a certain threshold level. The method is based on the visual masking phenomenon at large intensity transitions in the neighborhood of the pixel. In the frequency domain, DCT coefficients with significant variance are chosen and modulated using the private key sequence. Both spatial and DCT schemes are evaluated in terms of peak signal-to-noise ratio (PSNR).

<table>
<tr><th>S. no</th><th>Author name/Year</th><th>Techniqu-e</th><th>Image Details</th><th>Result</th></tr>
<tr><td>1</td><td>Blossom Kaur, Jasdeep Singh, Amandeep Kaur/2011</td><td>Digital Cosine Transform</td><td>
</td><td>PSNR=51.12 at noise density 0.02
PSNR=41.63 at noise density 0.06</td></tr>
<tr><td>2</td><td>Remya Elizabeth Philip, Sumithra M.G./2013</td><td>DCT and DWT</td><td>

Date : 11-02-2012
Doctor : Dr. Shyam Kumar
Patient : Ms. Anjali S
Gender : Female
Age : 25
Weight : 53 kg.
Height : 165 cm
Blood Group : A +ve</td><td><table>
<tr><th>Alpha</th><th>DWT level1</th><th>DWT level2</th><th>DWT level3</th><th></th></tr>
<tr><td>5</td><td>85.9218</td><td>87.603</td><td>96.773</td><td></td></tr>
<tr><td>8</td><td>76.731</td><td>77.239</td><td>87.687</td><td></td></tr>
<tr><td>15</td><td>63.633</td><td>64.458</td><td>78.967</td><td></td></tr>
</table></td></tr>
<tr><td>3</td><td>Jagadish Nayak, PSubbanna Bhat, Rajendra Acharya and Niranjan UC/2004</td><td>DPCM TECHNIQUE And DCT</td><td>DATA SIZE 130 BYTES


Results of DPCM techniques: a) Original signal b) Reconstructed ECG signal C) Error signal
Original MRI size is 8*8 pixel</td><td>The error signal e_n obtained from DPCM is interleaved into the DCT coefficients of the MRI image The resulting interleaved image


Result of interleaving DPCM error in the MRI Image in DCT domain:</td></tr>
</table>

<table>
<tr><th>S. no</th><th>Author name/Year</th><th>Technique</th><th>Image Details</th><th>Result</th></tr>
<tr><td>4</td><td>V. Lokeswara Reddy, Dr. A. Subramanym , Dr.P.Chenna Reddy /2007</td><td>Spatial domain</td><td>
</td><td>
Comparison of LSB technique for various file formats
<table>
<tr><th></th><th>LSB In BMP</th><th>LSB in GIF</th><th>LSB In PNG</th></tr>
<tr><td>Percentage Distortion less resultant image</td><td>High</td><td>Medium</td><td>High</td></tr>
<tr><td>Invisibility</td><td>High</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Steganalysis detection</td><td>Low</td><td>Low</td><td>Low</td></tr>
<tr><td>Image manipulation</td><td>Low</td><td>Low</td><td>Low</td></tr>
<tr><td>Amount of embedded data</td><td>High</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Payload capacity</td><td>High</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Independent of file format</td><td>Low</td><td>Low</td><td>High</td></tr>
</table></td></tr>
<tr><td>5</td><td>Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan/2011</td><td>DWT
And
GAUSSIA-N SEQUEN-CE</td><td></td><td>PSNR=37.518
At K= 0.5
PSNR=25.477
At K= 2.0</td></tr>
<tr><td>6</td><td><b>W.</b> N. Cheung/2004</td><td>DCT</td><td> </td><td>PSNR= 32.8
AT B=10</td></tr>
</table>

CHAPTER 3

Proposed Method for Image Watermarking Using Secure Spread-Spectrum and Discrete Wavelet Transform

