Network Modeling Analysis in Health Informatics and Bioinformatics (2018) 7:6
https://doi.org/10.1007/s13721-018-0169-x

REVIEW ARTICLE

# Applications of data hiding techniques in medical and healthcare systems: a survey

Hedieh Sajedi[1]

Received: 4 November 2017 / Revised: 12 April 2018 / Accepted: 19 April 2018 / Published online: 30 April 2018

## Abstract

Nowadays, scientists make effort to provide security for the communication channels. Several security and privacy threats are introduced via the Internet as the major communication channel. Therefore, information exchanging through the Internet should be protected and secured. Now healthcare systems are getting very common in the world. A health care system should preserve privacy while sending patients' information, prevent the patients' information from tampering, and prevent any sabotage in the healthcare systems. Therefore, it is crucial to provide security in such systems to attract the confidence of people for using the Internet (network)-based health care systems. In this respect, the goal of this paper is to review the accessories to provide security in healthcare systems. Our objective is to state the achievements of a literature review regarding the security of health care systems provided by information hiding methods including cryptography, steganography and watermarking methods. Furthermore, discussion about these methods, the media employed in these methods such as medical images and biomedical signals, their pros and cons and the applications in healthcare systems are provided. Correspondingly, we share the visions into the open research problems and highlight future directions in this extent.

**Keywords** Healthcare · Medical application · Security · Information hiding · Steganography · Watermarking

## 1 Introduction

During the recent years, telemedicine platforms provided significant tools for the improvement of patient treatment in remote areas (Lin 1999), reducing transport, accommodation, and medical personnel-related costs, and enabling a full time, 24×7 patient monitoring (Traver et al. 2003). In addition, computer-based emergency health care systems are expanding to support geographically isolated areas. Health monitoring can be used not only in the hospital environment but at home as well, through modern homecare tele-monitoring systems, providing better managing of care (Joseph and Remya 2014).

Over the years, health care has many progresses because of information and communication technology. Recently, these progresses and development of telecommunication have affected the health care vastly. Nowadays, physicians and medical professionals around the world provide electronic medical prescription and wireless media to exchange medical information. Many medical centers and hospitals also transmit medical data to/from other hospitals or medical centers to advance the diagnostic outcomes and communicate to study a therapeutic case (Chakraborty et al. 2013). Therefore, security and protection of patients' information needs special treatment.

In the previous and some current healthcare systems, there is the risk of intentionally or unintentionally manipulating data about patients, diagnosis, prescriptions, etc. An attacker could intentionally change the data related to the health of famous actors, politicians, entrepreneurs, writers, artists, and humanitarians. This may cause intervention in the improvement of the disease or in the worst-case death.

These days, scientists attempt to afford security for most of the communication channels such as Skype and Wi-Fi networks. For instance, the research on Mazurczyk et al. (2013) introduces the ways to hide messages in Skype calls, Wi-Fi networks, Bit Torrent, etc.; for example, silences in a telephone conversation can cover a great deal of meaning and concealed information (Mazurczyk et al. 2013).

✉ Hedieh Sajedi
hhsajedi@ut.ac.ir

[1] Department of Mathematics, Statistics and Computer Science, College of Science, University of Tehran, Tehran, Iran

Medical devices are the newest cases in the growing list of Internet of Things, which have the risk for potential hacks. Medical data (i.e., medical image, medical record etc.) are private which should be protected before being transferred or stored. Medical records of patients are sensitive information, needing security while they have been stored and transmitted. Additionally, these records often have to be traceable to patient medical data such as X-ray or scan images (Correa and Leber 2011). The definition of Security and Privacy in the healthcare is as follows (Vargheese et al. 2014):

- Security: Protection of healthcare data from unauthorized access during transport or in place.
- Privacy: Guarantee that only persons and/or entities authorized by the owner of the data owner (in most cases, the patient) can view and access the data.

At Black Hat cyber security conference in 2011, a diabetic man showed how a person could hack into a wireless insulin pump (Poremba 2015). It may seem almost foolish to worry about some strangers want to control a person's insulin dosage or shut off a pacemaker or manipulate health data; but we also wondered why anyone would want to hack a cloud storage to steal photos of actresses or someone would stage a major attack on an entertainment company in retaliation for a movie (Poremba 2015). Not considering the security, may expose medical devices, and the patients with a great risk.

