CHAPTER-1

1.1ABSTRACT

In the current open society and with the growth of human rights, people are more and more concerned about the privacy of their information and other important data. This study makes use of electrocardiography (ECG) data in order to protect individual information. New technologies in multimedia and communication fields have introduced new ways to transfer and save the medical image data through open networks, which has introduced new risks of inappropriate use of medical information. Electrocardiograms as personal data are being applied more and more as a biometric and deserve to be protected. In this paper, a wavelet based steg-anography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data. Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems.. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, some distortion measurement metrics have been used: the Percentage Residual Difference (PRD) , the root mean square error(RMSE), peak to peak signal to niose ratio(PSNR) and correlation coeffiecient.It is found that the proposed technique provides high security protection for patients data with low distortion and ECG data remains diagnosable after watermarking (i.e. hiding patient confidential data) and as well as after watermarks (i.e. hidden data) are removed from the watermarked data.

1.2 PROBLEM STATEMENT

The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised. Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two sub-categories. Firstly, there are techniques that are based on encryption and cryptographic algorithms. These techniques are used to secure data during the communication and storage. As a result, the final data will be stored in encrypted format. The disadvantage of using encryption based techniques is its large computational overhead. Therefore, encryption based methods are not suitable in resource-constrained mobile environment. Other techniques are called steganography techniques; Steganography is the art of hiding secret information inside another type of data called host data .

1.3 LITERATURE SURVEY

- **V. Sankari and K. Nandhini**

Proposed a Steganography technique to secure patient confidential information using ECG signal.

ABSTRACT:

The number of aging population are growing significantly. In accordance with Health Insurance Portability and Accountability Act (HIPAA) the patient's privacy and security is important in the protection of healthcare privacy. Point-Of-care (PoC) is an application used in hospitals widely around the world. The Security Regulations are implemented to provide data integrity, confidentiality, and availability. Therefore, patients ECG signal and other physiological readings such as temperature, blood pressure, glucose reading, position, etc., are collected at homes by using Body Sensor Networks (BSNs) will be transmitted and diagnosed by remote patient monitoring systems. At the same cost that the patient confidentiality is protected against intruders while data traverse in open network and stored in hospital servers. In this project, to fulfill HIPAA act, a Discrete Wavelet Transform based steganography technique has been proposed. DWT technique allow ECG signal to put out of sight the patient confidential data and thus guarantees the patient's privacy and confidentiality. In addition the following mechanism were incorporated in this project: (1) encryption and decryption for data confidentiality and integrity (2) a three-tier security for data (3) ECG based Steganography to exchange data. A degree of high privacy is guaranteed for patient and simultaneously the Stego ECG remains diagnosable. Our scheme also ensures security, scalability, and efficiency.

- **N. Suganya , M.Marimuthu**

Proposed ECG Steganography Based Privacy Protecting Of Medical Data for Telemedicine Application.

ABSTRACT:

The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the ECG signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using chaos crypto system. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Here the discrete wavelet transformation is used to decompose an ECG signal to different frequency sub bands. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the high frequency coefficients. In the data extraction module, the secret data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

- **Ayman Ibaida and Ibrahim Khalil**

Proposed a Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems.

ABSTRACT:

With the growing number of aging population and a significant portion of that suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as point-of-care (PoC) applications in hospitals around the world. Therefore, huge amount of ECG signal collected by body sensor networks from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level, etc., and diagnosed by those remote patient monitoring systems. It is utterly important that patient confidentiality is protected while data are being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this paper, a wavelet-based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the proposed technique provides high-security protection for patients data with low (less than 1%) distortion and ECG data remain diagnosable after watermarking (i.e., hiding patient confidential data) and as well as after watermarks (i.e., hidden data) are removed from the watermarked data.

- **Mekala.R , Vanitha .S**

PROPOSED A PRIVACY PROTECTION OF MEDICAL DATAS USING ECG STEGANOGRAPHY.

ABSTRACT:

In wireless networks, the bio-medical data may be vulnerable to attacks like tampering, hacking etc.This paper proposes wavelet based steganography technique which is used to provide more security which combines encryption and concealing technique to protect patient confidential data while transmitted over the public network. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics such as Percentage RMSE Difference (PRD) and the other error performance metrics such as PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

- **Ms. Pawar Kshetramala Dilip, Prof. V. B. Raskar**

Proposed Hiding Patient Confidential Information in ECG Signal Using DWT Technique.

ABSTRACT:

The patient's confidential data should be safe and secure these is Act by Health Insurance Portability and Accountability Act (HIPAA). At the same time, there is a significantly growth in population. Numbers of patient care centers are used usually around the world in a Point - Of - care (PoC) applications. The Security systems are implemented to provide data integrity, privacy, and accessibility. Therefore, ECG signal of the patients and other physiological data of the patient’s like body temperature, glucose level, blood pressure, position, etc., are collected by Body Sensor Networks (BSNs) at home. After that it will transmitted over network and then stored at hospital server. In this paper, it used the steganography method which is depending on discrete wavelet transform to accomplish HIPAA act. DWT technique is applied on the ECG signal to hide confidential information of the patient which provides privacy to confidential information. High degree privacy is provided to patient, also Stego ECG remains diagnosable. In this paper the steganography technique is used to provide the three tire securities to patient’s data. Our system also ensures safety, scalability, and effectiveness.

- **Anish Singh Shekhawat ,Arnav Jain and Dipti Patil.**

Proposed A Study of ECG Steganography for Securing Patient's Confidential Data based on Wavelet Transformation.

ABSTRACT:

The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised. This paper discusses various data encryption techniques along with data embedding using signal transformation to ensure that the sanctity of the information.

- **Treesa Joseph, Remya U L**

Porposed An ECG Steganography based privacy protection of medical datas for telemedicine application

ABSTRACT:

Over 20 million people worldwide have abnormal electrocardiogram (ECG) signals, i.e., arrhythmias, each year. Most of the cardiac patients are elders.And if they increasingly move to nursing homes, it is a necessary tendency to reduce the medical labor cost by deploying self-organized wireless cardiac-monitoring hardware/ software systems in an area with a radius of hundreds of feet. Such medical information networks could allow the doctors to immediately capture the arrhythmia events of any patient without leaving their offices. In this paper, a wavelet based steganography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data.Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems. An added benefit is the freedom of movement for patients due to the wireless networking technologies. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics, the Percentage Residual Difference (PRD) has been used.

CHAPTER-2

2.1 INTRODUCTION TO AN ECG STEGANOGRAPHY

An Electrocardiogram (ECG) analysis is an important tool in the management of cardiac diseases. A security technique with ECG is proposed to guarantee secure transmission of patient confidential information combined with patient physiological readings from body sensors.The proposed technique is a hybrid between the two preceding categories. Firstly, it is based on using steganography techniques to hide patient confidential information inside patient biomedical signal. Moreover, the proposed technique uses encryption based model to allow only the authorized persons to extract the hidden data. The Electrocardiogram (ECG)signal is used here due to the fact that most of the health care systems will collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information. The steganography technique will be applied and patient secret information and physiologicalreadings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is sent to the hospital server via the Internet.

As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other reading sstored in the host ECG signal. The proposed steganography technique will provide the highest security that can be achieved [7]. The use of this technique will slightly affect the quality of ECG signal and also quality can be improved more than existing system. . This paper proposes the use of digital watermarking to increase the security of an ECG signal transmitted through a wireless network. The characteristic of the proposed watermarking scheme is that the blind recovery of the watermark is possible at the receiver and the embedded watermark can be fully removed. Hence, ECG can be viewed by a clinician with zero distortion which is an essential requirement for bio-medical data. Further, tampering such as noise addition and filtering attack can also be detected at the receiver.

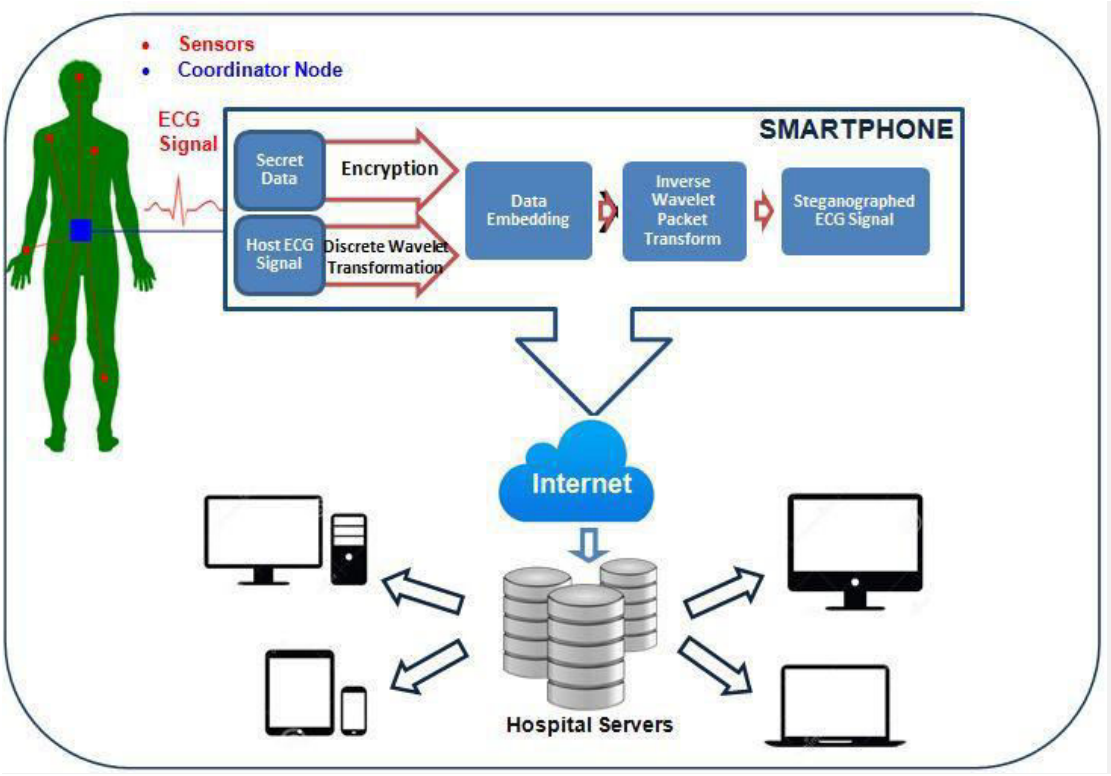


Figure 2.1: Architecture for ECG steganography and transmission of steganographed ECG signal

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryptionis illegal. Thus, where as cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

2.2 ELECTROCARDIOGRAPHY(ECG)

Electrocardiography (ECG or EKG from Greek: kardia, meaning heart) is the process of recording the electrical activity of the heart over a period of time using electrodes placed on a patient's body. These electrodes detect the tiny electrical changes on the skin that arise from the heart muscle depolarizing during each heartbeat.

In a conventional 12 lead ECG, ten electrodes are placed on the patient's limbs and on the surface of the chest. The overall magnitude of the heart's electrical potential is then measured from twelve different angles ("leads") and is recorded over a period of time (usually 10 seconds). In this way, the overall magnitude and direction of the heart's electrical depolarization is captured at each moment throughout the cardiac cycle. The graph of voltage versus time produce by this non invasive medical procedure is referred to as an electrocardiogram (abbreviated ECG or EKG).

During each heartbeat, a healthy heart will have an orderly progression of depolarization that starts with pacemaker cells in the sinoatrial node, spreads out through the atrium, passes through the atrioventricular node down into the Bundle of His and into the Purkinje fibers spreading down and to the left throughout the ventricles. This orderly pattern of depolarization gives rise to the characteristic ECG tracing. To the trained clinician, an ECG conveys a large amount of information about the structure of the heart and the function of its electrical conduction system. Among other things, an ECG can be used to measure the rate and rhythm of heartbeats, the size and position of the heart chambers, the presence of any damage to the heart's muscle cells or conduction system, the effects of cardiac drugs, and the function of implanted pacemakers.

An ECG is used to recording of the heart’s electrical activity. The deviations in the normal electrical patterns indicate various cardiac disorders. Cardiac cells, in the normal state are electrically polarized. Their inner sides are negatively charged relative to their outer sides. These cardiac cells can lose their normal negativity in a process called depolarization , which is the fundamental electrical activity of the heart. The ECG records the electrical activity of the heart, where each heart beat is displayed as a series of electrical waves characterized by peaks and valleys. Normally, the frequency range of an ECG signal is of 0.05 – 100 Hz and it’s dynamic range – of 1 – 10 mV. The ECG signal is characterized by five peaks and valleys labeled by the letters P, Q, R, S, T. In the normal sinus rhythm (normal state of the heart) the P-R interval is in the range of 0.12 to 0.2 seconds. The QRS interval is from 0.04 to 0.12 seconds .The Q-T interval is less than 0.42 seconds and the normal rate of the heart is from 60 to 100 beats per minute. So, from the recorded

shape ofthe ECG, we can say whether the heart activity is normal or abnormal. The normal value of heart beat lies in the range of 60 to 100 beats /minute .

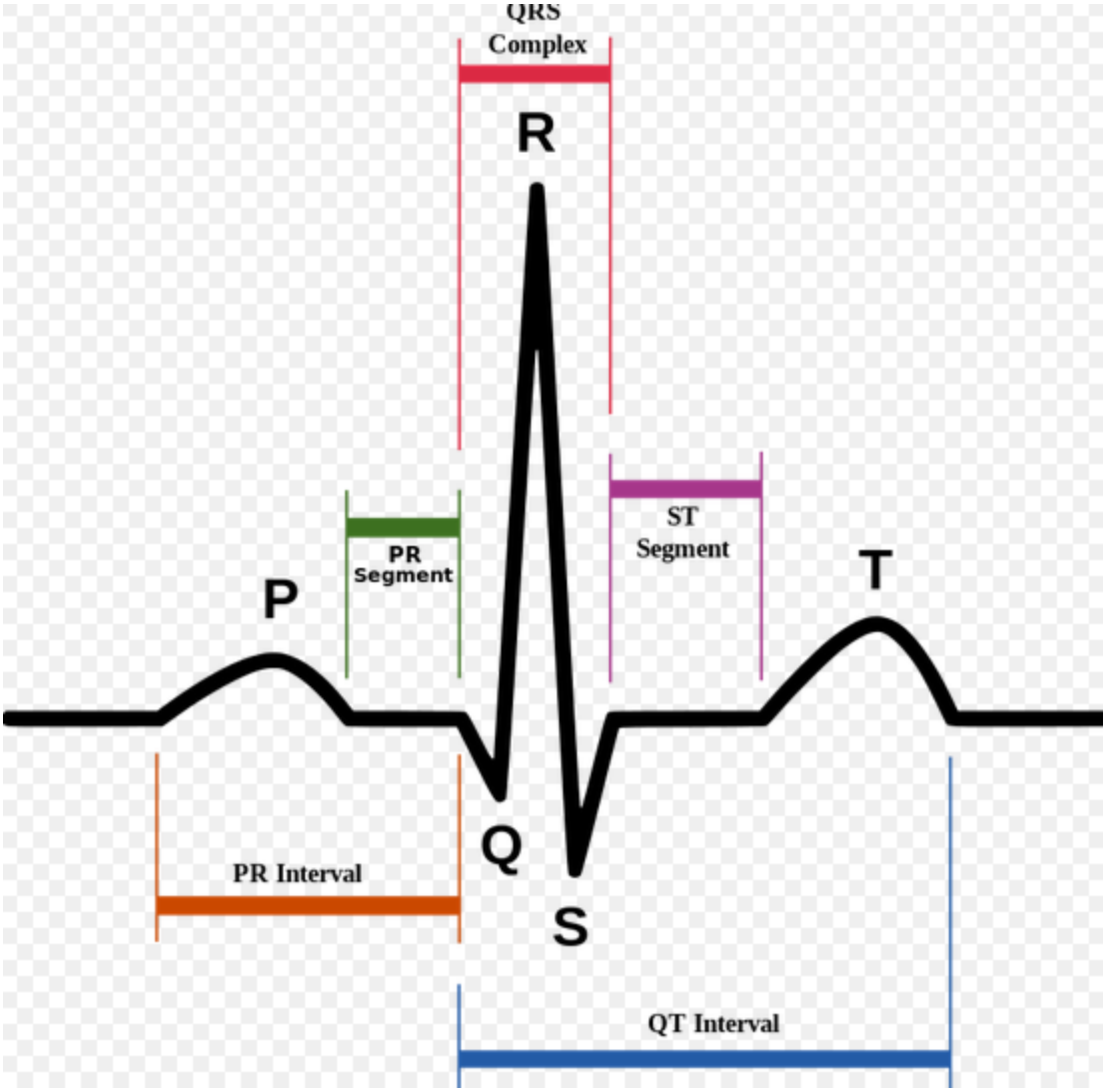


Figure 2.2:The normal ECG waveform

❖ Axis

The heart's electrical axis is the general direction of the ventricular depolarization wavefront (or mean electrical vector) in the sagittal plane (the plane of the limb leads and augmented limb leads). The QRS axis can be determined by looking for the limb lead or augmented limb lead with the greatest positive amplitude of its R wave. A lead can only detect changes in voltage that are aligned with that lead; therefore the lead that is best aligned with the axis of ventricular depolarization will have the tallest positive QRS complex. The normal QRS axis is generally down

and to the left, following the anatomical orientation of the heart within the chest. An abnormal axis suggests a change in the physical shape and orientation of the heart, or a defect in its conduction system that causes the ventricles to depolarize in an abnormal way.

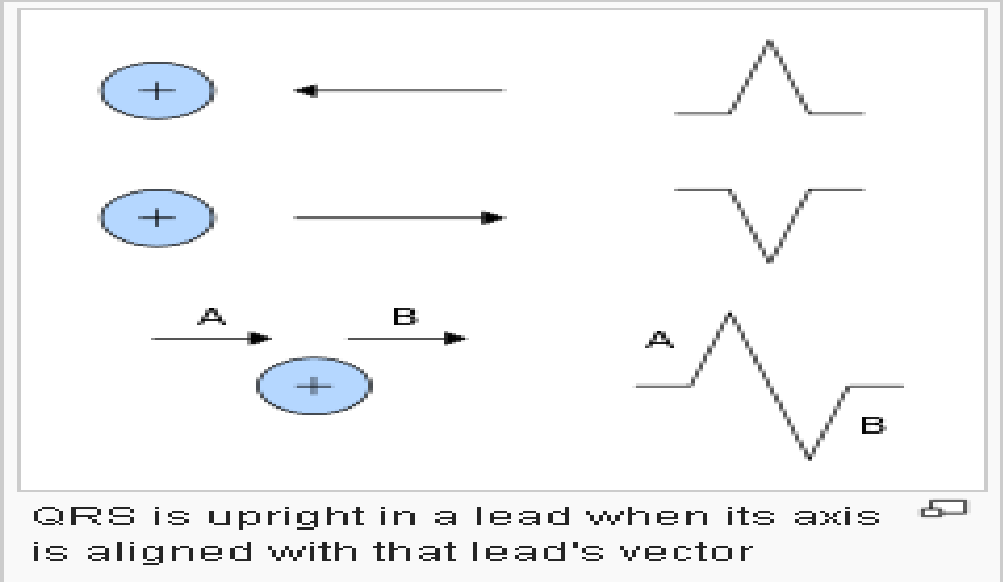


Figure 2.3:QRS

❖ P wave

The p-wave represents depolarization of the atria. Atrial depolarization spreads from the SA node towards the AV node, and from the right atrium to the left atrium.

The p-wave is typically upright in most leads except for aVR; an unusual p-wave axis (inverted in other leads) can indicate an ectopic atrial pacemaker. If the p wave is of unusually long duration, it may represent atrial enlargement. Typically a large right atrium gives a tall, peaked p-wave while a large left atrium gives a two-humped bifid p-wave.

Duration:-<80 ms

❖ PR interval

The PR interval is measured from the beginning of the P wave to the beginning of the QRS complex. This interval reflects the time the electrical impulse takes to travel from the sinus node through the AV node.

A PR interval shorter than 120 ms suggests that the electrical impulse is bypassing the AV node, as in Wolf-Parkinson-White syndrome. A PR interval consistently longer than 200 ms diagnoses first degree atrioventricular block. The PR segment (the portion of the tracing after the p-wave and before the QRS complex) is typically completely flat, but may be depressed in pericarditis. Duration:- 120 to 200 ms

The QRS complex represents the rapid depolarization of the right and left ventricles. The ventricles have a large muscle mass compared to the atria, so the QRS complex usually has a much larger amplitude than the P-wave.