3.0 ABOUT TECHNIQUE

3.0.1 Spread Spectrum Watermarking in Wavelet Transform Domain

Wavelet-based watermarking has freshly extended its great attention due to its ability to provide first-rate multi resolution analysis, superior HVS modeling and space-frequency localization . DWT (Discrete Wavelet Transform) split up an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be reiterated to computes multiple “scale” wavelet decomposition. Dyadic frequency decomposition of wavelet transform bear a resemblance to the signal processing of the HVS and therefore allows adapting the distortion lead by either quantization or watermark embedding to the masking properties of human eye. The watermarks are inserted in different decomposition levels and subbands depending on locations and their type specified by a random key; thus, they can be autonomously embedded and retrieved, without any intervention among them. It is evident that the energy of an image is intense in the high decomposition levels corresponding to the perceptually significant low frequency coefficients; the low decomposition levels gather a minor energy proportion, thus being exposed to image alterations. Therefore, watermarks containing crucial information that require great robustness are embedded in higher subbands. Normally, vertical and horizontal subbands have more or less the same behavior and characteristics, in contrast to diagonal ones. Therefore, watermark embedding in the horizontal and vertical subbands promises increased robustness, since their energy compaction makes them less exposed to attacks. This proposed image watermarking scheme uses spread-spectrum technique in which, different watermark message is conceal in the same transform coefficients of the cover image by using uncorrelated codes, i.e. low cross correlation value (orthogonal/near orthogonal) among codes[17].

3.0.2 Spread-Spectrum Watermarking Principle

The watermark should not be placed in insignificant regions of the image or its spectrum, since many common signal and geometric processes affect these components. The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum while preserving fidelity. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise. This problem can be addressed by applying spread-spectrum watermarking which can be easily understood with spread-spectrum communications analogy in which frequency domain of the image is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are treated as noise that the immersed signal must be immune to. In spread-spectrum communications, one transmits a narrowband signal over a much larger bandwidth, such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into single output with high signal-to-noise ratio (SNR)[17]. However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures sufficiently small energy in any single coefficient. A watermark that is well placed in the frequency domain of an image will be practically impossible to see.

3.1 PROPOSED ALGORITHM

In this a new DWT based spread-spectrum watermarking algorithm using medical image cover is being implemented. Dyadic subband decomposition is performed on the image using Haar wavelet transform. The watermark used in the algorithm is in binary image form. A watermark message is hidden in the same transform coefficients of the cover image using uncorrelated codes, *i.e.* low cross correlation value (orthogonal/ near orthogonal) among codes. For each message bit, two different Pseudo Noise (PN) matrices namely of size identical to the size of the wavelet coefficient matrices, are generated. Since the security level of the watermarking algorithm depends on the strength of its secret key, a grey scale image of size 1 × 35 is used as a strong key for generating pseudorandom sequences [17]. Based on the value of the bit for the message vector, the respective two PN sequence matrices are then added to the corresponding second level HL and LH coefficients matrices respectively according to the data embedding rule as follows:

$$W = V + Kx \qquad \text{if } b = 0$$

Where V is wavelet coefficient of the cover image, W is the wavelet coefficient after watermark embedding, k is the gain factor, X is the PN matrix and b is the bit of watermark that has to be embedded. Generation of a pair of PN matrices for embedding each bit enhances the security of the watermarking algorithm. Following steps are applied in data embedding process.

3.1.1 Embedding Process

Read the host image I (M, N) of size M *N

1) Read the message to be hidden and convert it into binary sequences D_d (D_d = 1to n).

2) Transform the host image using “Haar” Wavelet transform and get second level sub-band coefficients ccA, ccH, ccV, ccD.

3) Generate n different PN-sequence pairs (PN_h and PN_v) each of size M /4 * N /4 using a secret key to reset the random number generator.

4) For D_d = 1 to n, add PN sequences to ccH and ccV components when message = 0

$$\text{ccH} = \text{ccH} + k*\text{PN\_h};$$
$$\text{ccV} = \text{ccV} + k*\text{PN\_v};$$

where, k is the gain factor used to specify the strength of the embedded data.