❖ QRS complex

If the QRS complex is wide (longer than 120 ms) it suggests disruption of the heart's conduction system, such as in LBBB, RBBB, or ventricular rhythms such asventricular tachycardia. Metabolic issues such as severe hyper kalemia, or TCA overdose can also widen the QRS complex. An unusually tall QRS complex may represent left ventricular hypertrophy while a very low-amplitude QRS complex may represent apericardial effusion orinfiltrative myocardial disease. Duration:- 80 to 100 ms

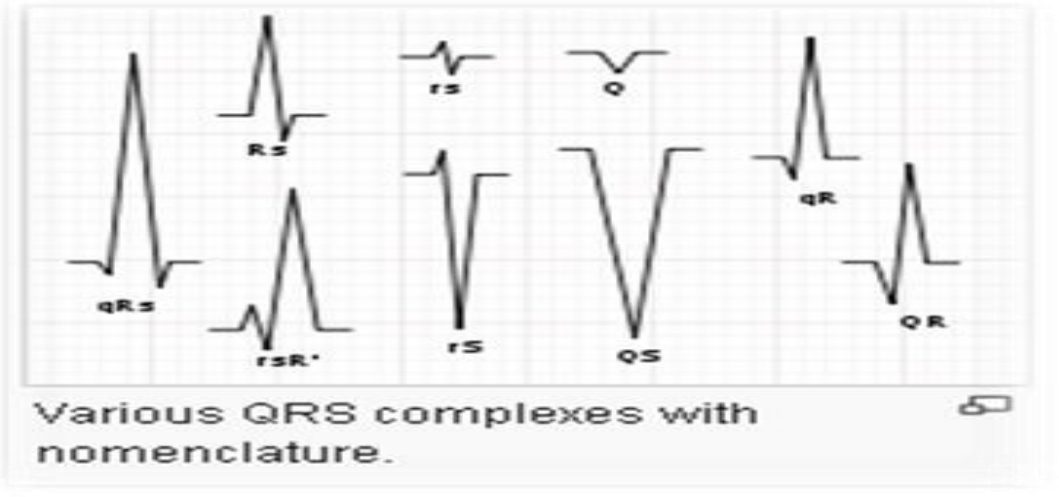


Figure 2.4: various QRS complexes with nomenclature

❖ ST segment

The ST segment connects the QRS complex and the T wave; it represents the period when the ventricles are depolarized.

It is usually isoelectric, but may be depressed or elevated with myocardial infarction or ischemia. ST depression can also be caused by LVH or digoxin.ST elevation can also be caused by pericarditis,Brugada syndrome, or can be a normal variant (J-point elevation).

❖ T wave

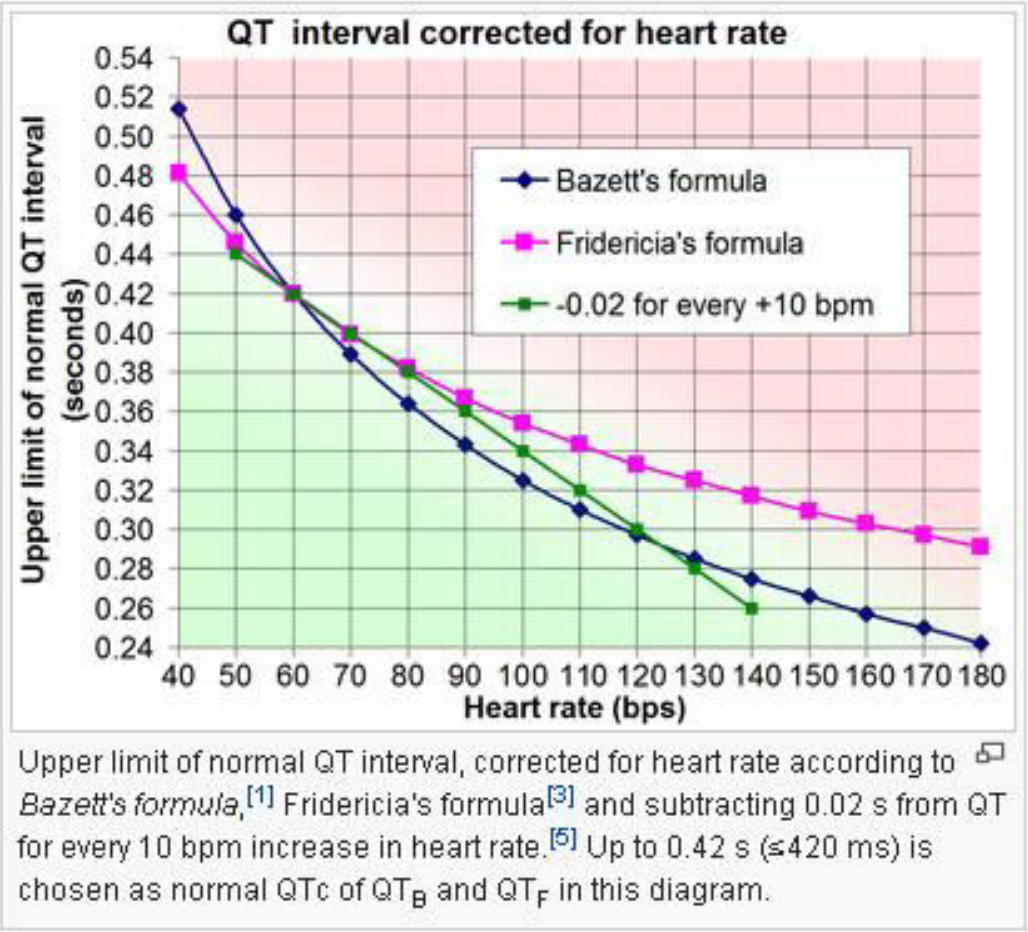
The T wave represents the repolarization of the ventricles. It is generally upright in all leads except aVR and lead V1. Inverted T waves can be a sign of myocardial ischemia,LVH, high intracranial pressure, or metabolic abnormalities. Peaked T waves can be a sign ofhyperkalemia or very earlymyocardial infarction. Duration:- 160 ms.

	Age (ethnicity)	n	V1	V2	V3	V4	V5	V6
Children								
	1 week - 1 y	210	92%	74%	27%	20%	0.5%	0%
	1 y - 2 y	154	96%	85%	39%	10%	0.7%	0%
	2 y - 5 y	202	98%	50%	22%	7%	1%	0%
	5 y - 8 y	94	91%	25%	14%	5%	1%	1%
	8 y - 16 y	90	62%	7%	2%	0%	0%	0%
Males								
	12 y - 13 y	209	47%	7%	0%	0%	0%	0%
	13 y - 14 y	260	35%	4.6%	0.8%	0%	0%	0%
	16 y - 19 y (whites)	50	32%	0%	0%	0%	0%	0%
	16 y - 19 y (blacks)	310	46%	7%	2.9%	1.3%	0%	0%
	20 - 30 y (whites)	285	41%	0%	0%	0%	0%	0%
	20 - 30 y (blacks)	295	37%	0%	0%	0%	0%	0%
Females								
	12 y - 13 y	174	69%	11%	1.2%	0%	0%	0%
	13 y - 14 y	154	52%	8.4%	1.4%	0%	0%	0%
	16 y - 19 y (whites)	50	66%	0%	0%	0%	0%	0%
	16 - 19 y (blacks)	310	73%	9%	1.3%	0.6%	0%	0%
	20 - 30 y (whites)	280	55%	0%	0%	0%	0%	0%
	20 - 30 y (blacks)	330	55%	2.4%	1%	0%	0%	0%

Table2.1 Frequency of inverted T-waves in precordial leads (lead V1 to V6) according to gender and age.

❖ Corrected QT interval

The QT interval is measured from the beginning of the QRS complex to the end of the T wave. Acceptable ranges vary with heart rate, so it must becorrected by dividing by the square root of the RR interval. A prolonged QTc interval is a risk factor for ventricular tachyarrhythmias and sudden death. Long QT can arise as a genetic syndrome, or as a side effect of certain medications. An unusually short QTc can be seen in severe hypercalcemia. Duration:-<440 ms



Upper limit of normal QT interval, corrected for heart rate according to *Bazett's formula*,[1] Fridericia's formula[3] and subtracting 0.02 s from QT for every 10 bpm increase in heart rate.[5] Up to 0.42 s (≤420 ms) is chosen as normal QTc of QT_B and QT_F in this diagram.

Figure 2.5: Corrected QT interval

❖ U wave

The U wave is hypothesized to be caused by the repolarization of the interventricular septum. It normally has a low amplitude, and even more often is completely absent.

Prominent U waves are most often seen in hypokalemia, but may be present inhypercalcemia, thyrotoxicosis, or exposure to digitalis, epinephrine, and Class 1A and 3 antiarrhythmics, as well as in congenital long QT syndrome, and in the setting of intracranial hemorrhage. An inverted U wave may represent myocardial ischemia (and especially appears to have a high positive predictive accuracy for left anterior descending coronary artery disease) or left ventricular volume overload. A U-wave can sometimes be seen in normal younger, athletic individuals.

2.3 STEGANOGRAPHY PRIMITIVES

Steganography is the art of hiding information in ways that prevent the detection of hidden messages". Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable.

➢ Steganography in history:

Steganography comes from Greek and means "covered writing." The ancient Greeks wrote text on wax-covered tablets. To pass a hidden message, a person would scrape off the wax and write the message on the underlying wood. He/she would then once again cover the wood with wax so it appeared unused.

➢ Steganography in digital image:

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images ,videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embeddingasecret message into the cover-image, a so-called stego-image is obtained.

- **Steganography in telemedicine :**

Telemedicine can be beneficial to patients living in isolated communities and remote regions, who can receive care from doctors or specialists far away without the patient having to travel to visit them. Recent developments in mobile collaboration technology can allow healthcare professionals in multiple locations to share information and discuss patient issuesas ifthey were in the same place. Remote patient monitoring through mobile technology can reduce the need for outpatient visits and enable remote prescription verification and drug administration oversight, potentially significantly reducing the overall cost of medical care . Telemedicine can also facilitate medical education by allowing workers to observe experts in their fields and share best practices more easily.

2.4 A wireless PDA-based physiological monitoring system for patient transport

A wirelesss PDA-based monitor is used to acquire continuously the patient's vital signs, including heart rate, three-lead electrocardiography, and SpO2. Through the WLAN, the patient's biosignals can be transmitted in real-time to a remote central management unit, and authorized medical staffs can access the data and the case history of the patient, either by the central management unit or the wireless devices. A prototype of this system has been developed and implemented. The system has been evaluated by technical verification, clinical test, and user survey. The evaluation of performance yields a high degree of satisfaction (mean=4.64, standard deviation-SD=0.53 in a five-point Likert scale) of users who used the PDA-based system for intrahospital transport. The results also show that the wireless PDA model is superior to the currently used monitors both in mobility and in usability, and is, therefore, better suited to patient transport.

2.4.1 Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign

Recently, a remote-sensing platform based on wireless interconnection of tiny ECG sensors called telecardiology sensor networks (TSN) provided a promising approach to perform low-cost real-time cardiac patient monitoring at any time in community areas (such as elder nursing homes or hospitals). The contribution of this research is the design of a practical TSN hardware/software platform for a typical U.S. healthcare community scenario (such as large nursing homes with many elder patients) to perform real-time healthcare data collections. On the other hand, due to the radio broadcasting nature of MANET, a TSN has the risk of losing the privacy of patients' data. Medical privacy has been highly emphasized by U.S. Department of Health and Human Services. This research also designs a medical security scheme with low communication overhead to achieve confidential electrocardiogram data transmission in wireless medium.

2.4.2 Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA) :

In Wireless telecardiology applications ECG signal is compressed before transmission to support faster data delivery and reduce consumption of bandwidth. However, most of the ECG analysis and diagnosis algorithms are based on processing of the original ECG signal. Therefore, compressed ECG data needs to be decompressed first before the existing algorithms and tools can be applied to detect cardiovascular abnormalities. Decompression will cause delay on the doctor's mobile device and in wireless nodes that have the responsibilities to detect and prioritize abnormal data for faster processing. This is undesirable in body sensor networks (BSNs) as high processing involved in decompression will waste valuable energy in the resource and power constrained sensor nodes. In order to diagnose cardiac abnormality such as Ventricular tachycardia, we applied a novel system to analyse and classify compressed ECG signal by using a PCA for feature extraction and k-mean for clustering of normal and abnormal ECG signals.

2.4.3 A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations are two crucial provisions in the protection of healthcare privacy. Privacy regulations create a principle to assure that patients have more control over their health information and set limits on the use and disclosure of health information. The security regulations stipulate the provisions implemented to guard data integrity, confidentiality, and availability. Undoubtedly, the cryptographic mechanisms are well defined to provide suitable solutions. To comply with the HIPAA regulations, a flexible cryptographic key management solution is proposed to facilitate interoperations among the applied cryptographic mechanisms. In addition, case of consent exceptions intended to facilitate emergency applications and other possible exceptions can also be handled easily.

2.5 Survey on recent digital image steganography techniques

Steganography is the science of hiding information that involves all the techniques used to exchange the secret message with low distortion of the cover medium. Many different cover medium formats such as (image, audio, video, and text) can be used to hide the secret message. Image files are mostly used because of their frequency on the Internet. Some of the old techniques used schemes to hide information are: invisible ink, null ciphers, micro-codes, and pink-pricks. Modern Steganography has gained a lot of attention for the last two decades because of the rapid growth of communication technologies such as Internet and the need of a secure channel to transmit the important information.

2.6 A High Capacity Reversible Multiple Watermarking Scheme - Applications to Images, Medical Data, and Biometrics

Modern technologies have eased the way for intruders and adversaries to bypass the conventional identity authentication and identification processes; hence security systems have been developed to a great extent for protection of privacy and security of identities in different applications. The focus of this thesis is digital watermarking as a part of Digital Rights Management (DRM), security and privacy, as well as the ability to employ electrocardiogram (ECG) as a method to enhance the security and privacy level. The contribution of this work consists of two main parts:

An application-specific high capacity reversible multiple watermarking scheme is introduced in the first part to mainly target the medical images. The proposed data hiding method is designed such that the embedding of sensitive personal information in a generic image without any loss of either the embedded or the host information is possible. Furthermore, in the second part, the use of ECG biometric signals in the form of the embedded watermark is studied. Proposed framework allows embedding of ECG features into the host image while retaining the quality of the image, the performance of the security system and the privacy of the identity. Experimental results indicate that the reversible data hiding scheme outperforms other approaches in the literature in terms of payload capacity and marked image quality. Results from the ECG mark embedding also show that no major degradation in performance is noticeable compared to the case where no watermarking is needed.

2.7 CRYPTOGRAPHY BASED METHODS

Cryptography is the art and science of achieving security by encoding messages to make them readable. The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of wireless communication, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the wireless. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. Personal Health Record is web based application that allows people to access and co-ordinate their lifelong health information. The patient have control over access to their own PHR. To achieve security of personal health records we use the attribute based encryption to encrypt the data before outsourcing it. Here we focus on multiple types of PHR owner scenario and division of personal health records users into multiple security domains which reduce key management complexity for owners and users. A high degree of patient's privacy is guaranteed. Our scheme gives personal health record owner full control of his/her data. Extensive security and performance analysis shows that the proposed scheme is highly efficient.

Personal Health Record (PHR) concept has emerged in recent years. We can say that it is a patient centric model as overall control of patient‟s data is with patient. He can create, delete, modify and share his PHR through the web. Due to the high cost of building and maintaining data centers, third-party service providers provide PHR service. But while using third party service providers there are many security and privacy risks for PHR. The main concern is whether the PHR owner actually gets full control of his data or not, especially when it is stored at third party servers which is not fully trusted. To ensure patient-centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. Our approach is to encrypt the data before outsourcing. PHR owner will decide which users will get access to which data in his PHR record. A PHR file should available to only those users who are given corresponding decryption key. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The authorized users may either need to access the PHR for personal use or professional purposes. We divide types of users into two domains, personal domain and public domain. To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using ABE, access policies are expressed based on attributes of users or data.

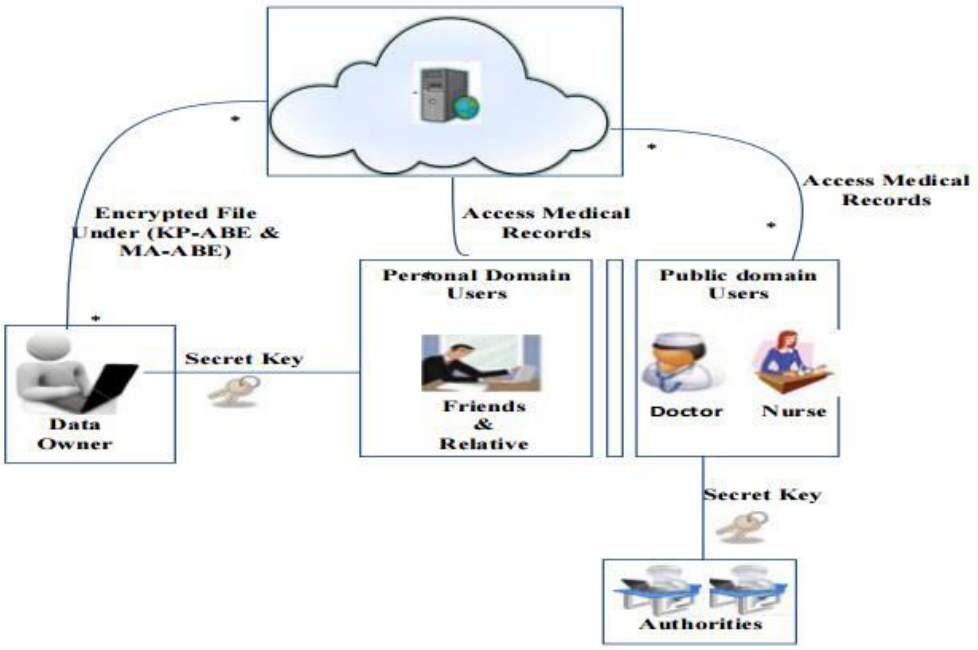


Figure 2.6: Architecture of Patient Medical Record Sharing

➢ Advantage of the propsed system :

1. Quickly find out information of patient details.

2. In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.

3. If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.

4. To provide easy and faster access information.

5.To provide user friendly environment

6. To provide data confidentiality and write access control.

➢ APPLICATION :

Any organization can use this application to store their employees‟ medical information.

➢ Some of the concepts used in cryptography are described here :

- Plain Text: Any communication in the language that
- we speak- that is the human language, takes the form of plain text. It is understood by the sender, therecipient and also by anyone who gets an access to that message.
- Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.
- Encryption: The process of encoding plain text messages into cipher text messages is called encryption.
- Decryption: The reverse process of transforming cipher text messages back to plain text is called as decryption.
- Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

- **Purposes of Cryptography**

Cryptography serves following purposes*:*

- Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.
- Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.
- Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.
- Non- repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.
- Access Control: Access Control specifies and controls who can access what.
- Availability: The principle of availability states that resources should be available to authorized parties all the times.

- **Types of Cryptography :**

Two types of cryptography are studied*:*

• Symmetric Key Cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography.

• Asymmetric Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography

1.7.1 PUBLIC KEY ENCRYPTION :

Public key Encryption (PKE) based scheme is one of the encryption method used for protecting data from third parties. But it has high key management overhead, or requires encrypting multiple copies of a file using different user's keys. Attribute based encryption is based on some access policies. These access policies are expressed based on the attribute of users or data which help to share PHR among set of users by encrypting the file under a set of attributes. Only authorized users with satisfying this access policy can access the PHR data. The main property of ABE is preventing against user collusion and the owner is not required to know the ACL.

- **Encryption scheme:-**

In this scheme plain text is converting into cipher text using public key. Then sender gives the cipher text for you and using your private key you can decrypt it. It is simple but main disadvantage of this scheme are uses up more computer resources, if an attacker determines a person private key, his or her entire messages can be read and the loss of a private key means that all received messages cannot be decrypted. The main steps used for this encryption is shown in Fig (2.7).

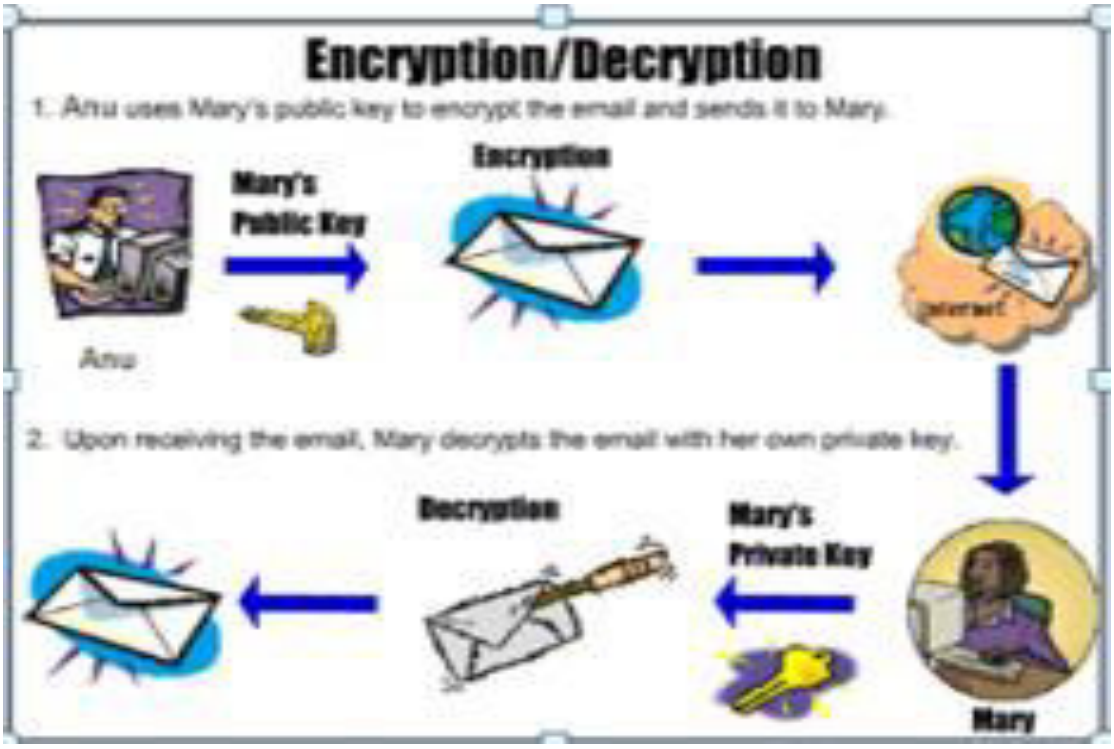


Figure 2.7: Public Key Encryption/Decryption

❖ Identity Based Encryption (IDE)

IBE sender can encrypt a message using only identity without need of public key certificate. Common feature of IBE is that they view identities as a string of characters. In IBE [7], ones publicly known identity (ex. email address) is being used as his/her public key where as corresponding private key is generated from the known identity. IBE [7] encryption scheme is a four algorithms/steps scheme where the algorithms are:

(1) Setup Algorithm .