Apply inverse “Haar” Wavelet transform to get the final stego (watermarked) image I_w (M, N).

3.0.3.2 Extraction Process

To detect the watermark we generate the same pseudorandom matrices used during insertion of watermark by using same state key and determine its average correlation with the two detail sub-bands DWT coefficients. Average of *n* correlation coefficients corresponding to each PN matrices is obtained for both LH and HL sub-bands. Mean of the average correlation values are taken as threshold *T* for message extraction. During detection, if the average correlation exceeds *T* for a particular sequence a “0” is recovered; otherwise a “1”. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered[17]. For extracting the watermark, following steps are applied to the watermarked image:

1) Read the stego image I_w (M, N)

2) Transform the stego image using “Haar” Wavelet transform and get ccA1, ccH1, ccV1, ccD1 coefficients

3) Generate one’s sequences (*msg*) equal to message vector (from 1 to *n*)

4) Generate *n* different PN-sequence pairs (PN_h1 and PN_v1) each of size M/4 * N/4 using same secret key used in embedding to reset the random number generator

5) For *i* = 1 to *n*
Calculate the correlations store these values in *corr_H (i)* and *corr_V (i)*.

```
    corr_H(i)=correlation between
              PN_h1(i) and ccH1(i)
    corr_H(i)=correlation between
              PN_h1(i) and ccH1(i)
```

6) Calculate average correlation

$avg\_corr(i) = (corr\_H(i) + corr\_V(i)) / 2$

7) Calculate the

$corr(n)$ = mean of all the values stored in avg_*corr(i)*

8) Extract the hidden bit 0, using the relationship given below

For j=1 to n
if $avg\_corr(j) > corr(n)$, $msg(j) = 0$

9) Rearrange these extracted message.

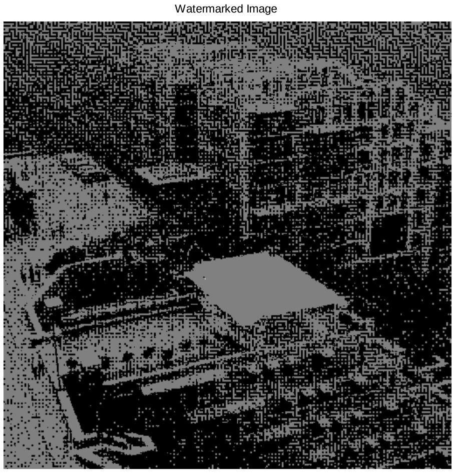
CHAPTER 4

EXPERIMENTS AND RESULTS

4.0 RESULTS

The performance of the proposed watermark algorithm was tested for image security applications. Experiments were carried-out using the cover image of size 512 × 512 available in reference. Information such as logo of an institute was embedded into host image as watermarks. This watermark is in binary image formats which add robustness by allowing recovery of the watermarks even at low correlation between original and extracted watermarks. Strength of watermarking is varied by varying the gain factor in the watermarking algorithm. Perceptual quality of the watermarked image is measured by calculating PSNR between host and watermarked image. At the receiver side, watermark is extracted from the watermarked image. Extracted watermark is evaluated by measuring its correlation with the original watermark. Figure 4.1 shows the cover image (a) watermark image (b) and watermarked image (c) with gain factor of 0.1 and the PSNR comes out to be 45.91 with similarity factor of 0.7029.

 Fig (a) cover image	 Fig (b) watermark image



Fig(c) watermarked image

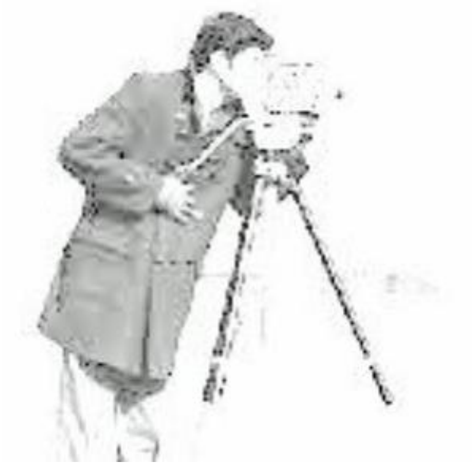


Fig (d) extracted watermark

Figure 4.1 cover image (a) watermark image (b) watermarked image (c) and extracted watermark (d) with gain factor 0.1

Table 2. Effect of gain factor

Gain Factor	**Watermark**	
	PSNR	**Similarity Factor**
0.1	45.91	0.7029
0.5	42.65	0.7588
1.5	38.03	0.81
3.0	31.02	0.88

It is observed from Table 2 that with the increase in the gain factor, PSNR of the watermarked image decreases and the degree of similarity between original and extracted watermark increases.

Table 3. Effect of subband levels (gain factor 0.1)

Levels	Watermark	
	PSNR	Similarity Factor
1	45.91	0.70
2	47.44	0.65
3	52.71	0.52

To show the effect of the decomposition levels, proposed algorithm with gain factor 0.1 was applied for embedding watermark in the horizontal and vertical subband coefficients of level 1, 2 and 3. It is observed from Table 2 that the PSNR value of the watermarked image increases and similarity factor between original and extracted watermark decreases with the increase in subband level for watermarking

4.1 Performance Analysis

Results of various attacks

Salt and pepper

Salt-and-pepper noise is a form of noise sometimes seen on images. It presents itself as sparsely occurring white and black pixels. An effective noise reduction method for this type of noise is a median filter or a morphological filter. For reducing either salt noise or pepper noise, but not both, a contra-harmonic mean filter can be effective. In this the embedded watermark is being exposed to salt and pepper noise with

J = imnoise (I ,'salt & pepper', D) where I is the watermarked image

adds "salt and pepper" noise to the image I, where D is the noise density. This affects approximately D * numel (I) pixels. Here D is 0.2.