(2) Key(private key)Generation Algorithm

. (3) Encryption Algorithm.

(4) Decryption Algorithm.

In Fuzzy identity based encryption view identities as a set of descriptive attributes. So in this scheme the error problems related to identities in IBE is solved.

1) Identity based encryption system that uses biometric identities.eg: iris scan.
2) It is used in Attribute based encryption

Attribute Based Encryption (ABE) Sahai and Waters [8] first introduced the attribute based encryption (ABE) for enforced access control [5] through public key cryptography. The main aspects are to provide flexibility, scalability and fine grained access control. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. Suppose the Attribute sets are Computer Science, Male and age 40.Tree access structure for this is shown in Fig (2.8).

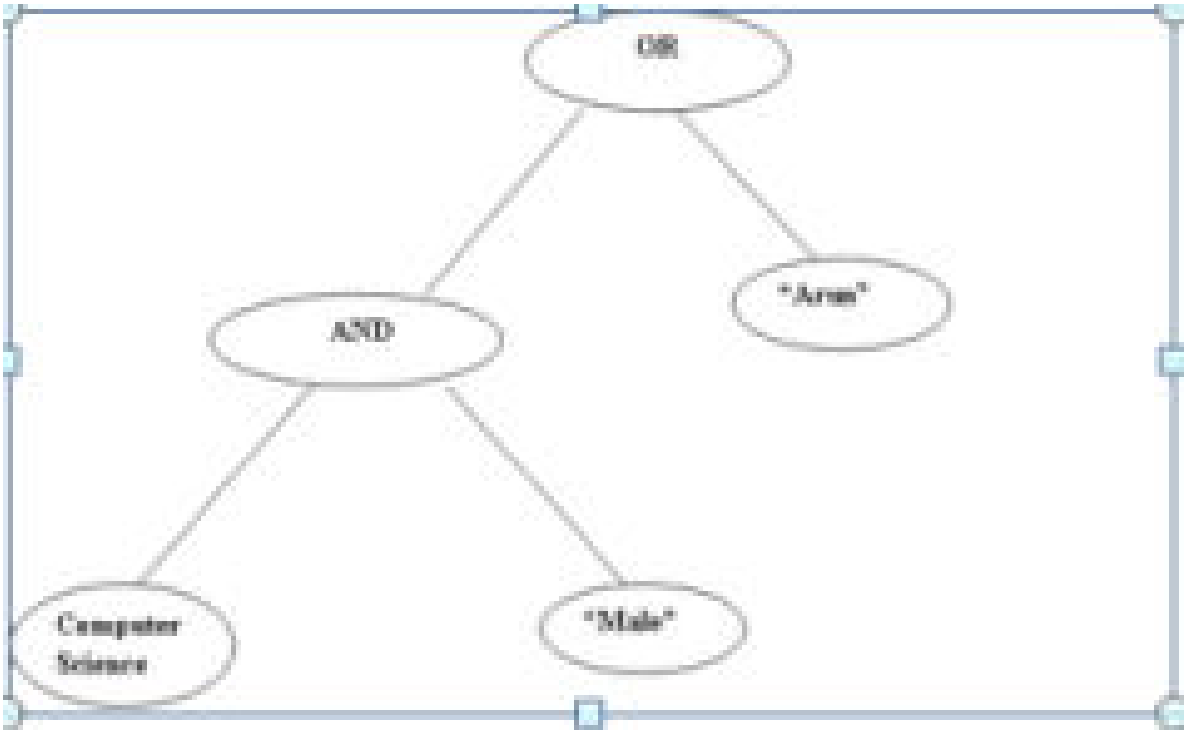


Figure 2.8:Tree acess structure

interior node consists of AND and OR gates and leaves consists of different attributes. Attribute sets that satisfy the tree can reconstruct the secret message and access it. In classical model, this can be achieved only when user and server are in a trusted domain. So different alternatives of ABE are introduced.

❖ Key Policy Attribute Based Encryption (KP-ABE)

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters [8] proposed a key- policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. In KP-ABE, a set of attributes is associated with cipher text and the users decryption key is associated with a monotonic access tree structure . When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text. Limitations of KP-ABE are Encryptor cannot decide who can decrypt the encrypted data, it is not suitable for certain applications such as sophisticated broadcast encryption and it provide fine grained access but has no longer with flexibility and scalability.

❖ Cipher text Policy Attribute Based Encryption (CP-ABE)

Sahai et al. introduced the concept of another modified form of ABE called CP-ABE that is Cipher- text Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. In a CP-ABE scheme, a cipher text is associated with a monotonic tree structure and a users decryption key is associated with set of attributes. Limitations of this scheme are: it cannot fulfill the enterprise requirements of access control which require considerable flexibility and efficiency.

2.7.2 SYMMETRIC KEY ENCRYPTION

When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography.

➢ Advanced Encryption Standard (AES)

AES is an Advanced Encryption Standard used for secure transmission of data that is personal health record in encrypted format. In our system AES is used for sending user authentication data in encrypted format. AES allows for three different key lengths: 128, 192, or 256 bits. For encryption, each round consist of the following four steps:

1) Substitute bytes

2) Shift rows

3) Mix columns

4) Add round key

The last step consists of XORing the output of the previous three steps. For decryption, each round consists of the following four steps:

1) Inverse shift rows

2) Inverse substitute bytes

3) Add round key

4) Inverse mix columns. The third step consists of XORing the output of the previous two steps.

Step1: Substitute bytes

This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array. The entries in the lookup table are created by using the notions of multiplicative inverses in GF(28) and bit scrambling to destroy the bit-level correlations inside each byte.

Step2: Shift rows

The first row of state is not altered. The second row is shifted 1 bytes to the left in a circular manner. The third row is shifted 2 bytes to the left in a circular manner. The fourth row is shifted 3 bytes to the left in a circular manner.

Step3: Mix columns

Mix Columns for mixing up of the bytes in each column separately during the forward process.(The access and loss). This paper proposed the new approach for existing PHR system for providing more security using attribute based encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance privacy guarantee.

➢ Chaos based cryptography

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications. Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behaviour is a subtle behaviour of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos is its extreme sensitivity to initial conditions of the system.

It was realised in the early 1990's that securing communications could be a potential application emerging out of studies on chaos theory. This was based on the discovery of chaotic synchronization principles, by Pecora& Carroll [1]. These works motivated communication and signal processing engineers and scientists to look into this. The defining properties of chaotic dynamics, namely, ergodicity, sensitivity on initial conditions and system parameters, are in fact the key features contributing towards building up of secure communication schemes based on chaos. In

this context, many hardware circuits were proposed and built . Interest in chaos based systems as an alternative to the existing schemes, such as RSA/ECC etc.

Cryptography is increasing in the past few years. The subtle chaotic behavior can be simulated in the simplest of one or two dimensional systems represented by discrete maps or in higher dimensional physical systems described by three or more first order autonomous differential equations or two or more first order ordinary non-autonomous differential equations. A large number of chaotic systems, both physical and mathematical, are now available which could potentially serve as both hardware and software equipments for realising encryption and decryption of messages. According to May ,simple nonlinear systems following iterative dynamics are potential generators of complicated dynamics. It is this dynamics which assumes importance in encryption/decryption algorithms of cryptography.

In chaotic synchronization of analog devices, the stability and drifts are important practical hurdles, which are to be overcome before application of synchronization-based schemes for cryptography. In contrast, a software approach becomes more practical and in tune with presentday advances in information processing. A synchronization-based scheme involves the chaotic signal carrier which is prone to cryptographic attack, via a possible break of cipher using reconstruction dynamics approach . An attempt has been made to overcome this defect in the work described in this paper.

Software schemes involving direct encryption of the trajectories using hopping Logistic map by Arvindet. al and generation of multiple keys using chaotic functions by Bose et. al have been proposed recently. A large number of schemes are available in literature exploiting chaotic functions for direct encryption using the system parameters as keys. However, a novel approach based on the ergodic nature of chaotic trajectory was suggested by Baptista . It uses the Logistic map with two of its parameters for chaotic encryption. A new encryption scheme based on Lorenz dynamics was developed, which extends Baptista's method to Lorenz system . The new scheme is further enriched to guard against reconstruction dynamics and statistical attack. This scheme has been tested for different types of textual messages leading to faithful message recovery.

Chaos based cryptography is still in its infancy and may not have exact parallelism to concepts and notions of traditional cryptographic and cryptanalysis approaches. In such a situation, our approach has been to enhance security of the scheme by providing larger key space, protection against reconstruction dynamics and resistance from statistical attack. Proving the security of encryption

based on chaos is still an open topic because one cannot use the analytical methods of classical cryptography which are based on number theoretic concepts or hardness of discrete logarithmic problem, etc. Before the details on the proposed modifications of the Baptista method in this scheme are presented, a short review on Chaos is given below.

❖ Chaotic systems

Chaos is one of the possible behaviours associated with evolution of a nonlinear physical system and occurs for specific values of system parameters. The discovery of this apparently random behaviour ensuing out of deterministic systems turned out to be quite revolutionary leading to many issues interconnecting stability theory, new geometrical features and new signatures characterising dynamical performances.

❖ Special Properties of Chaotic Systems :

Systems which are basically nonlinear and exhibiting an apparently random behaviour for certain range of values of system parameters are referred to as Chaotic. However, the solutions or trajectories of the system remain bounded within the phase space. This unstable state has a strong dependence on the values of the parameters and on the way the system begins. The following properties characterise chaotic dynamics.

- **Sensitivity to initial conditions :**

Given an initial state of a deterministic system [nonlinear system, in general], it is well known that the future states of the system can be predicted. However, for chaotic systems, longterm prediction is impossible. For specific values of parameters, two trajectories, which are initially very close, diverge exponentially in a short time. Initial information about the system is thus completely lost.

- **Ergodicity**

Ergodicity is that property in which a trajectory in phase space comes arbitrarily close to its earlier states. Trajectory of a chaotic system in its evolutionary wanderings also satisfies this property. It essentially reflects that the system eventually is confined to a spatial object, a set of points called an attractor. The density of such points is time invariant and this property is essential to cryptography.

- **Mixing**

It is a characteristic of a system in which a small interval of initial conditions gets spread over the full phase space in its asymptotic evolution. In a chaotic system, an arbitrary interval of initial conditions spreads over the part (attractor) of the phase space to which the trajectory asymptotically confines. Thus any region gets into every other region of the spatial attractor of phase space.

- **Illustrations of Chaotic Systems**

In the following discussions, we consider a discrete time evolution and a continuous time evolution systems. They are markedly different and are the best representatives of a general class of nonlinear systems.

Logistic map

This is one-dimensional map proposed by R. M. May representing an idealised ecological model for describing yearly variation in the population of an insect species. The population at (n+1)th year is mathematically related to that at the (n) th year by the following equation: For this map, different scenarios of evolutionary behaviour were established when the system parameter r was varied over the interval [0,4]. The iterates were confined to [0,1]. Possible behaviours [solutions xi's] in the asymptotic limit, resulting out of parametric variations.

❖ Chaos and Cryptography

The strength of cryptography lies in choosing the keys, which are secret parameters, used in encryption. It should not be possible to guess the key by an intruder. Chaotic systems are very sensitive to initial conditions and system parameters. For a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories. Therefore encryption / decryption scheme can be obtained if the parameters are chosen as "Keys" and "Trajectories" are used for encryption/decryption. Since the same parameters are used for encryption and decryption, the chaos scheme is symmetric. The parameters and the initial conditions form a very large key space thereby enhancing the security of the code.

- **Encryption**

Encryption of a message M is then carried out on the following lines. Lorenz dynamics is carried out using x (0), y (0) and z (0) and the values of the parameter σ, β, R. The chosen variable on transformation becomes: ν = ν m o d p Encryption of a character in M involves running the dynamics from initial conditions x (0), y (0) and z (0), until the ν value falls in the interval corresponding to the required site associated with the character. The number of time steps n [equivalent to number of iterations in Logistic map] to reach the required site should be greater than N0 (transient cross over). Further, a random number 'k' from a uniform distribution is generated and compared with a pre-chosen value η ∈ [0,1]. If k>η, then the number of time steps 'n' is the encryption of the character. This procedure is repeated until the whole message M is encrypted. The encrypted message Cn is now a set of integers less than 65532.

- **Decryption**

To decrypt the ciphertextCn: {n1, n2, n3……., ni ,….}, Lorenz dynamics is run with the same parameters and initial conditions as in the encryption. The time evolution is continued up to the number of time steps, ni = n1. The value of the chosen variable corresponding to n1 is located on one of the sites. The associated ASCII value of the reached site gives us the decrypted character. The steps are continued until the whole cipher text is decrypted

2.8 DIGITAL WATERMARKING

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should,[1] 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 tracingcopyright infringements and for banknote authentication. The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But where as steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

2.8.1 WATERMARKING TECHNIQUES

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

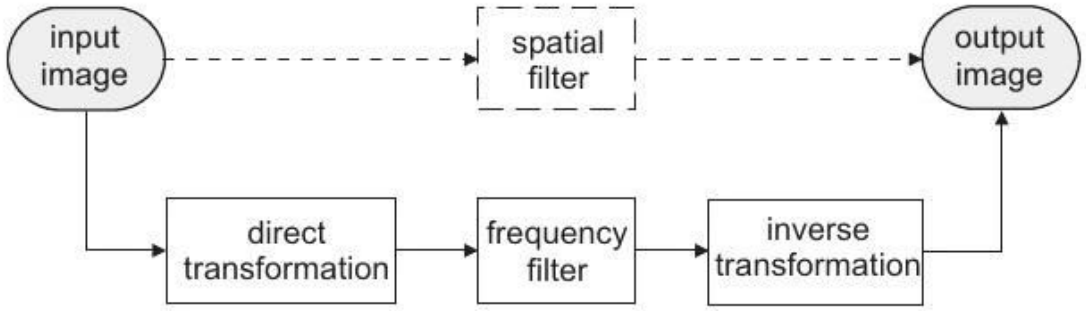


Figure 2.9: Brief Idea of Spatial and Frequency Domain

❖ Spatial domain:

Spatial domain digital watermarking algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image. Some of its main algorithms are as discussed below:

• Additive Watermarking:

The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low.

• Least Significant Bit:

Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

• SSM Modulation Based Technique:

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

- **Texture mapping coding Technique:**

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage), and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

- **Patchwork Algorithm:**

Patchwork is a data hiding technique developed by Bender etalii and published on IBM Systems Journal, 1996. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified).

The following are the steps involved in the Patchwork algorithm:

• Generate a pseudo-random bit stream to select pairs of pixels from the cover data. For each pair, let d be the difference between the two pixels.

• Encode a bit of information into the pair. Let d < 0 represent 0 and d > 0represent

• Given that the pixels are not ordered correctly, swap them.

• In the event that d is greater than a predefined threshold or if is equal to 0, ignore the pair and proceed to the next pair. Patchwork being statistical methods uses redundant pattern encoding to insert message within an image.

- **Correlation-Based Technique:**

In this technique, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image I(x, y). Iw(x, y) = I(x, y) + k*W(x, y) Where K represent the gain factor, Iw represent watermarked image ant position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

❖ Frequency domain:

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients.

• Discrete cosine transforms (DCT):

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

Steps in DCT Block Based Watermarking Algorithm

- Segment the image into non-overlapping blocks of 8x8
- Apply forward DCT to each of these blocks
- Apply some block selection criteria (e.g. HVS)
- Apply coefficient selection criteria (e.g. highest)
- Embed watermark by modifying the selected coefficients.
- Apply inverse DCT transform on each block.

- **Discrete wavelet transforms (DWT):**

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies.

- **Advantages of DWT over DCT:**

Wavelet transform understands the HVS more closely than the DCT. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.

- **Disadvantages of DWT over DCT:**

Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient.

- **Discrete Fourier transform (DFT):**

Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

- **Advantages of DFT over DWT and DCT:**

DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

2.8.2 CLASSIFICATION OF DIGITAL WATERMARKING

In this section the digital watermarks, features, their techniques and application are classified and segmented into various categories.

1) According to characteristics/robustness

- **Robust:**

Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.

- **Fragile:**

Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

- **Semi fragile:**

Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.

2) According to attached media/host signal

- **Image watermarking:**

This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.

- **Video watermarking:**

This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

- **Audio watermarking:**

This application area is one of the most popular and hot issue due to internet music, MP3.

- **Text watermarking:**

This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

- **Graphic watermarking:**

It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

3) According to perceptivity:

- **Visible watermark:**

The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.

- **Invisible watermarking:**

There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‘t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good.

4) According to its purpose:

- **Copyright protection watermarking:**

This means if the owner want others to see the mark of the image watermark, then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked.

- **Tampering tip watermarking:**

It protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats.

- **Anti-counterfeiting watermarking:**

It is added to the building process of the paper notes and can be detected after printing, scanning, and other processes.

- **Anonymous mark watermarking:**

It can hide important annotation of confidential data and restrict the illegal users to get confidential data.

5) According to watermark type:

- **Noise type:**

Noise type has pseudo noise, Gaussian random and chaotic sequences.

- **Image type:**

There are binary image, stamp, logo and label.

6) According to domain:

- **Spatial domain:**

This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Some of its algorithms are LSB, SSM Modulation based technique.

- **Frequency domain**:

This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT.

7) According to detection process:

- **Visual watermarking:**

It needs the original data in the testing course, it has stronger robustness, but its application is limited.

- **Semi blind watermarking:**

It does not require an original media for detection.

- **Blind watermarking:**

It does not need original data, which has wide application field, but requires a higher watermark technology.

8) According to use of keys:

- **Asymmetric watermarking:**

This is technique where different keys are used for embedding and detecting the watermark.

- **Symmetric watermarking:**

Here same keys are used for embedding and detecting the watermark.

2.8.3 FEATURES OF DIGITAL WATERMARKING

Various features of watermarking are as follows:

- **Robustness:**

Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack.

- **Imperceptibility:**

Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.

- **Security:**

A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.

- **Verifiability:**

Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

- **Capacity and data payload:**

Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work. The number of watermark bits in a message in data payload and the maximum repetition of data payload within an image is the watermark capacity. Depending on the application some watermarking methods require a data payload exceeding 10,000 bits. A watermark may have high data capacity but low data payload.

- **Computational cost:**

In order to reduce computational cost, a watermarking method should be less complex. Watermarking methods with high complex algorithms will require more software as well as hardware resources and thus incur more computational cost. Computational simplicity usually preferred in resource-limited environments like mobile devices.

- **Watermark detection reliability:**

To model robust watermarking in a copyright protection scenario, we can use a watermark that consists of a pseudo-random binary sequence to represent the identity of a copyright holder. The correlation value between the identity and a correctly detected watermark is usually very high

compared to the correlation value between the identity and randomly chosen watermark. In this case a graph of correlation values plotted against watermarks has a significant peak at the correctly detected watermark which corresponds to the copyright holder‘s identity. This is watermark detection outcome.

For an image with watermark embedded, there are 2 possible results of its watermark detection:

1) The successful detection of the watermark is called a true positive.
2) The unsuccessful detection of the watermark is called a false negative.

Likewise, for a given cover image (or un-watermarked test image), there are 2 possible results of its watermark detection:

1. The absence of watermark is called a true negative.
2. An incorrectly detected watermark causes a false positive (a.k.a false alarm)

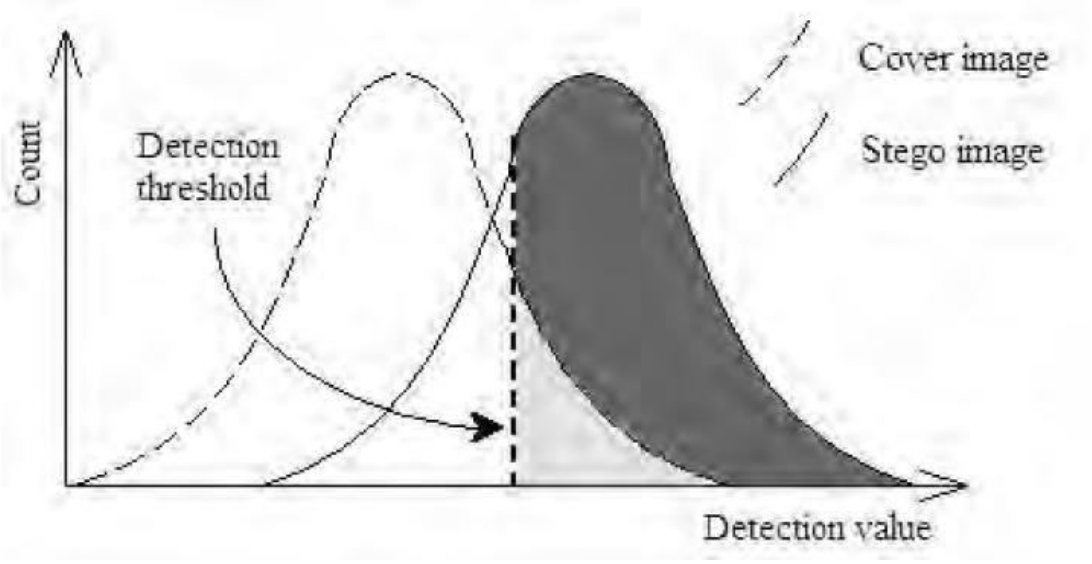


Figure Figure 2.10: Distribution of Watermark Detection Values for Cover and Stego Images. The Sum Of The Lightly Shaded And Heavily Shaded Areas Is A Probability Of True Positive.

- **Blind or non-blind detection of watermark:**

A watermarking technique is said to be blind, if it does not require original image to recover the watermark from the watermarked image. Conversely, a watermarking technique is said to be non-blind, if it needs original image for extracting the watermark from the watermarked image. The

blind technique is also referred as oblivious. The non-blind watermarking systems are more robust than blind watermarking systems due to availability of original cover image at the time of detection. However, blind or oblivious watermarking systems are more popular. The oblivious watermarking systems decrease the overhead of cost and memory for storing original images.

❖ Tradeoff between performance factors:

A basic principle of watermarking is to exploit redundancy in images for embedding the watermark information. Given the fact that many of the existing image compression algorithms are not perfect, watermarking is made possible by embedding extra information in the redundant parts. In addition, enhancing watermark robustness normally requires more image distortions and increased redundancy. This causes lower imperceptibility and more likely to be removed under malicious attacks.

2.8.4 REQUIREMENTS OF DIGITAL WATERMARKING :

There are a number of important characteristics that a watermark can exhibit, Jalil and Mirza (2010), Bandyopadhyay and Paul (2010). The most important properties of digital watermarking techniques are transparency, robustness, security, capacity, invert ability (reversibility) and complexity and possibility of verification. Transparency relates to the properties of the human sensory. A transparent watermark causes no artifacts or quality loss.

• Robustness:

Robustness means Resistance to ―blind‖, non-targeted modifications, or common media operations. For example the Stirmark or Mosaik tools attack the robustness of watermarking algorithms with geometrical distortions. For manipulation recognition the watermark has to be fragile to detect altered media. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it. When a signal is distorted, its fidelity is only preserved if its perceptually significant regions remain intact, while perceptually insignificant regions might be drastically changed with little effect on fidelity.

- **Security**:

Security describes whether the embedded watermarking information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, except the key, and the knowledge of at least one watermarked data. 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.

- **Capacity:**

Capacity describes how many information bits can be embedded. It addresses also the possibility of embedding multiple watermarks in one document in parallel. Capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness (Fig 2.11). A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

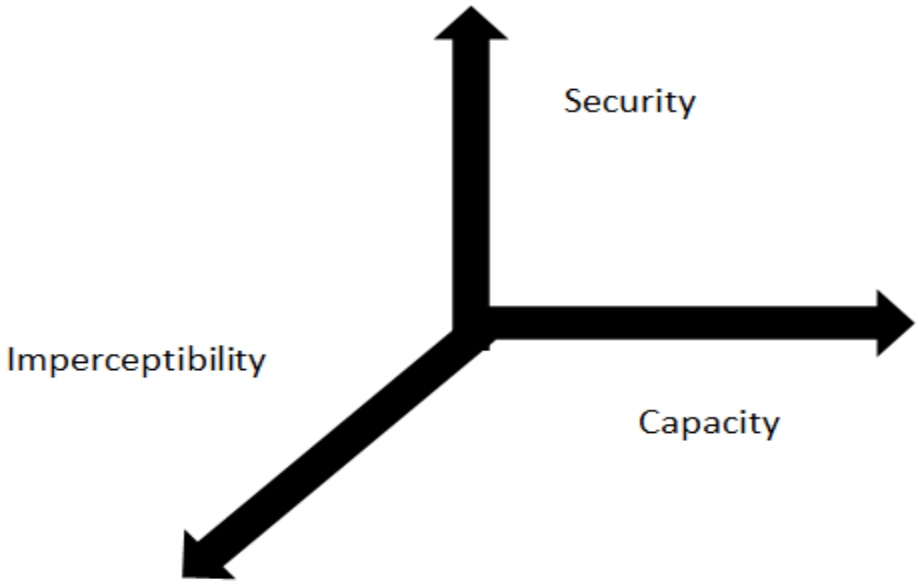


Figure 2.11:The Tradeoffs among Imperceptibility, Robustness, and Capacity

- **Imperceptibility:**

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term ―imperceptible‖ is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.

- **Modification and Multiple Watermarks:**

Changing a watermark can be accomplished by either removing the first watermark or then adding a new one, or Inserting a second watermark. The first alternative goes against the principle of tamper resistance, because it implies that a watermark is easily removable. Allowing multiple watermarks to coexist is the preferred solution. There is however security problem related to the use of multiple watermarks. The basis of watermarking security should lie on Kirchhoff‘s assumption that one should assume that the method used to encrypt the data is known to the unauthorized party. It means that watermarking security can be interpreted as encryption security leading directly to the principle that it must lie mainly in the choice of the embedded key. Allows insertion of multiple, independently detectable watermarks in an Image.

- **Invertibility:**

Invertibility describes the possibility to produce the original data during the watermark retrieval. The optimization of the parameters is mutually competitive and cannot be clearly done at the same time. If we want to embed a large message, we cannot require large robustness simultaneously. A reasonable compromise is always a necessity. On the other hand, if robustness to strong distortion is an issue, the message that can be reliably hidden must not be too long.

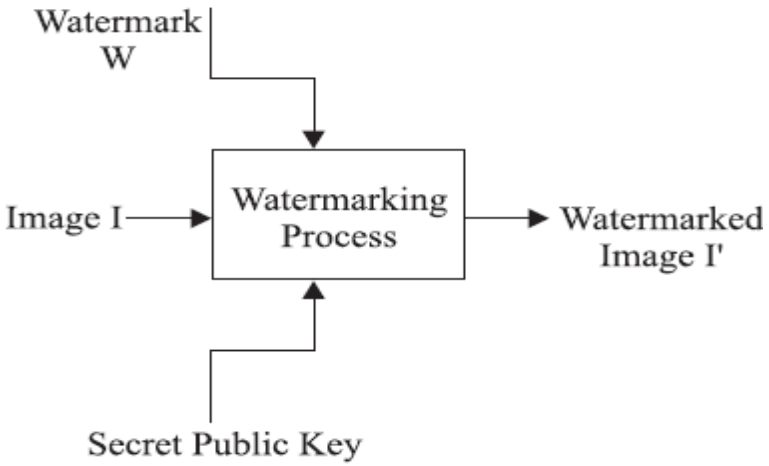


Figure 2.12: Architecture of Digital watermarking

2.8.5 SIMPLE DIGITAL WATERMARKING:

Simple Digital watermarking is a technology in which a watermark (secret information) is hidden in the digital media using an appropriate algorithm for the authentication and identification of original owner of the product. Outcome we get is watermarked image. Simple digital watermarking technique consists of two modules watermark embedding module and watermark detection and extraction module. Watermark embedding embeds the watermark into the original image using a key. The watermark embedding module is as Fig(2.13)

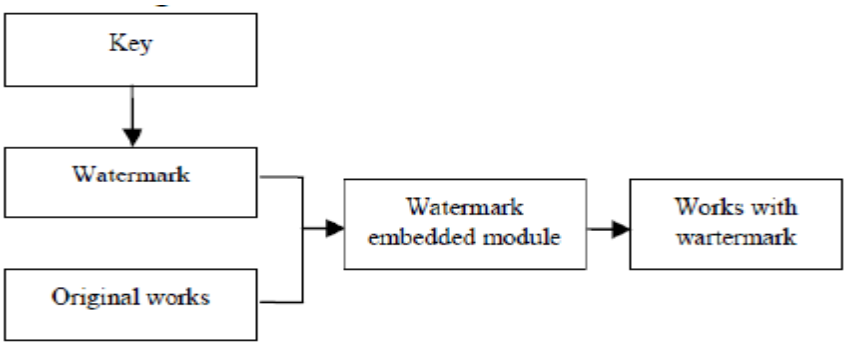


Figure 2.13: Watermark Embedding Module

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted. Watermark Detection and Extraction Module is as Figure below.

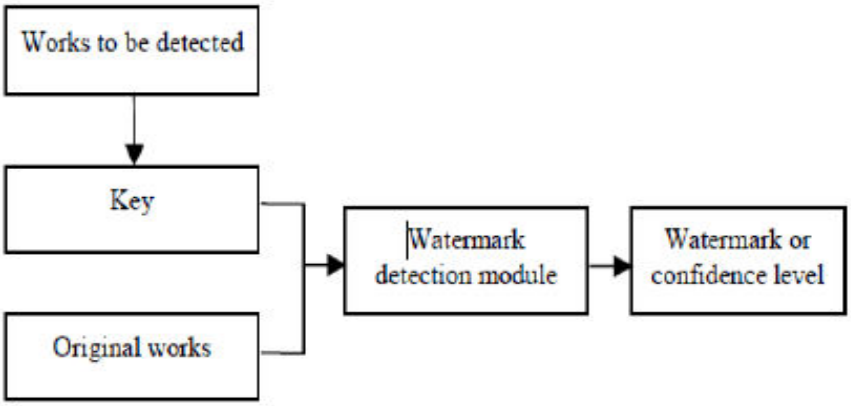


Figure 2.14: Watermark Detection and Extraction Module

2.8.6 STYLES OF ROBUST WATERMARKS

There various types of styles watermarks, some of them are discussed in this survey.

- **Noise Watermark:**

Noise watermark is most commonly used type of robust watermark. For the reason of security and statistical undetectivity, it is demonstrated that the watermark is most secure, if it is in the form of Gaussian random sequence. To measure the similarity between original and extracted sequence, the correlation value is used to indicate the similarity.

- **Logo Watermark:**

Logo is another form of robust watermark. The logo is small image pattern in binary form. It can be company logo used in commercial applications. The quality of logo image is measured by human perception. That is, it is subjective measure of verifying authenticity of the digital content.

- **Message Watermark:**

Message watermark is comprised of text. Message watermark has the advantage of easy to use in comparison with noise-type watermark or logo watermark. However, the message watermark require bit error rate approaching to zero, because any bit error will cause major fault in the final result. In most cases it is required that information with at least 64 bit (or 8 ASCII character can be carried by multimedia).

2.8.7 APPLICATIONS OF DIGITAL WATERMARKING

Digital Watermarks are potentially useful in many applications, including:

- **Ownership assertion:**

Watermarks can be used for ownership assertion. To assert ownership of an image, Alice can generate a watermarking signal using a secret private key, and then embed it into the original image. She can then make the watermarked image publicly available. Later ,when Bob contends the ownership of an image derived from this public image, Alice can produce the unmarked original image and also demonstrate the presence of her watermark in Bob's image .Since Alice's original image is unavailable to Bob, he cannot do the same. For such a scheme to work, the watermark has to survive image processing operations aimed at malicious removal. In addition, the watermark should be inserted in such a manner that it cannot be forged as Alice would not want to be held accountable for an image that she does not own.

- **Fingerprinting:**

In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data. If, at a later point in time, unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the fingerprint. In this application the watermark needs to be invisible and must also be invulnerable to deliberate attempts to forge, remove or invalidate. Furthermore, and unlike the ownership assertion application, the watermark should be resistant to collusion. That is, a group of k users with the same image but containing different fingerprints, should not be able to collude and invalidate any fingerprint or create a copy without any fingerprint.

- **Copy prevention or control:**

Watermarks can also be used for copy prevention and control .For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a systemic the Digital Versatile Disc (DVD). In fact, a copy protection mechanism that includes digital2watermarking at its core is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence .Another example is in digital cinema, where information can be embedded as a watermark in every frame or a sequence of frames to help investigators locate the scene of the piracy more quickly and point out weaknesses in security in the movie's distribution. The information could include data such as the name of the theater and the date and time of the screening. The technology would be most useful in fighting a form of piracy that's surprisingly common, i.e., when someone uses a camcorder to record the movie as it's shown in a theater, then duplicates it onto optical disks or VHS tapes for distribution.

- **Fraud and tamper detection:**

When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the data. Subsequently, when the photo is checked, the watermark is extracted using a unique key associated with the source, and the integrity of the data is verified through the integrity of the extracted watermark. The watermark can also include information from the original image that can aid in undoing any modification and recovering the original. Clearly a watermark used for authentication purposes should not affect the quality of an image and should be resistant to forgeries. Robustness is not critical as removal of the watermark renders the content inauthentic and hence of no value.

- **ID card security:**

Information in a passport or ID (e.g., passport number, person's name, etc.) can also be included in the person's photo that appears on the ID. By extracting the embedded information and comparing it to the written text, the ID card can be verified. The inclusion of the watermark provides an additional level of security in this application. For example, if the ID card is stolen and the picture is replaced by a forged copy, the failure in extracting the watermark will invalidate the ID card. The above represent a few example applications where digital watermarks could potentially be of use. In addition there are many other applications in rights management and protection like tracking use of content, binding content to specific players, automatic billing for viewing content, broadcast monitoring etc. From the variety of potential applications exemplified above it is clear that a digital watermarking technique needs to satisfy a number of requirements. Since the specific requirements vary with the application, watermarking techniques need to be designed within the context of the entire system in which they are to be employed. Each application imposes different requirements and would require different types of invisible or visible watermarking schemes or a combination thereof. In the remaining sections of this chapter we describe some general principles and techniques for invisible watermarking. Our aim is to give the reader a better understanding of the basic principles, inherent trade-offs, strengths, and weakness, of digital watermarking. We will focus on image watermarking in our discussions and examples. However as we mentioned earlier, the concepts involved are general in nature and can be applied to other forms of content such as video and audio.

- **Digital right management:**

Digital right management (DRM) can be defined as ―the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets‖. It concerns the management of digital rights and the enforcement of rights digitally.

- **Tamper proofing:**

Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

- **Broadcast monitoring:**

Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.

- **Access control:**

Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

- **Medical application:**

Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

- **Image and content authentication:**

In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera .

- **Annotation and privacy control:**

Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic `document indexing and automated information retrieval.

- **Media forensics:**

Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

- **Communication enhancement:**

Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.

- **Content protection for audio and video content:**

Modern digital formats employed for sale or rental of commercial audio and video content to consumers-such as DVD, Blu-Ray Disc, and iTunes-incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content.

- **Content filtering:**

The lean-back experience of watching television has radically changed over the last few years. Today people want to watch content in their own time and place. The proliferation of set top boxes (STB) in homes evidences this, as people want to watch video on demand or on a time-shifted schedule. Today, more than a device to watch films/series, sports or even play games, the STB has become an interactive device providing multiple services.

- **Communication of ownership and objects:**

Digital content continues to proliferate as today's consumers seek information and entertainment on their computers, mobile phones and other digital devices. In our cyber culture, digital has become a primary means of communication and expression. The combination of access and new tools enables digital content to travel faster and further than ever before as it is uploaded, dispersed, viewed, downloaded, modified and repurposed at breathtaking speed. Whether you are a global media corporation or a freelance photographer, the ability to communicate your copyright ownership and usage rights is essential.

- **Document and Image security:**

Consider documents and images that are generated in support of a major product launch. Corporate communications professionals face significant challenges in managing these assets through very complex sales and marketing channels. Images and documents are distributed to remote offices, agencies, distributors, dealers and more, and must be managed to ensure confidential information is not leaked before the launch date.

- **Locating content online:**

The volume of content being uploaded to the web continues to grow as we rely more and more on the Internet for information sharing, customer engagement, research and communication. It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world.

- **Audience measurement:**

In this new media world of insatiable content consumption, audience measurement is becoming more and more critical. Beyond the hard numbers of how many people are accessing a program, understanding who is watching, how they engage with the content, when, where and through which media is essential for content providers, advertisers and broadcasters to better tailor their offerings and maximize impact.

- **Improved auditing:**

Media content of all types -television, music, movies, etc. - continues to proliferate and make its way onto many new consumer devices as well as many sites across the internet. Digital watermarking applications for auditing give all members within the value chain the ability to verify usage to support highly accurate billing and contract enforcement.

- **Advantages of watermarking**

1. High security by using the watermarking method

2. To provide the better quality of the signal (PSNR)

3. To decrease the noise quantity (MSE)

4. Low Distortion

5. Loss Data recovery

6. Highly Protection of Confidential data

7. To increase the data hiding (more data) by using chaos encryption method and also we can provide more security for information when compared to our old methods like DES, RSA, AESetc.

CHAPTER-3

3.1 BASICS OF MATLAB

MATLAB is an interactive program for numerical computation and data visualization; it is used extensively by control engineers for analysis and design. There are many different toolboxes available which extend the basic functions of MATLAB into different application areas; in these tutorials, we will make extensiveuse of the Control Systems Toolbox. MATLAB is supported on Unix, Macintosh,and Windows environments; a student version of MATLAB is available for personal computers.

The idea behind these tutorials is that you can view them in one window while running MATLAB in another window. You should be able to re-do all of the plots and calculations in the tutorials by cutting and pasting text from the tutorials into MATLAB or an m-file.

3.1.1 Vectors:

Let's start off by creating something simple, like a vector. Enter each element of the vector (separated by a space) between brackets, and set it equal to a variable. For example, to create the vector **a**, enter the following into the MATLAB command window (you can **Copy** and **Paste** from your browser into MATLAB to make it easy) and MATLAB should return the following:

```
a = [1 2 3 4 5 6 9 8 7]
```

```
a =

   1   2   3   4   5   6   9   8   7
```

Let's say you want to create a vector with elements between 0 and 20 evenly spaced in increments of two (this method is frequently used to create a time vector):

```
t = 0:2:20
```

```
t =
```

```
0    2    4    6    8    10    12    14    16    18    20
```

Manipulating vectors is almost as easy as creating them. First, suppose you would like to add 2 to each of the elements in the vector **a**. The equation for that looks like:

```
b = a + 2
b =
    3    4    5    6    7    8    11    10    9
```

Now suppose, you would like to add two vectors together. If the two vectors are the same length, it is easy. Simply add the two as shown below:

```
c = a + b

c =

    4    6    8    10    12    14    20    18    16
```

Subtraction of vectors of the same length works exactly the same way.