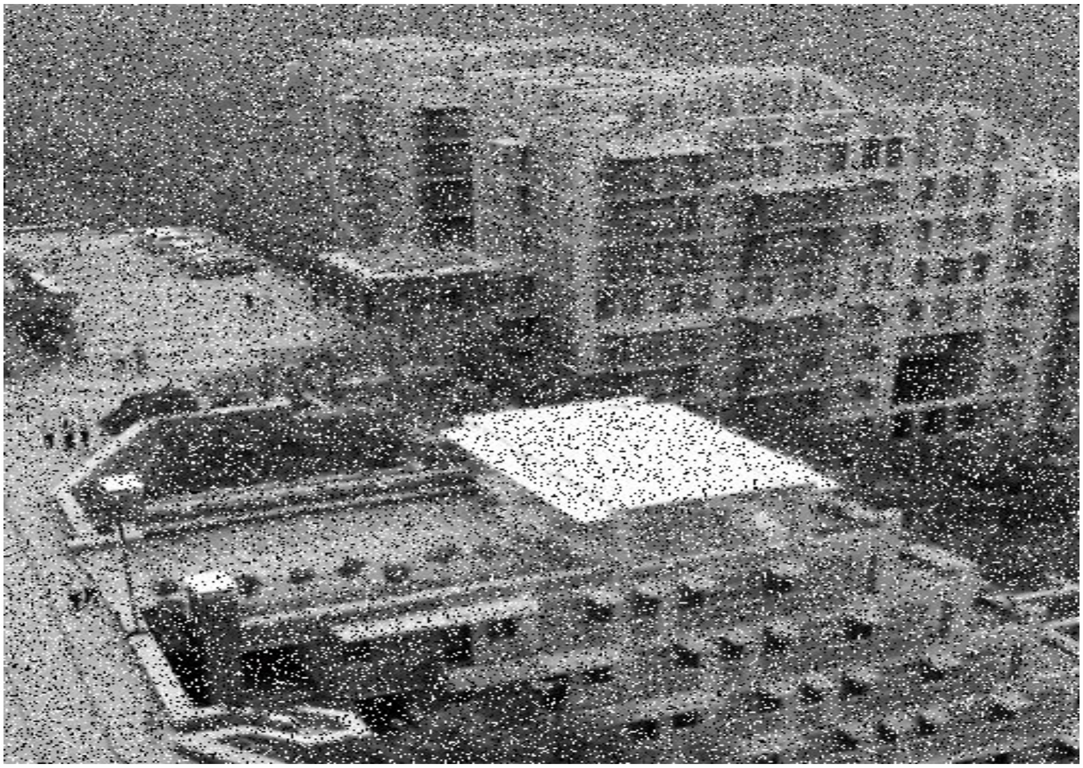


Figure 4.2 Effect of salt and pepper noise on watermarked image

Speckle Noise

Speckle is a granular 'noise' that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images.

Speckle noise in conventional radar results from random fluctuations in the return signal from an object that is no bigger than a single image-processing element. It increases the mean grey level of a local area.

Speckle noise in SAR is generally more serious, causing difficulties for image interpretation. It is caused by coherent processing of backscattered signals from multiple distributed targets. In SAR oceanography, for example, speckle noise is caused by signals from elementary scatterers, the gravity-capillary ripples, and manifests as a pedestal image, beneath the image of the sea waves. In figure 4.3 watermarked image ,I, is being exposed to noise where

J = imnoise(I,'speckle',V)

adds multiplicative noise to the image I, using the equation J = I + n*I, where n =3 is uniformly distributed random noise with mean 0 and variance V. The default for V is 0.04.

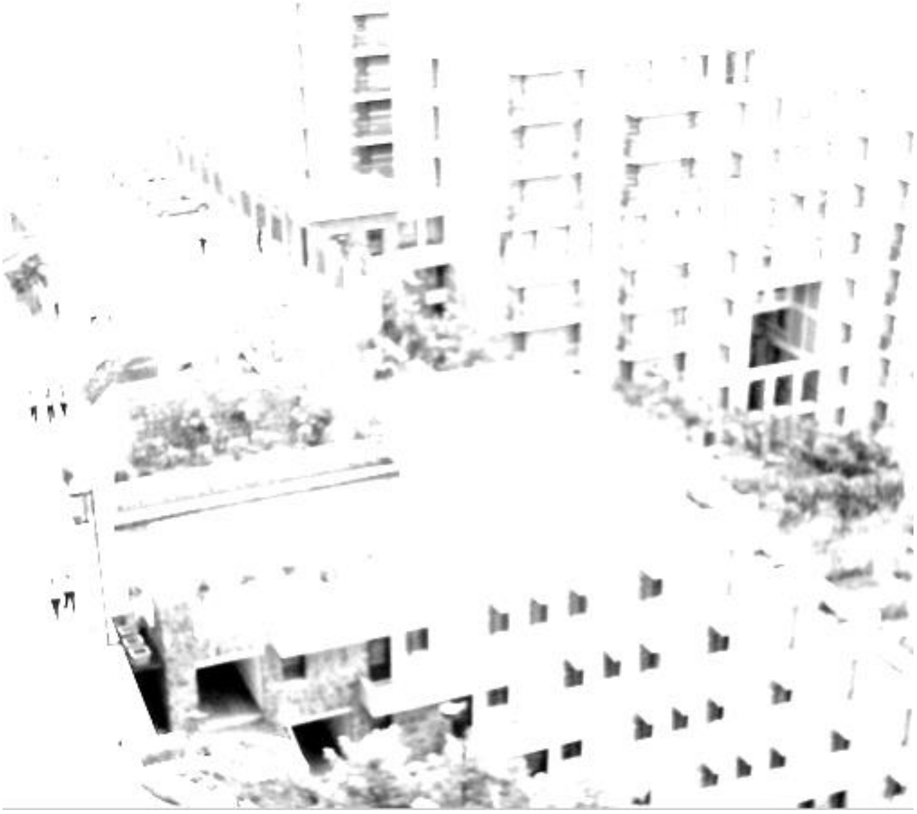


Figure 4.3 Effect of speckle noise on watermarked image with v=0.04

Cropping

Through such noise watermarked image is being resized depending upon the dimensions

Result

Figure 4.4 Effect of cropping on watermarked image with dimensions with X_{MIN}=160, X_{MAX}=40, Y_{MIN}=100, Y_{MAX}=90.