3.1.2 Functions:

To make life easier, MATLAB includes many standard functions. Each function is a block of code that accomplishes a specific task. MATLAB contains all of the standard functions such as sin, cos, log, exp, sqrt, as well as many others. Commonly used constants such as pi, and i or j
for the square root of -1, are also incorporated into MATLAB.

```
sin(pi/4)
ans =

    0.7071
```

To determine the usage of any function, type help [function name] at the MATLAB command window. MATLAB even allows you to write your own functions with the **function** command;

3.1.3 Plotting:

It is also easy to create plots in MATLAB. Suppose you wanted to plot a sine wave as a function of time. First, make a time vector (the semicolon after each statement tells MATLAB we don't want to see all the values) and then compute the sin value at each time. The commands after
the plot function (title, xlabel, ylabel) will add annotations to the plot.

```
t = 0:0.25:7;
y = sin(t);
plot(t ,y)
title('Sine Wave as a Function of Time')
xlabel('Time (secs)')
ylabel('Amplitude')
```

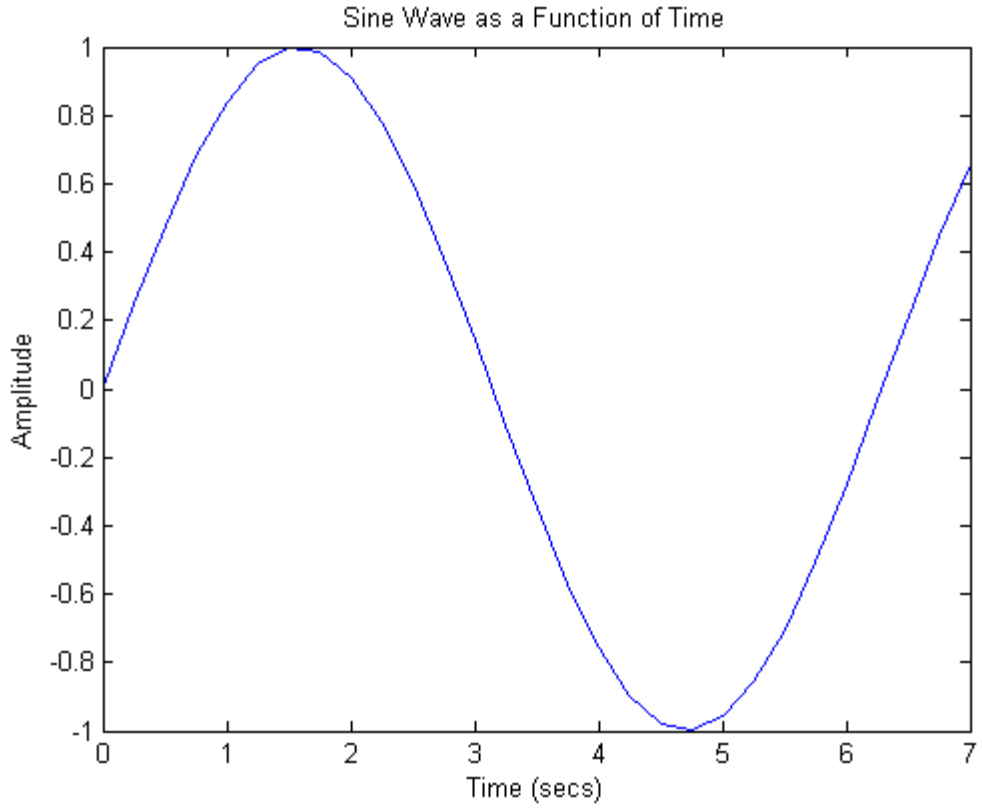


Figure 3.1:- Sine wave model

The plot contains approximately one period of a sine wave. Basic plotting is very easy in MATLAB, and the plot command has extensive add-on capabilities.

3.1.4 Polynomials as Vectors:

In MATLAB, a polynomial is represented by a vector. To create a polynomial in MATLAB, simply enter each coefficient of the polynomial into the vector in descending order. For instance, let's say you have the following polynomial:

$$s^4 + 3s^3 - 15s^2 - 2s + 9$$

To enter this into MATLAB, just enter it as a vector in the following manner:

```
x = [1 3 -15 -2 9]
x =
     1    3   -15   -2    9
```

MATLAB can interpret a vector of length n+1 as an nth order polynomial. Thus, if your polynomial is missing any coefficients, you must enter zeros in the appropriate place in the vector. For example,

$$s^4 + 1$$

Would be represented in MATLAB as:

```
y = [1 0 0 0 1]

y =
     1    0    0    0    1
```

You can find the value of a polynomial using the polyval function. For example, to find the value of the above polynomial at s = 2,

```
z = polyval([1 0 0 0 1],2)
z =
    17
```

You can also extract the roots of a polynomial. This is useful when you have a high-order polynomial such as

$$s^4 + 3s^3 - 15s^2 - 2s + 9$$

Finding the roots would be as easy as entering the following command:

```
roots([1 3 -15 -2 9])
ans =
    -5.5745
     2.5836
    -0.7951
     0.7860
```

Let's say you want to multiply two polynomials together. The product of two polynomials is found by taking the convolution of their coefficients. MATLAB's function conv will do this for you.

```
x = [1 2];
y = [1 4 8];
z = conv(x,y)
z = 1     6     16     16
```

Dividing two polynomials is just as easy. The deconv function will return the remainder as well as the result. Let's divide z by y and see if we get x.

```
[xx, R] = deconv(z ,y)
xx =
     1     2
R =
     0     0     0     0
```

As you can see, this is just the polynomial/vector x from before. If y had not gone into z evenly, the remainder vector would have been something other than zero.

3.1.5 Polynomials Using the s Variable:

Another way to represent a polynomial is to use the Laplace variable s within MATLAB. This method is mainly used throughout these tutorials.Let's ignore the details of the Laplace domain for now and just represent polynomials with the s variable. To define the variable, type the following into the MATLAB command window:

```
s = tf('s')
s = s
```

Continuous-time transfer function.

Recall the polynomial given above:

$$s^4 + 3s^3 - 15s^2 - 2s + 9$$

To represent this in MATLAB, type the following into the MATLAB command window:

```
polynomial = s^4 + 3*s^3 - 15*s^2 - 2*s + 9

polynomial =
                s^4 + 3 s^3 - 15 s^2 - 2 s + 9
```

Continuous-time transfer function.

Instead of using the roots function, we can use the zero function to find the roots of the polynomial.

```
zero(polynomial)
ans =
   -5.5745
    2.5836
   -0.7951
    0.7860
```

As you can see, the result is the same as above using the roots command and the coefficients of the polynomial. You can also multiply two polynomials together using the s variable. Let's redefine x and y.

```
x = s + 2;
y = s^2 + 4*s + 8;
z = x * y
z =s^3 + 6 s^2 + 16 s + 16
```

Continuous-time transfer function.

The resulting polynomial has the same coefficients as the resulting vector from the conv function above.

3.1.6 Matrices:

Entering matrices into MATLAB is the same as entering a vector, except each row of elements is separated by a semicolon (;) or a return:

```
B = [1 2 3 4; 5 6 7 8; 9 10 11 12]
      B = [ 1 2 3 4
            5 6 7 8
            9 10 11 12 ]
B =
     1  2   3    4
     5   6   7   8
     9   10   11   12
B =
     1   2   3   4
     5   6   7   8
     9   10   11   12
```

Matrices in MATLAB can be manipulated in many ways. For one, you can find the transpose of a matrix using the apostrophe key:

```
C = B'
```

```
C =
      1    5     9
      2    6    10
      3    7     11
      4    8     12
```

It should be noted that if *C* has been complex, the apostrophe would have actually given the complex conjugate transpose. To get the transpose in this case, use .' (the two commands are the same if the matrix is notcomplex).

Now you can multiply the two matrices *B* and *C* together.

Remember that order matters when multiplying matrices.

```
D = B * C
D = C * B
D =
```

```
    30    70     110
    70   174     278
   110   278     446

D =

   107   122   137   152
   122   140   158   176
   137   158   179   200
   152   176   200   224
```

Another option for matrix manipulation is that you can multiply the corresponding elements of two matrices using the. * operator (the matrices must be the same size to do this).

```
E = [1 2; 3 4]
F = [2 3; 4 5]
G = E .* F

E = 1   2
    3   4

F =

    2   3
    4   5

G =

    2    6
   12   20
```

If you have a square matrix, like *E*, you can also multiply it by itself as many times as you like by raising it to a given power.

```
E^3

ans =

   37   54
   81   118
```

If you wanted to cube each element in the matrix, just use the element-by-element cubing.

```
E.^3
ans =
     1     8
    27    64
```

You can also find the inverse of a matrix:

X = inv(E)

```
X =

   -2.0000
    1.0000    1.5000
   -0.5000
```

or its eigenvalues

```
eig(E)

ans =

   -0.3723

    5.3723
```

There is even a function to find the coefficients of the characteristic polynomial of a matrix. The poly function creates a vector that includes the coefficients of the characteristic polynomial.

```
p = poly(E)

p =

    1.0000   -5.0000   -2.0000
```

Remember that the eigenvalues of a matrix are the same as the roots of its characteristic polynomial:

roots(p)

ans =

5.3723

-0.3723

3.1.7 Printing:

Printing in MATLAB is pretty easy. Just follow the steps illustrated below:

a. Macintosh

- To print a plot or a m-file from a Macintosh, just click on the plot or m-file, select Print under the File menu, and hit Return.

b. Windows

- To print a plot or a m-file from a computer running Windows, just select Print from the File menu in the window of the plot or m-file, and hit Return.

c. Unix

- To print a plot on a Unix workstation enter the command: print - P<printername>.
- If you want to save the plot and print it later, enter the command: print plot.ps
- . Sometime later, you could print the plot using the command lpr -P plot.ps If you are using a HP workstation to print, you would instead use the command lpr -d plot.ps.
- To print a m-file, just print it the way you would any other file, using the command lpr -P *name of m-file*.m. If you are using a HP workstation to print, you would instead use the command lpr -d plot.ps *name of m-file*.m.

3.1.8 Using m-files in MATLAB:

There are slightly different things you need to know for each platform.

a. **Macintosh**

- There is a built-in editor for m-files; choose New M-file from the File menu. You can also use any other editor you like (but be sure to save the files in text format and load them when you start MATLAB).

b. **Windows**

- Running MATLAB from Windows is very similar to running it on a Macintosh. However, you need to know that your m-file will be saved in the clipboard. Therefore, you must make sure that it is saved as filename.m.

c. **Unix**

You will need to run an editor separately from MATLAB. The best strategy is to make a directory for all your m-files, then cd to that directory before running both MATLAB and the editor. To start MATLAB from your Xterm window, simply type: matlab .You can either type commands directly into MATLAB, or put all of the commands that you will need together in a m-file, and just run the file. If you put all of your m-files in the same directory that you run MATLAB from, then MATLAB will always find them.

3.1.9 Getting Help in MATLAB

MATLAB has a fairly good on-line help, type:

Help command name

For more information on any given command. You do need to know the name of the command that you are looking for; a list of the all the ones used in these tutorials is given in the command listing; a link to this page can be found at top right of this page.

3.2 DIGITAL SIGNAL PROCESSING (DSP)

DSP is the mathematical manipulation of an information signal to modify or improve it in some way. It is characterized by the representation of discrete time, discrete frequency, or other discrete domain signals by a sequence of numbers or symbols and the processing of these signals.

The goal of DSP is usually to measure, filter and/or compress continuous real-world analog signals. Usually, the first step is conversion of the signal from an analog to a digital form, by sampling and then digitizing it using an analog-to-digital converter (ADC), which turns the analog signal into a stream of discrete digital values. Often, however, the required output signal is also analog, which requires a digital-to-analog converter (DAC). Even if this process is more complex than analog processing and has a discrete value range, the application of computational power to signal processing allows for many advantages over analog processing in many applications, such as error detection and correction in transmission as well as data compression.

Digital signal processing and analog signal processing are subfields of signal processing. DSP applications include audio and speech signal processing, sonar and radar signal processing, sensor array processing, spectral estimation, statistical signal processing, digital image processing, signal processing for communications, control of systems, biomedical signal processing, seismic data processing, among others. DSP algorithms have long been run on standard computers, as well as on specialized processors called digital signal processors, and on purpose-built hardware such as application-specific integrated circuit (ASICs). Currently, there are additional technologies used for digital signal processing including more powerful general purpose microprocessors, field-programmable gate arrays (FPGAs), digital signal controllers (mostly for industrial applications such as motor control), and stream processors, among others.

Digital signal processing can involve linear or nonlinear operations. Nonlinear signal processing is closely related to nonlinear system identification and can be implemented in the time, frequency, and spatio -temporal domains.

3.2.1 APPLICATIONS

The main applications of DSP are audio signal processing, audio compression, digital image processing, video compression, speech processing, speech recognition, digital communications, radar, sonar, financial signal processing, seismology and biomedicine. Specific examples are speech compression and transmission in digital mobile phones, room correction of sound in hi-fi and sound reinforcement applications, weather forecasting, economic forecasting, seismic data processing, analysis and control of industrial processes, medical imaging such as CAT scans and MRI, MP3 compression, computer graphics, image manipulation ,hi-fi loudspeaker crossovers and equalization, and audio effects for use with electric guitar amplifiers

3.2.2 SIGNAL SAMPLING

The increasing use of computers has resulted in the increased use of, and need for, digital signal processing. To digitally analyze and manipulate an analog signal, it must be digitized with an analog-to-digital converter. Sampling is usually carried out in two stages, discretization and quantization. In the discretization stage, the space of signals is partitioned into equivalence classes and quantization is carried out by replacing the signal with representative signal of the corresponding equivalence class. In the quantization stage, the representative signal values are approximated by values from a finite set.The Nyquist–Shannon sampling theorem states that a signal can be exactly reconstructed from its samples if the sampling frequency is greater than twice the highest frequency of the signal, but this requires an infinite number of samples. In practice, the sampling frequency is often significantly higher than twice that required by the signal's limited bandwidth Some (continuous-time) periodic signals become non-periodic after sampling, and some non-periodic signals become periodic after sampling. In general, for a periodic signal with period T to be periodic (with period N) after sampling with sampling interval T_s, the following must be satisfied: $T_s N = Tk$ Where *k is an integer.*

3.2.3 DSP DOMAIN'S

In DSP, engineers usually study digital signals in one of the following domains: time domain (one-dimensional signals), spatial domain (multidimensional signals), frequency domain, and wavelet domains. They choose the domain in which to process a signal by making an informed assumption (or by trying different possibilities) as to which domain best represents the essential characteristics of the signal. A sequence of samples from a measuring device produces a temporal or spatial domain representation, whereas a discrete Fourier transform produces the frequency domain information, that is, the frequency spectrum. Autocorrelation is defined as the cross-correlation of the signal with itself over varying intervals of time or space.

➢ Time and space domains

The most common processing approach in the time or space domain is enhancement of the input signal through a method called filtering. Digital filtering generally consists of some linear transformation of a number of surrounding samples around the current sample of the input or output signal. There are various ways to characterize filters; for example:

- A "linear" filter is a linear transformation of input samples; other filters are "non-linear". Linear filters satisfy the superposition condition, i.e. if an input is a weighted linear combination of different signals, the output is a similarly weighted linear combination of the corresponding output signals.

- A "causal" filter uses only previous samples of the input or output signals; while a "non-causal" filter uses future input samples. A non-causal filter can usually be changed into a causal filter by adding a delay to it.

- A "time-invariant" filter has constant properties over time; other filters such as adaptive filters change in time.

- A "stable" filter produces an output that converges to a constant value with time, or remains bounded within a finite interval. An "unstable" filter can produce an output that grows without bounds, with bounded or even zero input.

- A "finite impulse response" (FIR) filter uses only the input signals, while an "infinite impulse response" filter (IIR) uses both the input signal and previous samples of the output signal. FIR filters are always stable, while IIR filters may be unstable.

A filter can be represented by a block diagram, which can then be used to derive a sample processing algorithm to implement the filter with hardware instructions. A filter may also be described as a difference equation, a collection of zeroesand poles or, if it is an FIR filter, an impulse response or step response.

The output of a linear digital filter to any given input may be calculated by convolving the input signal with the impulse response.

➢ Frequency domain

Signals are converted from time or space domain to the frequency domain usually through the Fourier transform. The Fourier transform converts the signal information to a magnitude and phase component of each frequency. Often the Fourier transform is converted to the power spectrum, which is the magnitude of each frequency component squared.

The most common purpose for analysis of signals in the frequency domain is analysis of signal properties. The engineer can study the spectrum to determine which frequencies are present in the input signal and which are missing.

In addition to frequency information, phase information is often needed. This can be obtained from the Fourier transform. With some applications, how the phase varies with frequency can be a significant consideration.

Filtering, particularly in non-real time work can also be achieved by converting to the frequency domain, applying the filter and then converting back to the time domain. This is a fast, O(n log n) operation, and can give essentially any filter shape including excellent approximations to brick wall filters.

There are some commonly used frequency domain transformations. For example, the cestrum converts a signal to the frequency domain through Fourier transform, takes the logarithm, then applies another Fourier transform. This emphasizes the harmonic structure of the original spectrum.

Frequency domain analysis is also called *spectrum-* or *spectral analysis*.

➢ Z-plane analysis:

Whereas analog filters are usually analyzed in terms of transfer functions in the s plane using Laplace transforms, digital filters are analyzed in the z plane in terms of Z-transforms. A digital filter may be described in the z plane by its characteristic collection of zeroes and poles. The z plane provides a means for mapping digital frequency (samples/second) to real and imaginary z components, where for continuous periodic signals and (is the digital frequency). This is useful for providing a visualization of the frequency response of a digital system or signal.

➢ Wavelet:

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time).

3.2.4 signal

A signal as referred to in communication systems, signal processing, and electrical engineering is a function that "conveys information about the behavior or attributes of some phenomenon".[1] In the physical world, any quantity exhibiting variation in time or variation in space (such as an image) is potentially a signal that might provide information on the status of a physical system, or convey a message between observers, among other possibilities.[2] The *IEEE Transactions on Signal Processing* states that the term "signal" includes[3] audio, video, speech, image, communication, geophysical, sonar, radar, medical and musical signals.

➢ Classification of Signals

Some important classifications of signals

- **Analog vs. Digital signals**: as stated in the previous lecture, a signal with a magnitude that may take any real value in a specific range is called an analog signal while a signal with amplitude that takes only a finite number of values is called a digital signal.
- **Continuous-time vs. discrete-time signals**: continuous-time signals may be analog or digital signals such that their magnitudes are defined for all values of t, while discrete-time

signal are analog or digital signals with magnitudes that are defined at specific instants of time only and are undefined for other time instants.

- **Periodic vs. aperiodic signals**: periodic signals are those that are constructed from a specific shape that repeats regularly after a specific amount of time T_0, [i.e., a periodic signal $f(t)$ with period T_0 satisfies $f(t) = f(t+nT_0)$ for all integer values of n], while aperiodic signals do not repeat regularly.
- **Deterministic vs. probabilistic signals**: deterministic signals are those that can be computed beforehand at any instant of time while a probabilistic signal is one that is random and cannot be determined beforehand.
- **Energy vs. Power signals**: as described below.

Energy and Power Signals

The total energy contained in and average power provided by a signal $f(t)$ (which is a function of time) are defined as

$$E_f = \int_{-\infty}^{\infty} |f(t)|^2 \, dt ,$$

And

$$P_f = \lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{T/2} |f(t)|^2 \, dt ,$$

Respectively.

For periodic signals, the power P can be computed using a simpler form based on the periodicity of the signal as

$$P_{Periodic\ f} = \frac{1}{T} \int_{t_0}^{T+t_0} |f(t)|^2 \, dt ,$$

where T here is the period of the signal and t_0 is an arbitrary time instant that is chosen to simply the computation of the integration (to reduce the functions you have to integrate over one period).

- **Classification of Signals into Power and Energy Signals**

Most signals can be classified into Energy signals or Power signals. A signal is classified into an energy or a power signal according to the following criteria

a)Energy Signals: an energy signal is a signal with finite energy and zero average power $(0 \leq E<\infty,\ P=0)$,

b)Power Signals: a power signal is a signal with infinite energy but finite average power $(0<P<\infty,\ E\rightarrow\infty)$.

3.2.5 SIGNAL PROCESSING

Signal processing is an enabling technology that encompasses the fundamental theory, applications, algorithms, and implementations of processing or transferring information contained in many different physical, symbolic, or abstract formats broadly designated as *signals*.[1] It uses mathematical, statistical, computational, heuristic, and linguistic representations, formalisms, and techniques for representation, modeling, analysis, synthesis, discovery, recovery, sensing, acquisition, extraction, learning, security, or forensics

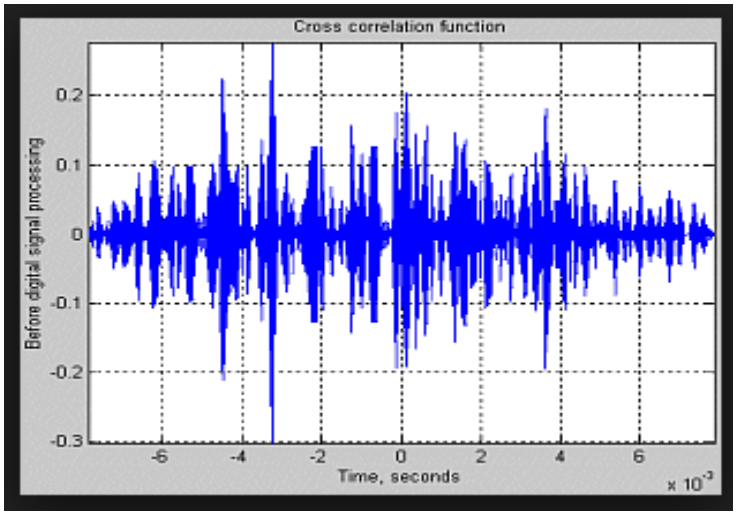


Figure 3.2:signal in time domain

3.2.5.1 Categories of signal processing

- **Analog signal processing**

Analog signal processing is for signals that have not been digitized, as in legacy radio, telephone, radar, and television systems. This involves linear electronic circuits as well as non-linear ones. The former are, for instance, passive filters,active filters, additive mixers, integrators and delay lines. Non-linear circuits include compandors, multiplicators (frequency mixers and voltage-controlled amplifiers), voltage-controlled filters, voltage-controlled oscillators and phase-locked loops.

- **Discrete-time signal processing**

Discrete-time signal processing is for sampled signals, defined only at discrete points in time, and as such are quantized in time, but not in magnitude.

Analog discrete-time signal processing is a technology based on electronic devices such as sample and hold circuits, analog time-division multiplexers, analog delay lines and analog feedback shift registers. This technology was a predecessor of digital signal processing (see below), and is still used in advanced processing of gigahertz signals.