4.2 CONCLUSION

In this project ,watermarking technique is applied on an image using secure spread spectrum and discrete wavelet transform (DWT). Through secure spread spectrum technique more robustness is achieved as in this watermark is spread throughout the spectrum of an image which ensures a large measure of security against unintentional attack. Performance of the scheme is tested for the image by embedding message as watermark. Various types of attacks has been introduced to the watermarked image like salt and pepper noise, speckle noise and cropping to check the robustness of the technique. Furthermore, by changing the gain factor by different values the effect is calculated on the watermarked image. Through this proposed technique the problem of watermark security is solved to some extent.it is designed to be good at combating interference due to jamming, hiding a signal by transmitting it a low power and achieving secrecy. These properties make spread-spcetrum very popular in present-day digital watermarking.

In the near future, we will try to improve the various parameters like Robustness, fidelity, computational cost, imperceptibility, capacity of watermark, and security to greater level.

APPENDIX

Implementation Code

Embedding of watermark into the cover image

```
function X = DWTImageEmbed()

clear all;

k=0.5; %Gain Factor Specifying the strength of embedded data

file_name='img3.jpg'; %Cover Image

cover_image=imresize(im2double(rgb2gray(imread(file_name))),[512 512]);

I=cover_image;

figure(1);imshow(cover_image);title('Cover Image');

% determine size of watermarked image

Mc=size(cover_image,1); %Height

Nc=size(cover_image,2); %Width

file_name='download1.jpg';

message=imresize(im2double(rgb2gray(imread(file_name))),[40 80]);

figure(2);
```

```
imshow(message);

title('Watermark'); %Watermark (Message)

Mm=size(message,1); %Height

Nm=size(message,2); %Width

message_vector=round(reshape(message,Mm*Nm,1)./256); %Converting the message into a vector (sequence)

key=10; %Key to reset the PN Generator

rand('twister',key); %Setting the PN Generator

[LL,LH,HL,HH] = dwt2 (cover_image,'haar');

[cA1,cH1,cV1,cD1] = dwt2 (LL,'haar'); %Wavelet Transform

[cA2,cH2,cV2,cD2] = dwt2(cA1,'haar'); %Wavelet Transform

 % Adding PN Sequences to H1 and V1 components when message = 0

for (kk=1:length(message_vector))

 pn_h=round(2*(randn(Mc/4,Nc/4)-0.5)); %Generating PN Sequences using secret key

 pn_v=round(2*(randn(Mc/4,Nc/4)-0.5));

 if (message(kk) == 0) %Adding PN Sequences to H1 and V1 components when message = 0
 cH1=cH1+k*pn_h;

 cV1=cV1+k*pn_v;

 end

end

% IDWT

watermarked_image1 = idwt2(cA2,cH2,cV2,cD2,'haar',[Mc,Nc]); %Inverse “Haar” Wavelet transform

watermarked_image2 = idwt2(watermarked_image1,cH1,cV1,cD1,'haar',[Mc,Nc]); %Inverse “Haar” Wavelet transform

watermarked_image = idwt2(watermarked_image2,LH,HL,HH,'haar',[Mc,Nc]);

watermarked_image_uint8=uint8(watermarked_image);

imwrite(watermarked_image_uint8,'dwt_watermarked.jpg','jpg','quality',100); %Writing Watermarked Image

figure (3)
imshow (watermarked_image_uint8,[])

title ('Watermarked Image')

% ATTACKS

% Salt & Pepper Noise
```

```
%salt_img= imnoise (watermarked_image,'salt & pepper',0.2);

%figure(3)
%imshow(salt_img);title('Salt and Pepper Noise');

% Speckle Noise

 %V= 0.04

 %n=3

 %J = imnoise(I,'Speckle',V)

 %J=I+n*I

 %figure(5)

 %imshow(J);title('speckle');

% Poisson Noise

 %J = imnoise(I,'poisson')
 %figure(6)

 %imshow(J);title('poisson');

 % cropping

 I2=imcrop(watermarked_image,[160 40 100 90]);
 figure(7)
 imshow(I2);title('cropping');
```

Extraction of watermark from watermarked image

```
function X = DWT extract()
% DWT Watermark Extraction
clear all;
file_name='img3.jpg'; %Cover Image
cover_image = imresize(im2double(rgb2gray(imread(file_name))),[512 512]);
I=cover_image;
file_name='dwt_watermarked.jpg'; % Read the watermarked Image
watermarked_image= im2double(imread(file_name));
% Size of watermarked image
Mw=size(watermarked_image,1); %Height
Nw=size(watermarked_image,2); %Width
% Read Original Watermark
file_name='download1.jpg';
```

```
orig_watermark=imresize(im2double(rgb2gray(imread(file_name))),[40 80]);
w1=orig_watermark;
% Size of original watermark
Mo=size(orig_watermark,1); %Height
No=size(orig_watermark,2); %Width
 key=10; % Same Secret Key to reset the PN Generator
rand('twister',key);
message_vector=ones(1,Mo*No); %Generate one’s sequences (msg) equal to message vector
[LL,LH,HL,HH] = dwt2(watermarked_image,'haar');
[cA1,cH1,cV1,cD1] = dwt2(LL,'haar'); % Haar Wavelet Transform
% Adding PN Sequences to H1 and V1 components when message = 0
for (kk=1:length(message_vector))
 pn_h=round(2*(rand(Mw/4,Nw/4)-0.5)); %Generating PN Sequences using same secret key
 pn_v=round(2*(rand(Mw/4,Nw/4)-0.5));
 correlation_h(kk)=corr2(cH1,pn_h); %Correlation Calculation
 correlation_v(kk)=corr2(cV1,pn_v); %Correlation Calculation

 correlation(kk)=(correlation_h(kk)+correlation_v(kk))/2; %Average Correlation

 end
for (kk=1:length(message_vector))

 if (correlation(kk) > mean(correlation))

 message_vector(kk)=0;      %Extraction of hidden bit 0

 end

end

figure(2)

message=reshape(message_vector,Mo,No); %rearranging extracted message

W=message;

imshow(W,[])
title('Recovered Watermark')

%%SNR Calculation

z1=double(watermarked_image);

snr_num=0;

snr_den=0;
```

```
for  i=1:512

    for j=1:512

 snr_num=snr_num+(z1(i,j)*z1(i,j));

     snr_den=snr_den+((I(i,j)-z1(i,j))*(I(i,j)-z1(i,j)));

    end

end

snr=abs(10*(log10(snr_num/snr_den))) %SNR

%Similarity Factor (SF)Calculation

 sf_num=0;

sf_den=0;

a=0;

b=0;

for  i=1:Mo

    for j=1:No

        sf_num=sf_num+(w1(i,j)*W(i,j));
        a=a+(W(i,j)*W(i,j));

       b=b+(w1(i,j)*w1(i,j));

        sf_den=sqrt(sf_den+a*b);
   end

end

sf=(sf_num/sf_den) %Similarity Factor
```

REFERENCES

[1] Blossom Kaur, Jasdeep Singh, Amandeep Kaur,"Staganographic approach for hiding image in DCT domain," International Journal of Advances in Engineering & Technology, July 2011.