The concept of discrete-time signal processing also refers to a theoretical discipline that establishes a mathematical basis for digital signal processing, without taking quantization error into consideration.

- **Nonlinear signal processing**

Nonlinear signal processing involves the analysis and processing of signals produced from nonlinear systems and can be in the time, frequency, or spatio-temporal domains. Nonlinear systems can produce highly complex behaviors including bifurcations, chaos, harmonics, and sub harmonics which cannot be produced or analyzed using linear methods.

3.2.6 DIGITAL SIGNALS

A digital signal refers to an electrical signal that is converted into a pattern of bits. Unlike an analog signal, which is a continuous signal that contains time-varying quantities, a digital signal has a discrete value at each sampling point. The precision of the signal is determined by how many samples are recorded per unit of time. For example, the illustration below shows an analog pattern (represented as the curve) alongside a digital pattern (represented as the discrete lines).

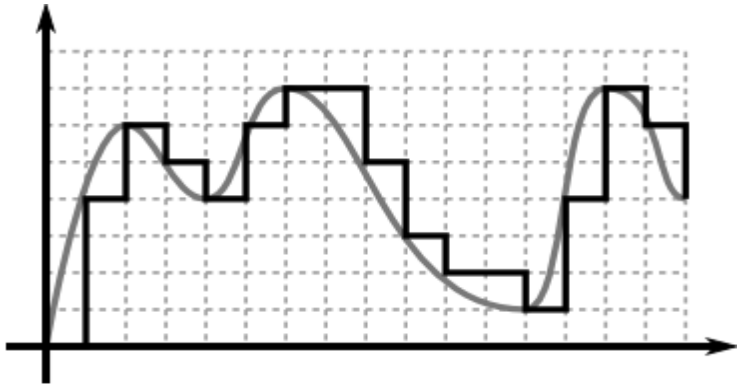


Figure 3.3: analog pattern (represented as the curve) alongside a digital pattern (represented as the discrete lines).

A digital signal is easily represented by a computer because each sample can be defined with a series of bits that are either in the state 1 (on) or 0 (off). Digital signals can be compressed and can include additional information for error correction.

3.2.7 SIGNAL FILE FORMATS

The **General Data Format for Biomedical Signals** is a scientific and medical data file format. The aim of GDF is to combine and integrate the best features of all biosignal file formats into a single file format.

The original GDF specification was introduced in 2005 as a new data format to overcome some of the limitations of the European Data Format for Biosignals (EDF). GDF was also designed to unify a number of file formats which had been designed for very specific applications (for example, in ECG research and EEG analysis). The original specification included a binary header, and used an event table. An updated specification (GDF v2) was released in 2011 and added fields for additional subject-specific information (gender, age, etc.) and utilized several standard codes for storing physical units and other properties.

The GDF format is often used in brain–computer interface research. However, since GDF provides a superset of features from many different file formats, it could be also used for many other domains. The free and open source software BioSig library provides implementations for reading and writing of GDF in GNU Octave/MATLAB and C/C++.A lightweight C++ library called libGDF is also available and implements version 2 of the GDF format. The binary nature of the meta-information might not be suitable for all applications.

The Extensible Data Format (XDF) is currently being developed with the aim of providing a flexible and extensible format for all kinds of data streams, but in particular for biosignal.3

3.2.8 SIGNAL COMPRESSION

In signal processing, data compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation. Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy . No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it. The process of reducing the size of a data file is referred to as data compression. In the context of data transmission, it is called source coding (encoding done at the source of the data before it is stored or transmitted) in opposition to channel coding. Compression is useful because it helps reduce resource usage, such as data storage space or transmission capacity. Because compressed data must be decompressed to use, this extra processing imposes computational or other costs through decompression; this situation is far from being a free lunch. Data compression is subject to a space–time complexity trade-off. For instance, a compression scheme for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage. The design of data compression schemes involves trade-offs among various factors, including the degree of compression, the amount of distortion introduced (when using lossy data compression), and the computational resources required to compress and decompress the data.

3.3 SIGNAL NOISE

signal processing, noise is a general term for unwanted (and, in general, unknown) modifications that a signal may suffer during capture, storage, transmission, processing, or conversion. Sometimes the word is also used to mean signals that are random (unpredictable) and carry no useful information; even if they are not interfering with other signals or may have been introduced intentionally, as in comfort noise.

Noise reduction, the recovery of the original signal from the noise-corrupted one, is a very common goal in the design of signal processing systems, especially filters. The mathematical

limits for noise removal are set by information theory, namely the Nyquist–Shannon sampling theorem.

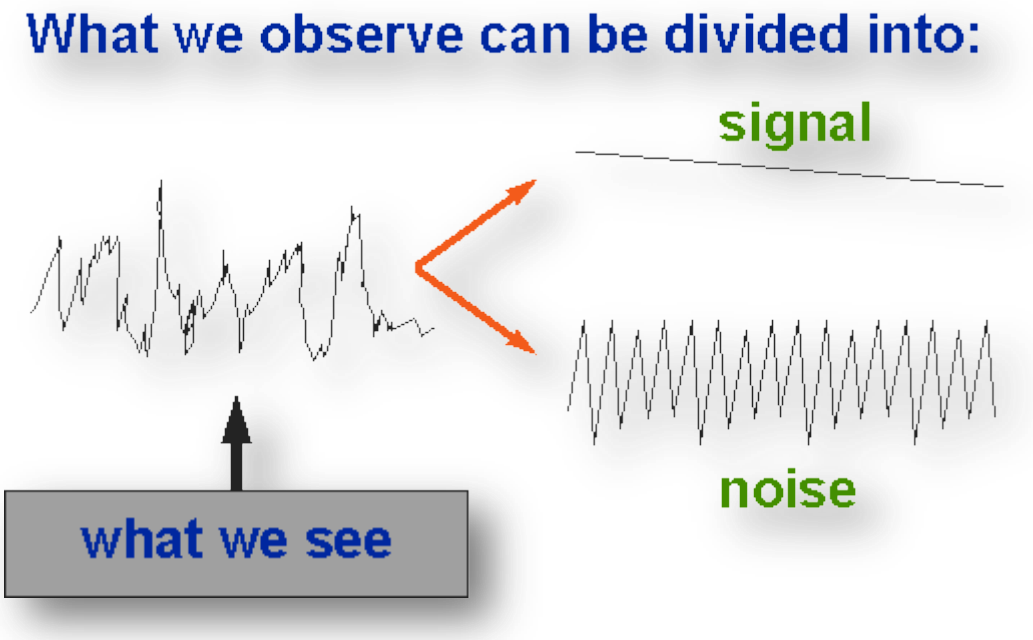


Figure 3.4:the signal and the noise

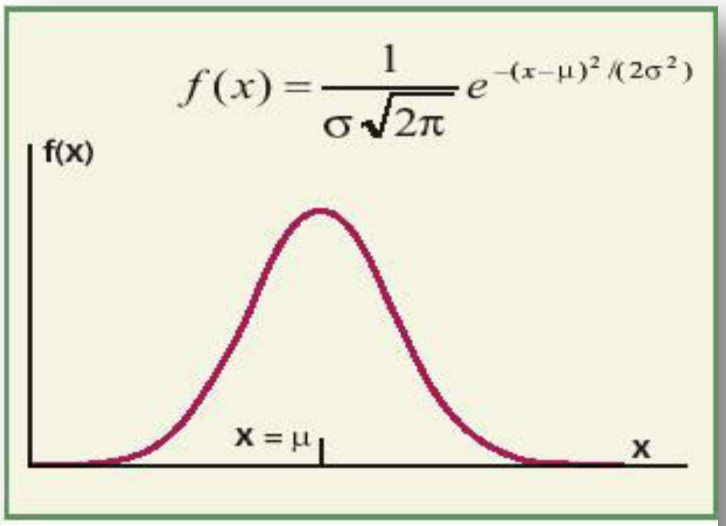
Signal processing noise can be classified by its statistical properties (sometimes called the "color" of the noise) and by how it modifies the intended signal:

➢ Additive white Gaussian noise (AWGN)

AWGN is a basic noise model used in Information theory to mimic the effect of many random processes that occur in nature. The modifiers denote specific characteristics:

- *Additive* because it is added to any noise that might be intrinsic to the information system.
- *White* refers to the idea that it has uniform power across the frequency band for the information system. It is an analogy to the color white which has uniform emissions at all frequencies in the visible spectrum.
- *Gaussian* because it has a normal distribution in the time domain with an average time domain value of zero.

Wideband noise comes from many natural sources, such as the thermal vibrations of atoms in conductors (referred to as thermal noise or Johnson-Nyquist noise), shot noise,black body radiation from the earth and other warm objects, and from celestial sources such as the Sun. The central limit theorem of probability theory indicates that the summation of many random processes will tend to have distribution called Gaussian or Normal.



1. Gaussian noise can be represented by a distribution of fluctuations about a mean.

Figure 3.5:Gaussian noise

- **Multiplicative noise**

In signal processing, the term multiplicative noise refers to an unwanted random signal that gets multiplied into some relevant signal during capture, transmission, or other processing.

An important example is the speckle noise commonly observed in radar imagery. Examples of multiplicative noise affecting digital photographs are proper shadows due to undulations on the surface of the imaged objects, shadows cast by complex objects like foliage and Venetian blinds, dark spots caused by dust in the lens or image sensor, and variations in the gain of individual elements of the image sensor array.

➢ Quantization error

Quantization, in mathematics and digital signal processing, is the process of mapping a large set of input values to a (countable) smaller set. Rounding and truncation are typical examples of quantization processes. Quantization is involved to some degree in nearly all digital signal processing, as the process of representing a signal in digital form ordinarily involves rounding. Quantization also forms the core of essentially all lossy compression algorithms. The difference between an input value and its quantized value (such as round-off error) is referred to as quantization error. A device or algorithmic function that performs quantization is called a quantizer. An analog-to-digital converter is an example of a quantizer.

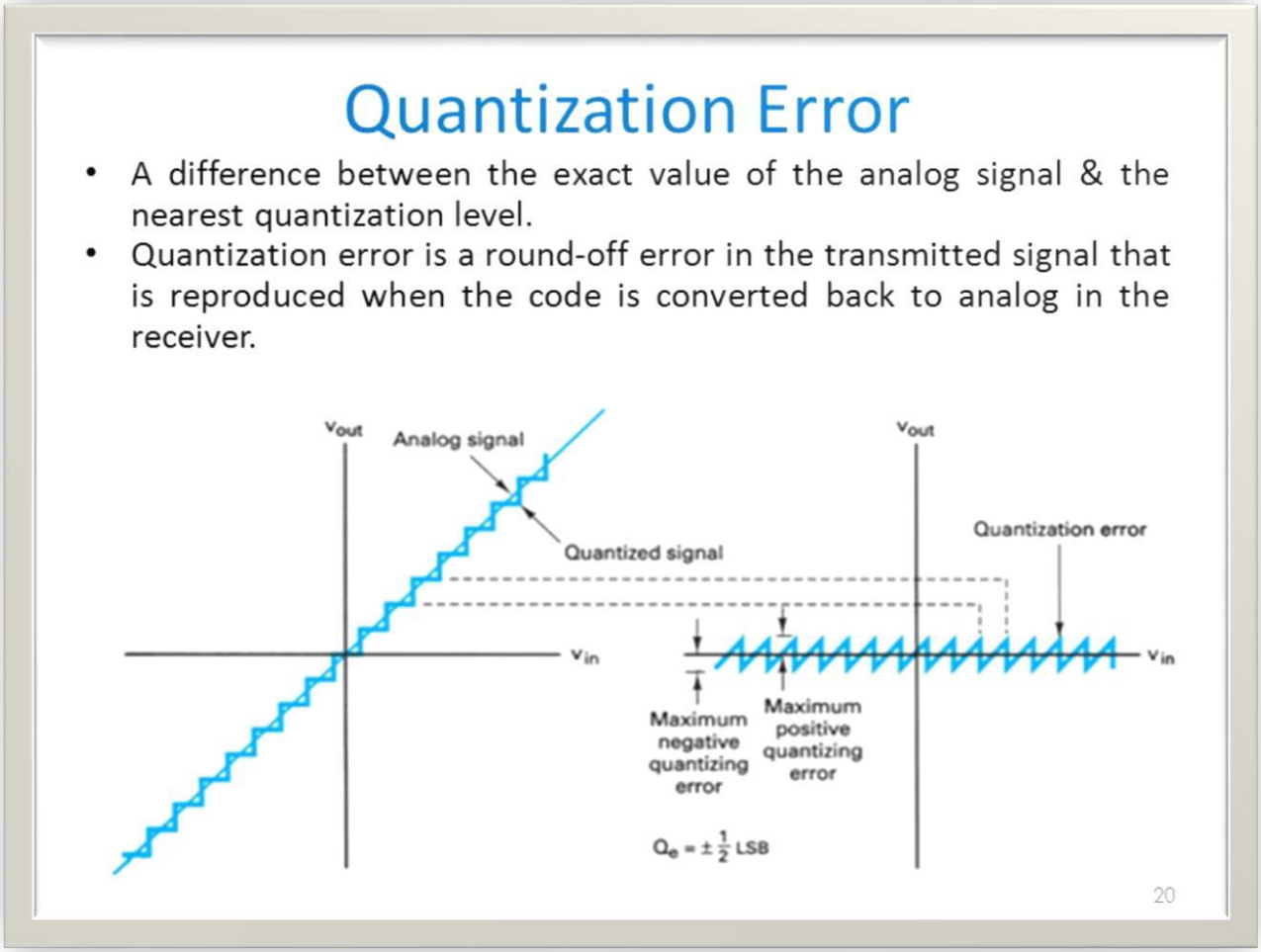


Figure 3.6:Quantization error

- **Shot noise**

Shot noise or Poisson noise is a type of electronic noise which can be modeled by a Poisson process. In electronics shot noise originates from the discrete nature of electric charge. Shot noise also occurs in photon counting in optical devices, where shot noise is associated with the particle nature of light.

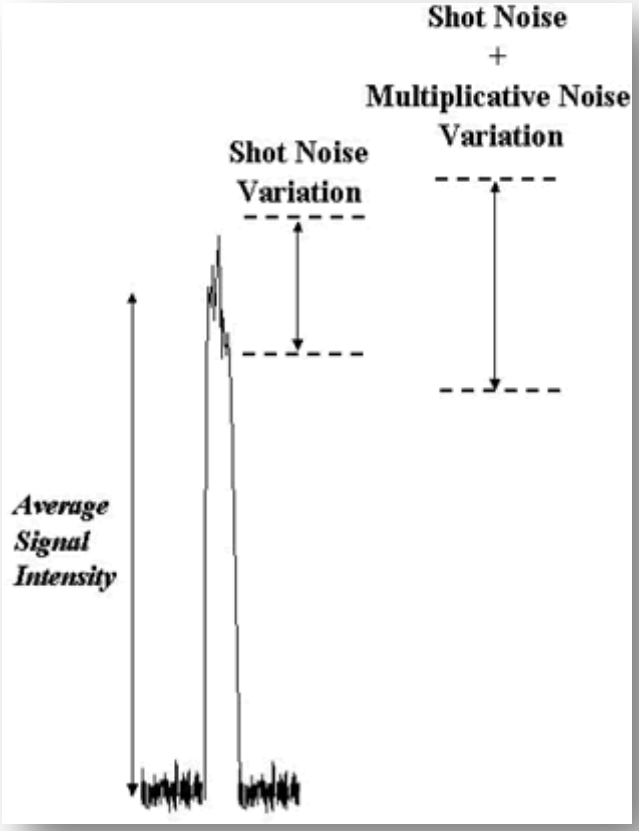


Figure 3.7: Shot noise and multiplicative noise

- **Phase noise**

In signal processing, phase noise is the frequency domain representation of rapid, short-term, random fluctuations in the phase of a waveform, caused by time domaininstabilities ("jitter"). Generally speaking, radio frequency engineers speak of the phase noise of an oscillator, whereas digital system engineers work with the jitter of a clock.

CHAPTER-5

5 . RESULTS

GUI output representation:

1. RUNNING CODE

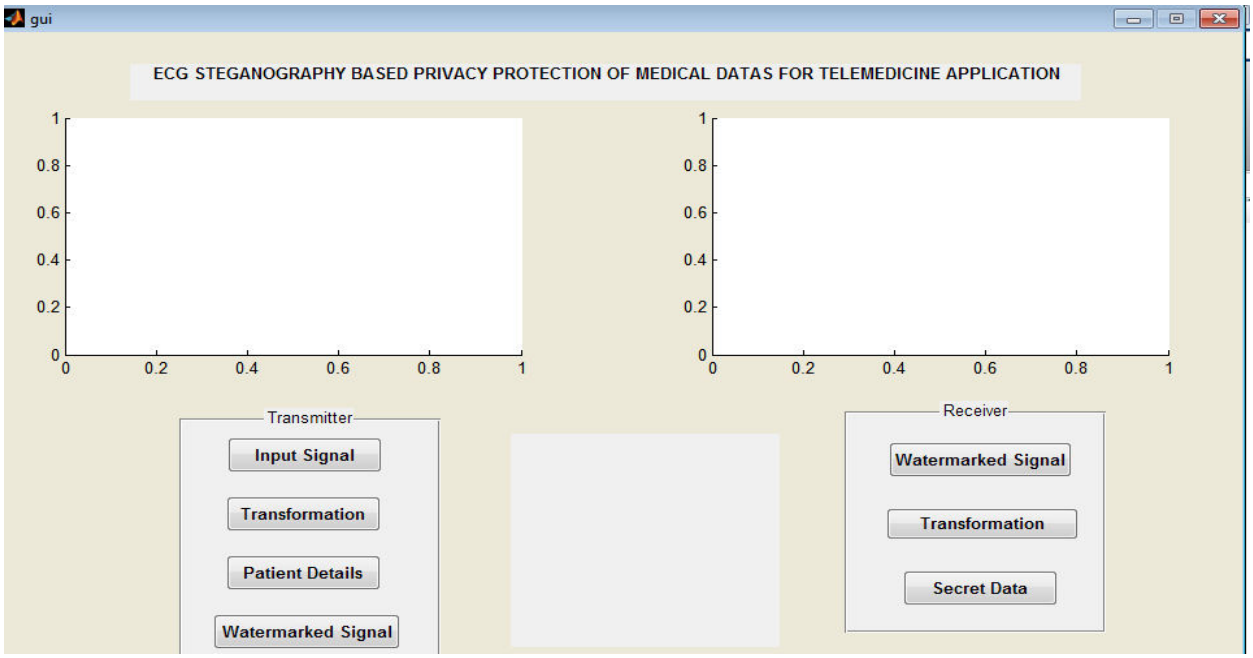


Figure 5.1: Running code

2. LOAD ECG SIGNAL

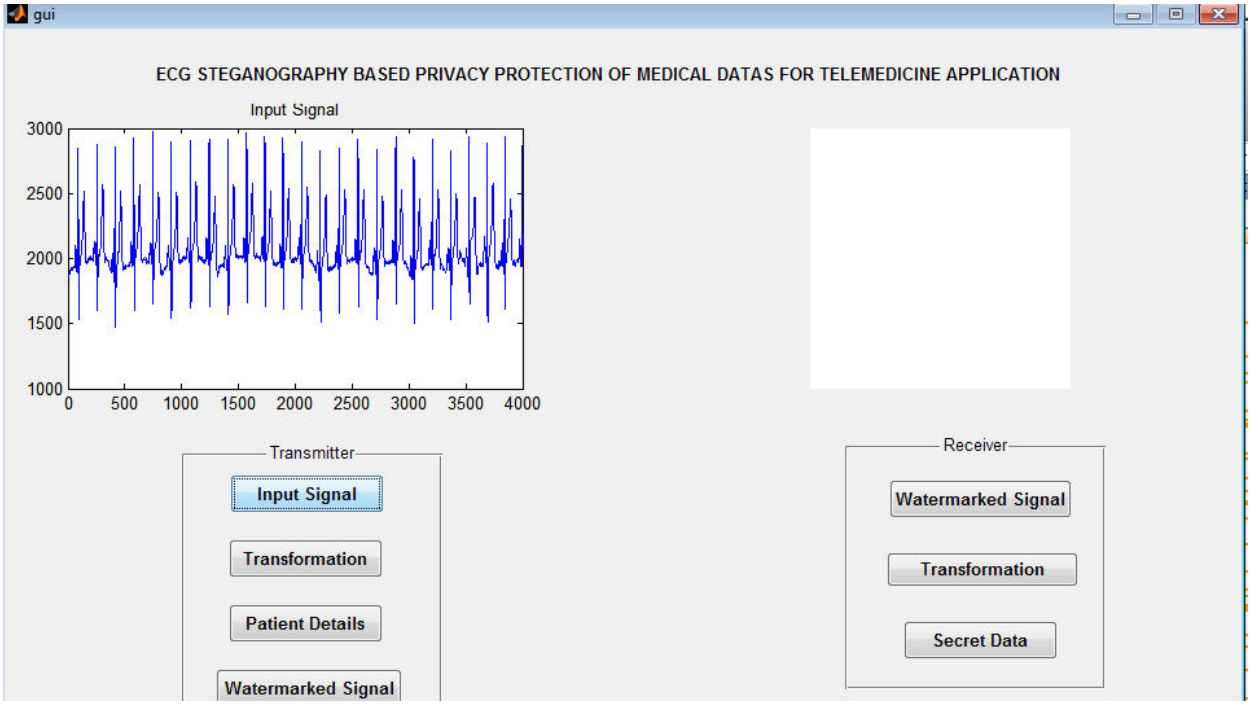


Figure 5.2 :Load the ECG signal

3. MULTILEVEL WAVELET DECOMPOSITION

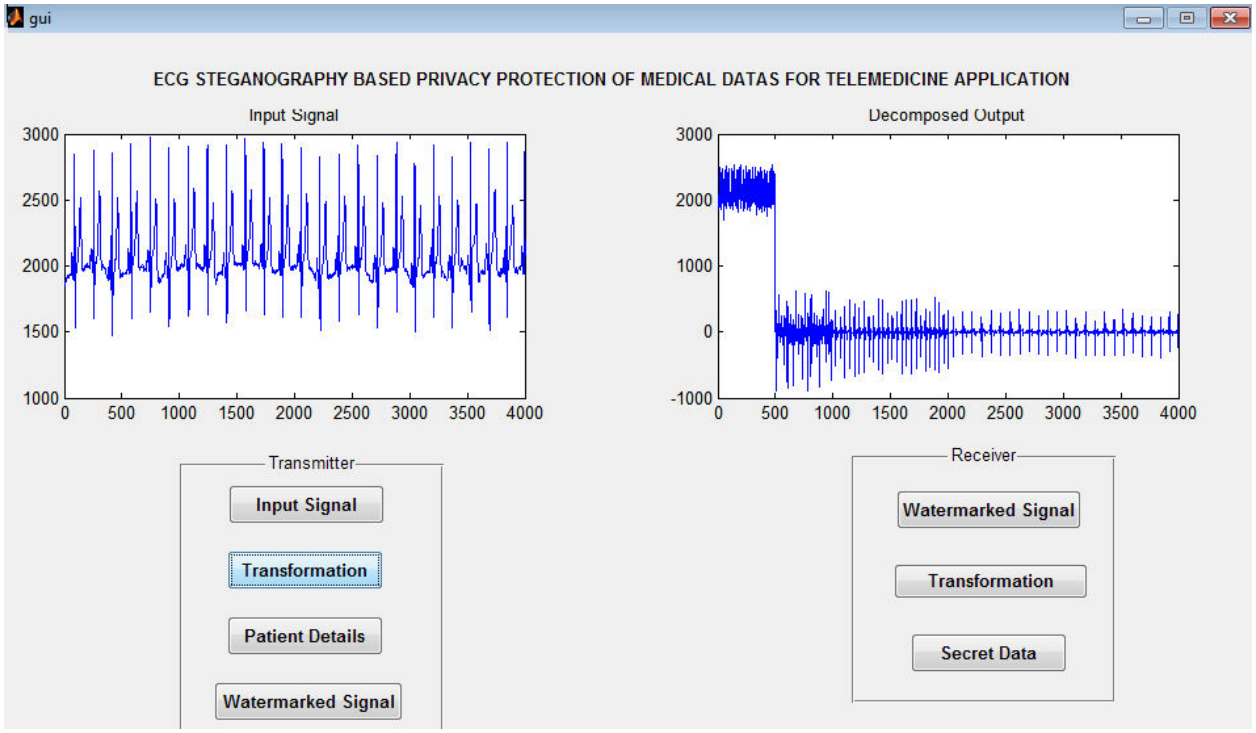


Figure 5.3:Multilevel wavelet decomposition

4. Embedded patient details in ECG signal

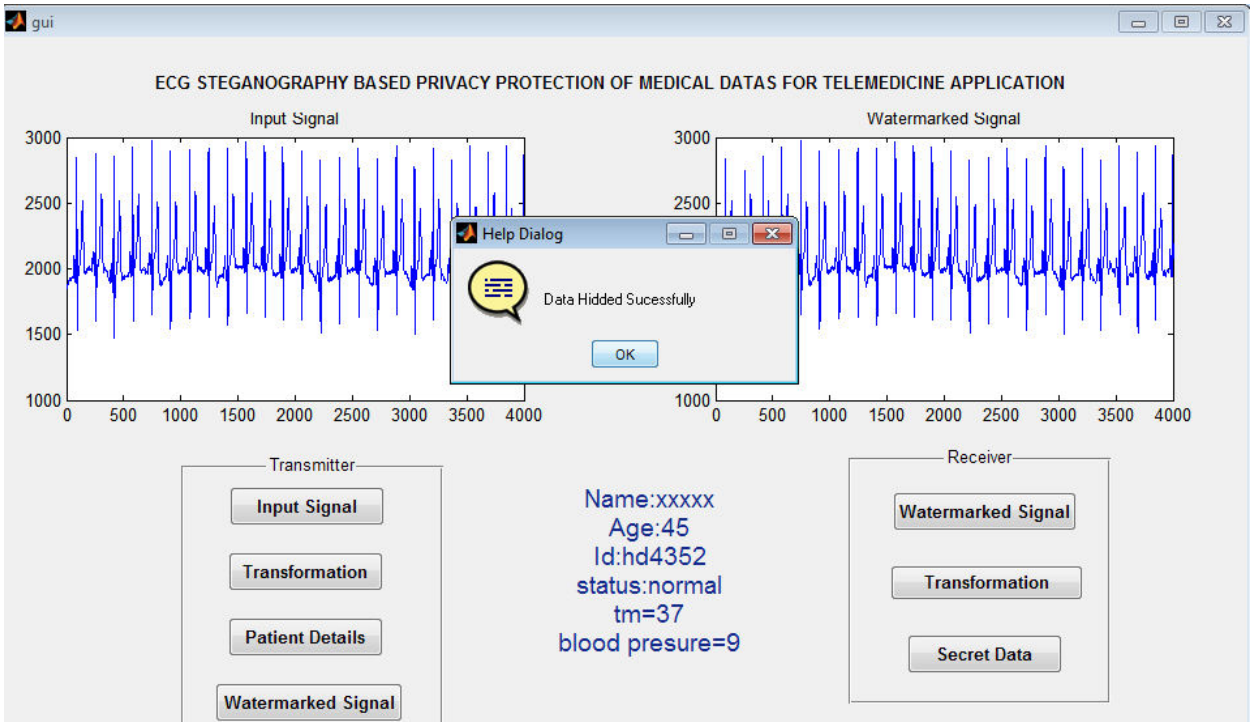


Figure 5.4:Embedded patient details in ECG signal

5. THE WATERMARKRD SIGNAL

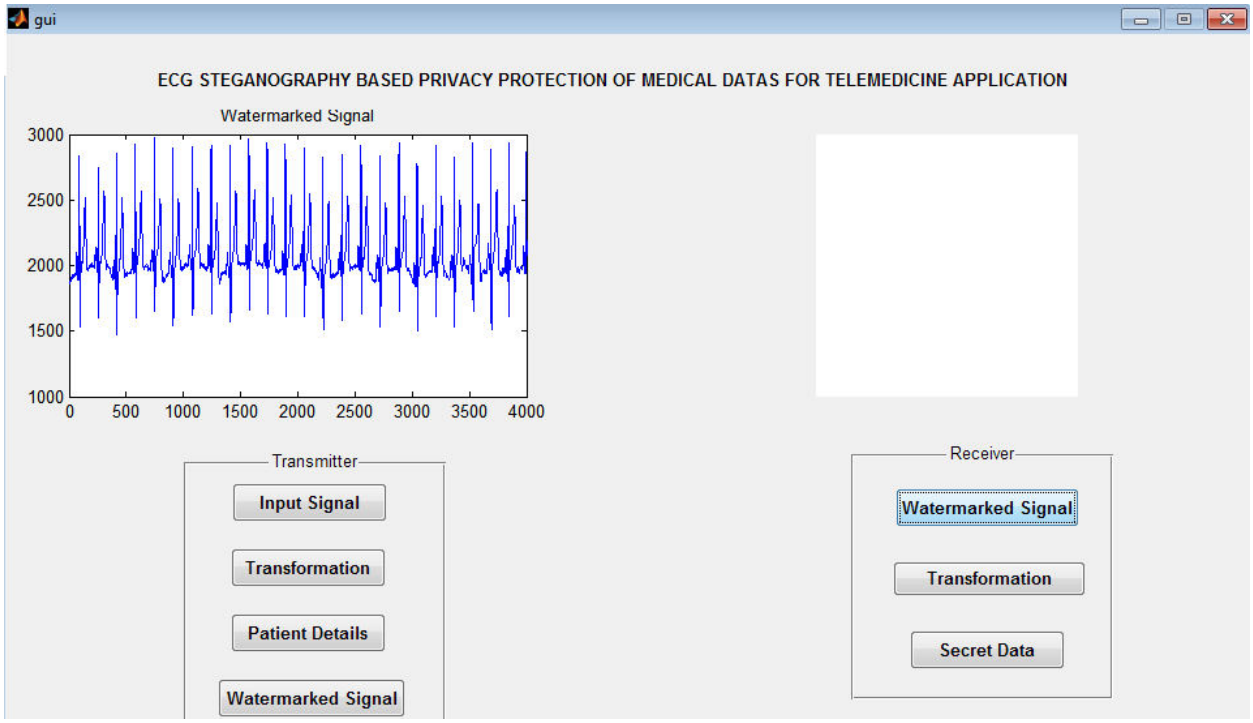


Figure 5.5:The Watermared signal

6. EXTRACTION PROCESS:

a.multilevel decomposition:

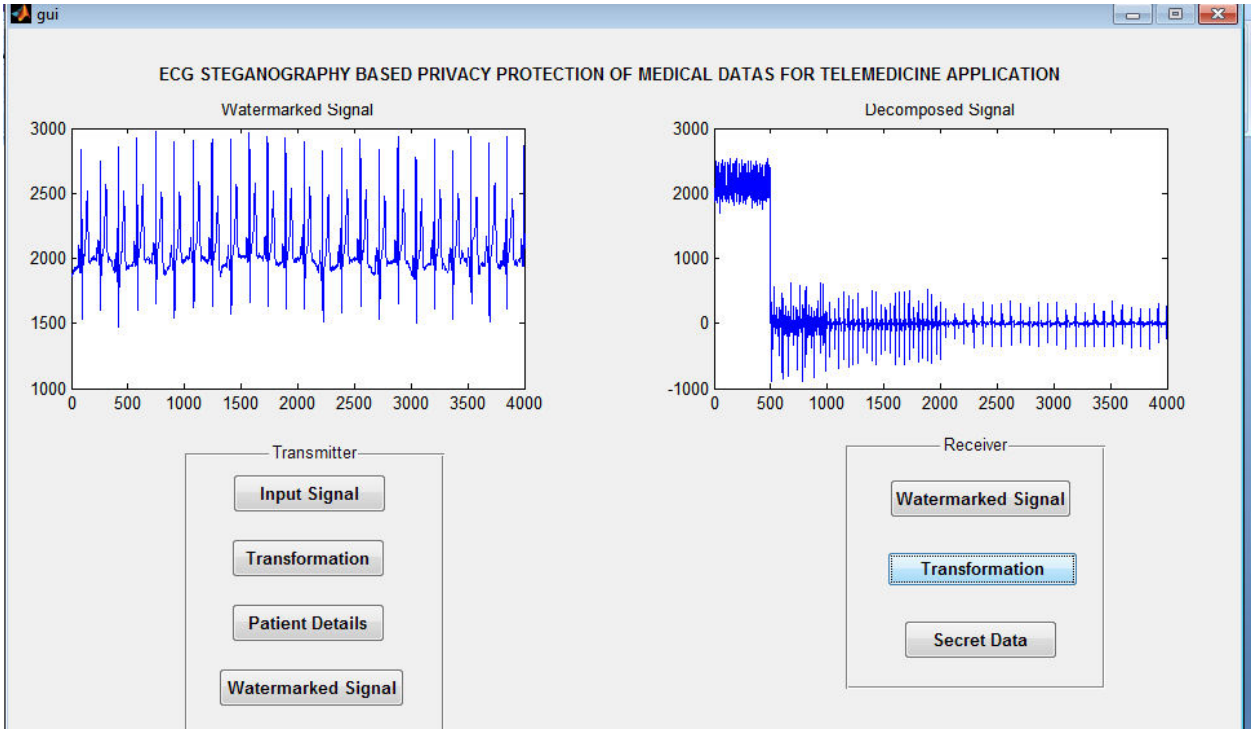


Figure 5.6: multilevel decomposition of the watermaked signal

b. Secret data extraction:

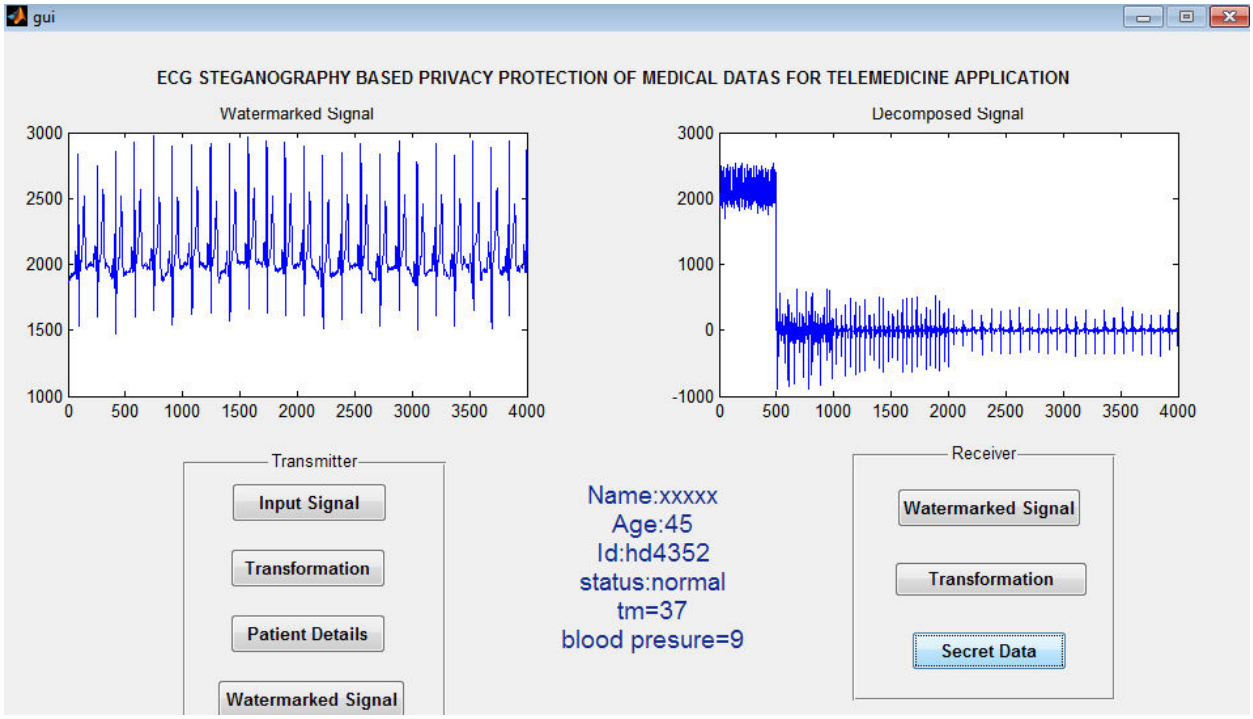


Figure 5.7 : secret data extraction

7.Performance values:

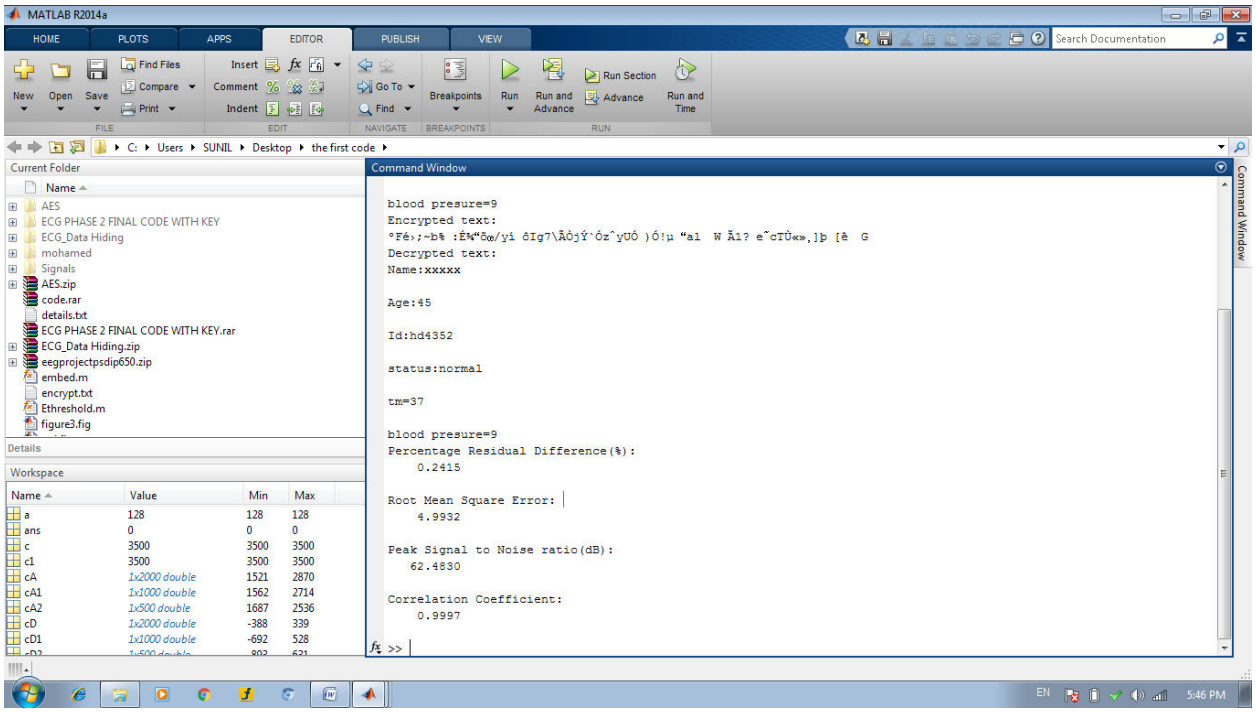


Figure 5.8: performance values (PRD,RMSE,PSNR AND CC)

CHAPTER-4

4.1 PROPOSED SYSTEM

The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised.

The proposed method presents the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the ECG signal coefficients. Finally, Signal and hidden text will be recovered without any loss based same methods which are used at embedding stage. In this paper, a wavelet based steg-anography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data. Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems.. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, some distortion measurement metrics have been used: the Percentage Residual Difference (PRD) , the root mean square error(RMSE), peak to peak signal to niose ratio(PSNR) and correlation coeffiecient.It is found that the proposed technique provides high security protection for patients data with low distortion and ECG data remains diagnosable after watermarking (i.e. hiding patient confidential data) and as well as after watermarks (i.e. hidden data) are removed from the watermarked data.

4.2 METHODOLOGY OF THE PROPOSED SYSTEM

The sender side of the proposed steganography technique consists of four integrated stages as shown in Fig(4.1). The proposed technique is designed to ensure secure information hiding with minimal distortion of the host signal. Moreover, this technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.

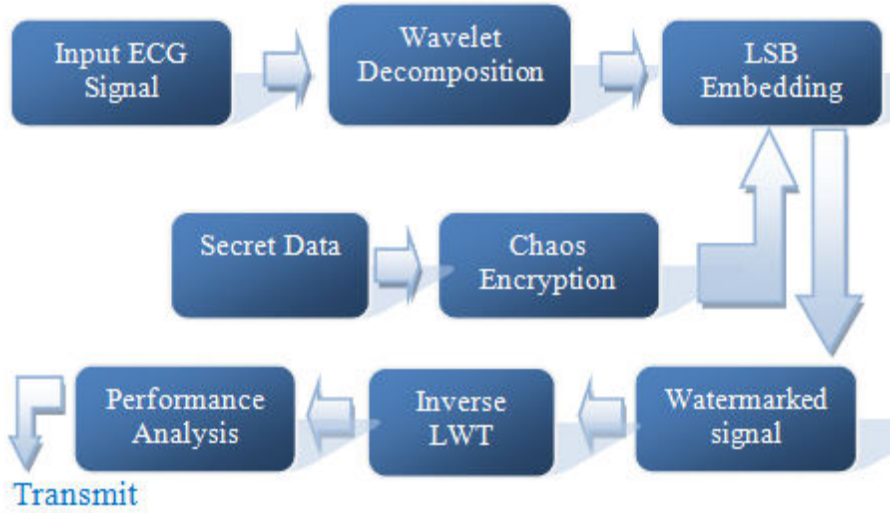


Figure 4.1 :block diagram of the sender steganography which includes ecryption,wavelet decomposition and secret data embedding.

4.2.1 ENCRYPTION

The process of transforming plain text to an unreadable format using a cipher is called encryption. Data Encryption is used to encrypt the confidential data to prevent any unauthorized access. Data Encryption is carried out before embedding of data into the signal to provide additional security. Various encryption techniques are available to encrypt the data but not all are possible to implement inside a smartphone due to computational limitations. The processors used on mobile devices are less capable than the ones used on a desktop system. Only few devices have the computational prowess to implement high-end encryption techniques..

- Chaotic map based text encryption

The aim of this stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons who does not have the shared key- from accessing patient

confidential data. In this stage XOR ciphering technique is used.It encrypts the original text data's with encryption key value generated from chaotic sequence with threshold function by bitxor operatio as shown in Fig 4.2 . XOR ciphering is selected because of its simplicity. As a result, XOR ciphering can be easily implemented inside a mobile device. Fig (4.3) shows an example of what information could be stored inside the ECG signal. Details are converted to ASCII codes and then encryption is applied. This techniques works on the following principles:

a) 0 + 0 = 0

b) 0 + 1 = 1

c) 1 + 0 = 1

d) 1 + 1 = 0

e) A + (B + C) = (A + B) + C

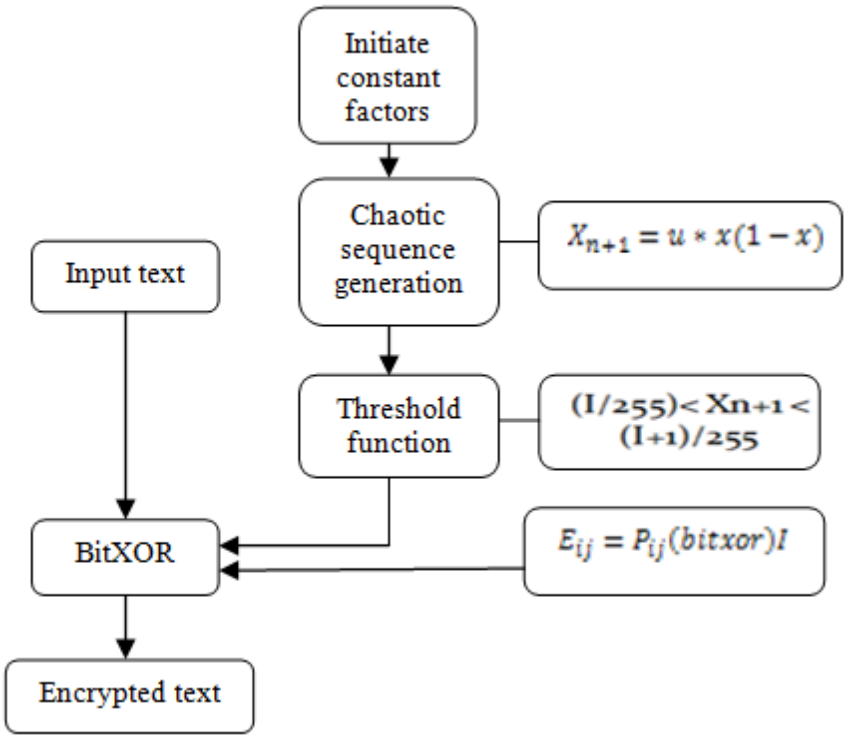


Figure 4.2:Block Diagram showing the detailed construction of the chaotic encryption operation

Figure 4.3: Original data consisting of patient information and sensor readings

4.2.2 WAVELET DECOMPOSITION

In order to hide the data we should convert the time domain signal into the frequency domain. The transformation of a signal is nothing but representing the signal in a different form. There is no change in the information inside the signal.

For the correct analysis it takes multistage wavelet decomposition. The fig(4.4) shows „h" is low-pass filter, „g" is high-pass filter, and „↓2 "is down sampling. Wavelet transform is a process that decomposes the given signal into high frequency and low frequency coefficients. Wavelet transform can be definedas shown in Eq 1

$$C(S,P)= \int_{-\infty}^{\infty} f(t)\Psi(S,P)dt \qquad (1)$$

where Ψ represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters . Wavelet transform is a powerful tool to combine time domain with frequency domain in one transform. In most applications discrete signals are used.

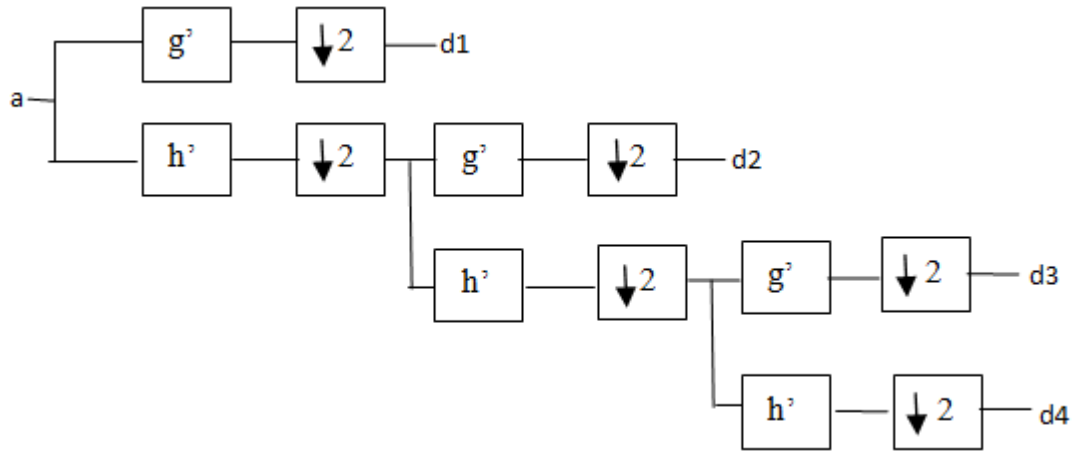


Figure 4.4 :Multilevel decomposition

The Wim Sweldens developed the lifting scheme for the construction of biorthogonal wavelets. The main feature of the lifting scheme is that all constructions are derived in the spatial domain. It does not require complex mathematical calculations that are required in traditional methods. Lifting scheme is simplest and efficient algorithm to calculate wavelet transforms. It does not depend on Fourier transforms. Lifting scheme is used to generate second-generation wavelets, which are not necessarily translation and dilation of one particular function.Digital signals are usually a sequence of integer numbers, while wavelet transforms result in floating point numbers. For an efficient reversible implementation, it is of great importance to have a transform algorithm that converts integers to integers. Fortunately, a lifting step can be modified to operate on integers, while preserving the reversibility. Thus, the lifting scheme became a method to implement reversible integer wavelet transforms.

We have used lifting scheme of wavelet transform because lifting scheme is having following advantages over conventional wavelet transform technique.It allows a faster implementation of the wavelet transform. It requires half number of computations as compare to traditional convolution based discrete wavelet transform. This is very attractive for real time low power applications**.** In each decomposition iteration the original signal is divided into two signals. Moreover, the frequency spectrum is distributed on these two signal. Therefore, one of the resulting signals will represent the high frequency component and the other one represents the low frequency component. Most of the important features of the ECG signal are related to the

low frequency signal. Therefore, this signal is called the approximation signal (A). On the other hand, the high frequency signal represents mostly the noise part of the ECG signal and is called detailsignal (D). As a result, a small number of the sub-bands will be highly correlated with the important ECG features while the other sub bands will be correlated with the noise components in the original ECG signal . Therefore, in our proposed technique different number of bits will be changed in each wavelet coefficient (usually called steganography level) based on its sub-band. As a result, a different steganography level will be selected for each band in such a way that guarantees the minimal distortion of the important features for the host ECG signal. The process of steganography levels selection was performed by applying lot of experimentation . Accordingly it is clear that, hiding data in some sub-bands will highly affect the original signal, while hiding in other sub-bands would result in small distortion effect.

4.3.3 WATERMARK EMBEDDING PROCESS

Watermarking is the process that embeds data called a watermark into an image or audio or video]. The watermark can be detected and extracted later from the carrier (cover). It can contain information such as copyright, license, authorship etc. Any watermarking algorithm consists of three parts:

a) The watermark, which is unique to the owner.
b) The encoder for embedding the watermark into the data.
c) The decoder for extraction and verification

At this stage the proposed technique will use a special security implementation to ensure high data security. Encrypted data is hidden onto the ECG signal via LSB embedding.

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. A detailed coefficients obtained from wavelet domain are used here for concealment process and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first bit selected coefficient and the second bit of message is embedded into the second bit location and so on. The resultant watermarked signal which holds the secret message with original form and difference between the input signal and the watermarked signal is not visually perceptible.

The embedding algorithm

1: cip : the cipher text
2: r : number of rows of det matrix

```
3: c : number of columns of det matrix
4: len : length of the cipher text
5: CH1&CH2 : 2 successive detailed coefficients
6: a threshold 240 is taken
7: det : detailed coefficients
8: det2 :embedded coefficients
9: embed(CH1,CH2,txt)
10: CH1←bitand(CH1,240)
11: CH2←bitand(CH2,240)
12: if bitand(txt,128)= =128
13: CH1←bitor(CH1,8)
14: end
15: if bitand(txt,64)= =64
16: CH1←bitor(CH1,4)
17: end
18: if bitand(txt,32)= =32
19: CH1←bitor(CH1,2)
20: end
21: if bitand(txt,16)= =16
22: CH1←bitor(CH1,1)
23: end
24: if bitand(txt,8)= =8
25: CH2←bitor(CH2,8)
26: end
27: if bitand(txt,4)= =4
28: CH2←bitor(CH2,4)
29: end
30: if bitand(txt,2)= =2
31: CH2←bitor(CH2,2)
32: end
33: if bitand(txt,1)= =1
34: CH2←bitor(CH2,1)
35: end 36: end
37: j ←1
38: for i=1 to len do
39: CH1←det[j]:detailed coefficient before
40: CH2←det[j+1] :successive detailed coefficient before embedding
41: txt ←cip(i)
42: call embed(CH1,CH2,txt)
43: det(j) ←CH1 :coefficient after embedding
44: det(j+1) ←CH2 :coefficient after embedding
45: increment j
46: end
47: det2 ←[rD,rD1,rD2]
48: Rs3 ←wavelet re-composition(det2)
```

4.3.4 INVERSE WAVELET RE COMPOSITION

In this final stage, the resultant watermarked sub-bands are recomposed using inverse wavelet packet re-composition. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal.

4.3.5 EXTRACTION PROCESS

the extraction starts by extracting the secret bits in the correct order from the LSB .Finally ,the extracted bits are decrypted. The extraction process is almost similar to the embedding process except that instead of changing the bits of the selected coefficients, it is required to read values of the bits in the selected coefficients, and then resetting them to zero.

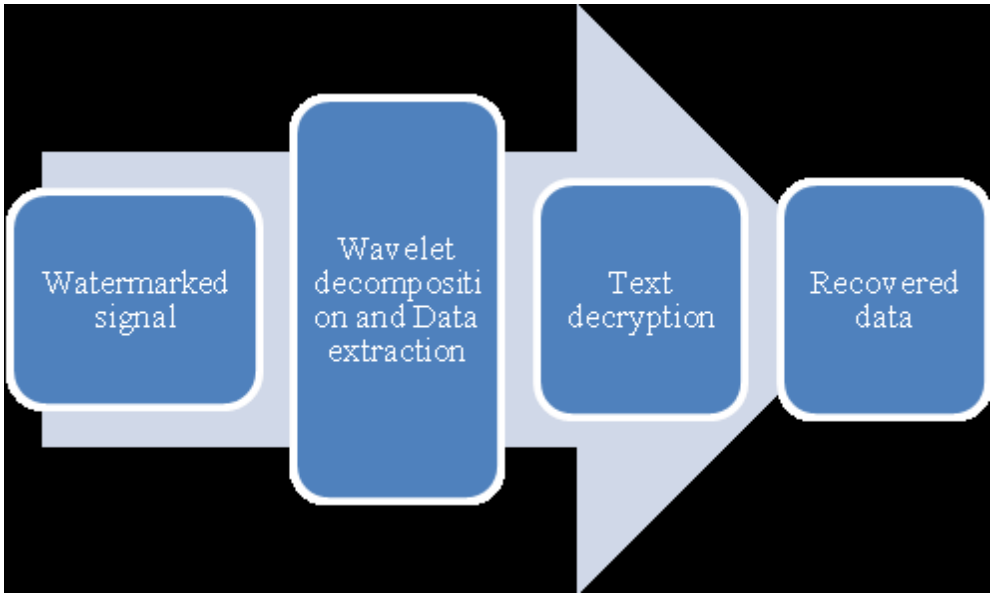


Figure4.5:Block diagram of the receiver steganography which includes wavelet decomposition ,extraction and decryption

CHAPTER-6

6.1 PERFORMANCE ANALYSIS

Remote healthcare monitoring and Point of Care (PoC) based systems are widely used for managing diagnostic information of patients. These systems introduce many threats such as privacy, security data integrity, reliability, accuracy, etc. issues. In this paper, a new technique is introduced for solving the problem of privacy and security issues. In this chapter,we evaluate the performance of the method. In this paper, three different types of ECG signals are used for experimentation.

6.1.1 percentage residual difference(PRD)

To evaluate the proposed model, the PRD (percentage residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal .The PRD is given by:-

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=0}^{N}(x_i - y_i)^2}{\sum_{i=0}^{N} x^2}}$$

Where x represents the original ECG signal, and y is the watermarked signal.

6.1.2 ROOT MEAN SQUARE ERROR(RMSE)

Root-mean-square error (RMSE) is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed. The RMSE represents the sample standard deviation of the differences between predicted values and observed values. These individual differences are called residuals when the calculations are performed over the data sample that was used for estimation, and are called prediction errors when computed out-of-sample. The RMSD serves to aggregate the magnitudes of the errors in predictions for various times into a single measure of predictive power. RMSD is a good measure of accuracy, but only to compare forecasting errors of different models for a particular variable and not between variables, as it is scale-dependent.

The RMSD of an estimator $\hat{\theta}$ (unwatermarked ECG)with respect to an estimated parameter θ (watermarked ECG)is defined as the square root of the mean square error:

$$\mathrm{RMSD}(\hat{\theta}) = \sqrt{\mathrm{MSE}(\hat{\theta})} = \sqrt{\mathrm{E}((\hat{\theta} - \theta)^2)}.$$

6.1.3 correlation coefficient (COR-COF)

A correlation coefficient is a coefficient that illustrates a quantitative measure of some type of correlation and dependence, meaning statistical relationships between two or more random variables or observed data values.

The mathematical formula for computing **r** is:

$$r = \frac{n\sum xy - \left(\sum x\right)\left(\sum y\right)}{\sqrt{n\left(\sum x^2\right) - \left(\sum x\right)^2}\sqrt{n\left(\sum y^2\right) - \left(\sum y\right)^2}}$$

where *n* is the number of pairs of data. Where x represents the original ECG signal, and y is the watermarked signal.

6.1.4 peak signal-to –noise ratio(PSNR)

Peak signal-to-noise ratio, often abbreviated **PSNR**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

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*, *MSE* is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

6.2 Evaluation

In this section ,we evaluate the performance of the proposed method. In this paper, three different types of ECG signals are used for experimentation. A tested of 4 ECG samples is used for experimentation. The set of samples consist of (2) normal (NSR) ECG samples, (1) Ventricular fibrillation ECG samples and (1)Ventricular Tachycardia ECG samples. . Each sample is 10 seconds long with 250 Hz sampling frequency. To evaluate the proposed model, the PRD (percentage residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal. To validate diagnosability of the digitally processed ECGs 4 ECG Segments for both normal and abnormal cases are used,as shown in the tables:

TABLE I: performance analysis for normal ecg of the proposed methods

Sample no.	PRD	RMSE	PSNR	COR –COF
1	0.2415	4.9932	62.4830	0.9997
2	0.2452	5.0611	63.6887	0.9996

TABLEII: performance analysis for abnormal ecg of the proposed methods

Sample no.	PRD	RMSE	PSNR	COR –COF
1(VT)	0.2456	5.0638	62.6526	0.9995
2(VF)	0.1923	4.1105	64.6827	0.9999

Finally, these tables shows the PRD measured after extracting the watermark. It is obvious from the tables that removal of the watermark will have a small impact on the PRD value. As a result, the ECG signal can still be used for diagnoses purposes after removing the watermark.

CHAPTER-7

7.1 CONCLUSION

This paper discusses an innovative idea using the CHOAS encryption to encrypted confidential data . A novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. this algorithm can be used to hide confidential data inside the ECG signal. The suggested technique provides an authentication technique to prevent unauthorized persons from gaining access to the confidential data. Thus this algorithm can be used for secure transmission in cardiac monitoring systems and also for storage of patient information in the cloud. It can also be used for secure transmission of user identification data for validation using biometric wrist bands where data privacy is critical. The proposed technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal. A 3-level wavelet decomposition is applied. In this paper we tested the diagnoses quality distortion. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

7.2 FUTURE WORK

ECG Steganography provides secured transmission of secret information such as patient personal information through ECG signals. In future work we suggest an approach that uses discrete wavelet transform to decompose signals and singular value decomposition (SVD) to embed the secret information into the decomposed ECG signal. The novelty of the suggested method is to embed the watermark using SVD into the two dimensional (2D) ECG image. The embedding of secret information in a selected sub band of the decomposed ECG is achieved by replacing the singular values of the decomposed cover image by the singular values of the secret data. The performance assessment of the proposed approach allows understanding the suitable sub-band to hide secret data and the signal degradation that will affect diagnosability. Performance is measured using metrics like Kullback---Leibler divergence (KL), percentage residual difference (PRD), peak signal to noise ratio (PSNR) and bit error rate (BER). A dynamic location selection approach for embedding the singular values is also discussed. The suggested approach is demonstrated on a MIT-BIH database and the observations validate that HH is the ideal sub-band to hide data. This method gives the higher security compared to all others previous algorithms

7.3 REFERENCES

[1] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments. ACM, 2007, p. 12.

[2] J. C. Lin, "Applying telecommunication technology to health care delivery," IEEE Eng. Med. Biol. Mag., vol. 18, no. 4, pp. 28–31, Jul./Aug. 1999.

[3] D. Hailey, R. Roine, and A. Ohinmaa, "Systematic review of evidence for the benefits of telemedicine," J. Telemed. Telecare, vol. 8, pp. 1–7, 2002.

[4] K. Zheng and X. Qian, "Reversible Data Hiding forElectrocardiogram Signal Based on Wavelet Transforms," in International Conference on Computational Intelligence and Security, 2008. CIS'08, vol. 1, 2008.

[5] H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in IEEE International Symposium on Signal Processing and Information Technology (ISSPIT),2009. IEEE, 2010, pp. 31–36.

[6] I. Maglogiannis, "Design and implementation of a calibrated store and forward imaging system for teledermatology," J. Med. Syst., vol. 28, no.5, pp. 455–467, 2004.

[7] A. Kollmann, D. Hayn, J. Garcia, B. Rotman, P. Kastner, and G. Schreier, "Telemedicine framework for manufacturer independent remote pacemaker follow-up," in Proc. Comput. Cardiol., 2005, pp. 49–52.

[8] V. Traver, E. Monton, J. L. Bayo, J. M. Garcia, J. Hernandez, and S. Guillen, "Multiagent home telecare platform for patients with cardiac diseases," in Proc. Comput. Cardiol., 2003, pp. 117–120.

[9] A. De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich-Mariscal, "A security framework for xml schemas and documents for healthcare," in Bioinformatics and Biomedicine Workshops (BIBMW), 2012 IEEE International Conference on, 2012, pp. 782–789.

[10] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign," IEEE Transactions on Information Technology in Biomedicine,, vol. 11, no. 6, pp. 619–627, 2007.

[11] H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynezhad,"Resource-aware secure ecg healthcare monitoring through body sensor networks," Wireless Communications, IEEE, vol. 17, no. 1, pp. 12–19,2010.

[12] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, "Digital Watermarking of ECG Data for Secure Wireless Commuication," in 2010 International Conference on Recent Trends in Information, Telecommunication and Computing. IEEE, 2010, pp. 140–144.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, pp. 131–143, 2013.

[14] Standards for privacy of individually identifiable health information," Fed. Regist., vol. 67, pp. 53181–53273, 2002.

[15] G.M. Stevens, "A brief summary of the medical privacy rule," CRS Rep. Congr. 2003.

[16] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[17] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982.

[18] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[19] Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," IEEE Transactions on information technology in biomedicine, vol. 8, no. 4,pp. 439–447, 2004.

[20] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in 5th International Conference on Intelligent Sensors,Sensor Networks and Information Processing (ISSNIP), 2009. IEEE, 2010, pp. 207–212.

[21] W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," IEEE Transactions on Information Technology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.

[22] Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," IEEE Transactions on Information Technology in Biomedicine,, vol. 13, no. 6, pp. 946–954, 2009.

[23] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," IEEE Transactions on Image Processing, vol. 8, no. 8,pp. 1075–1083, 1999.

[24] D. Stinson, Cryptography: theory and practice. CRC press, 2006.

[25] A. Poularikas, Transforms and Applications Handbook. CRC, 2009.

[26] A. Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 1, 2006.