[2] Remya Elizabeth Philip, Sumithra M.G," Development of A new watermarking Algorithm For Telemedicine Applications," Vol. 3, Issue 1, pp.962-968 January -February 2013.

[3**]** Jagadish Nayak**,** P Subbanna Bhat**,** Rajendra Acharya **,** Niranjan UC, **"**Simultaneous storage of medical images in the spatial and frequency domain",biomedical enginerring , june 2004, doi:10.1186/1475-925X-3 17

[4] Pratibha Sharma, Shanti Swami," Digital Image Watermarking Using 3 level Discrete Wavelet Transform," Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013) .

[5] Mona M. Soliman1, Aboul Ella Hassanien1, Neveen I. Ghali2 and Hoda M. Onsi," An adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent," ijitcs vol,01/2011

[6] Baisa L. Gunjal ,"Strongly Robust and Highly Secured DWT-SVD Based Color Image Watermarking: Embedding Data in All Y, U, V Color Spaces," IJITCS Vol. 4, No. 3, April 2012.

[7] Ajay Goel, O.P.Sahu, Rupesh Gupta, Sheifali Gupta," Improved Digital Watermarking Techniques and Data Embedding In Multimedia," (IJCSE) International Journal on Computer Science and Engineering,Vol. 02, No. 02, 2010, 164-168

[8] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy," Implementation of LSB Steganography and its Evaluation for Various File Formats," Int. J. Advanced Networking and Applications Pages: 868-872 (2011)

[9] J. B. Feng, I. C. Lin, C. S. Tsai and Y. P. Chu, " Reversible Watermarking: Current and Key Issues," International Journal of Network Security, Vol. 2, No. 3, May 2006, pp. 161-170.

[10] S. Lee, C. D. Chang and T. Kalker, "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform," IEEE Transaction on Information Forensics and Security, Vol. 2, No. 3, September 2007, pp. 321-330. doi:10.1109/TIFS.2007.905146

[11] M. Terry, “Medical Identity Theft and Telemedicine Security,” Telemedicine and e-Health, Vol. 15, No. 10, December 2009, pp. 1-5.

[12] F. Cayre, C. Fontaine and T. Furon, “Watermarking Security: Theory and Practice,” IEEE Transactions on Signal Processing, Vol. 53, No. 10, October 2005, pp. 3976 - 3987. doi:10.1109/TSP.2005.855418

[13] L. P. Freire, P. Comesana, J. R. T. Pastoriza and F. P. Gonzalez, “Watermarking Security: A Survey,” LNCS Transactions on Data Hiding and Multimedia Security, 2006, pp. 41-72.

[14] I. J. Cox, J. Kilian, F. Thomson Leighton and Talal Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, Vol. 6, No. 12, 1997, pp. 1673-1687.

[15] Chao Cao, Ruoyu Wang, Minghu Huang, Rujun Chen,” A New Watermarking Method Based on DWT and Fresnel Diffraction Transforms,” Electrical and Computer Engineering,The University of Texas at Austin, TX 78713 Texal, USA

[16] Vinita Gupta, Mr. Atul Barve,” A Review on Image Watermarking and Its Techniques ,”M. Tech. Scholar, Department of CSE O.I. S.T, Bhopal (M.P.), India Volume 4, Issue 1, January 2014

[17] Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan,” Secure Spread Spectrum Watermarking for Telemedicine Applications,” April 2011. doi:10.4236

[18] Naderahmadian, Y Hosseini-Khayat, S., "Fast Watermarking Based on QR Decomposition in Wavelet Domain," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.127,130, 15-17 Oct. 2010.

[19] W. N. Cheung,” Digital Image watermarking in spatial And transform domain,” Electrical and Computer Engineering, The University of Texas at Austin, TX 78213 Texal, USA

[20] Hardikkumar V. Desai,” Steganography, Cryptography, Watermarking: A Comparative Study,” journal of global research in computer science Volume 3, No. 12, December 2012