Recently, based on the Food and Drug Administration's new guidelines, most of the vendors are instructed to build cyber security functionality into the new medical devices. The way of addressing the cyber security functions rely on the device itself, its use, general vulnerability issues, and threats to the patient. The guidelines list the cyber security functions that should be included, such as layered authentication and timed usage sessions that ensure the device is not connected to the network any longer than necessary (Poremba 2015).

In medical and healthcare systems, the data about a person may contain patient information, sensor readings and patient biometric information and so on. Some possible patients' information is shown in Table 1.

**Table 1** Some possible patients' information

| | |
|---|---|
| General information | Date of birth |
| | Address |
| | Age |
| | Height |
| | Weight |
| | … |
| Confidential information | Name |
| | Medicare number/ health record identifier |
| | Social security number |
| | Telephone number |
| | Patient location |
| | … |
| Diagnosis information | Blood pressure |
| | Glucose level |
| | Temperature |
| | ECG |
| | … |
| Biometric information | Finger signature |
| | Iris image |
| … | … |

The population of aging patients in the world is increasing due to the recent medical advancements. Consequently, to reduce the medical cost, using remote healthcare monitoring systems and point-of-care (PoC) technologies have become popular. Monitoring a patient at his location can decrease the traffic at medical centers. Additionally, PoC solutions can provide further reliability in emergency services as patient medical information (ex. for diagnosis) can be sent immediately to physicians and response or proper treatment can be done right away. However, remote health care systems are used in large geographical areas, basically for monitoring channel used to transport information.

Usually, patient biological signals and other physiological readings are collected using body sensors. Afterward, the collected data are sent to the patient electronic device for analysis or diagnoses. At last, the signals and patient confidential information along with a diagnostic report or any urgent alerts are forwarded to the medical center servers through the Internet. Doctors can check those biomedical signals and decide about the emergency cases (Edward Jero et al. 2014).

By increasing the number of older population and a significant portion of that suffering from cardiac diseases, it is imaginable that remote ECG patient monitoring systems are expected to be extensively used as PoC applications in hospitals. Therefore, the enormous amount of ECG signal collected by body sensor networks (BSNs) from remote patients at homes will be transmitted accompanied by other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by the remote patient-monitoring systems.

Using the Internet as the main communication channel may cause security and privacy threats. It is noteworthy that patient confidentiality be protected while data is being transmitted over the public network and also when the data is stored in medical center servers used by remote monitoring systems. The research of Hafizah Hassan and Ismail (2012) states that for complex information system in healthcare environment, the number of possible attacks is potentially very large.

Users of medical information systems require assurance in the security of the medical system they are using. In addition, a evaluation method is required to compare the security capabilities of medical systems. Each system has its specific requirements for preserving confidentiality, integrity, and availability. To provide these necessities several security functions should be considered to cover areas such as information hiding, access control, auditing, error recovery, etc. (Pangalosa 1993).

The EUROMED-ETS (Pangalosa 1993) pilot system in 1999 offered a number of security functionalities using off-the-shelf available products, to protect Web-based medical applications. The basic concept used by it was the trusted third party (TTP). A TTP was used to generate, distribute, and revoke digital certificates to medical practitioners and healthcare organizations that wish to communicate securely. Digital certificates and digital signatures were used to provide peer and data origin authentication and access control. The research of Gritzalis et al. (1999) demonstrated that how TTPs can be used to develop medical applications that run securely over the World Wide Web.

The study in Gritzalisa et al. (1991) analyses the results of a recent survey performed among medical establishment personnel in Greece, evaluates information security legislation existing in other countries. In addition, it includes guidelines of international societies to offer principles governing a future legal framework. Furthermore, Gritzalisa et al. (1991) presents an approach for designing secure information systems and provides an example of the use of this approach in designing a database oriented secure medical information system with access rights incorporated.

Although mobile devices are increasingly being used to provide health related information to healthcare related services on the Internet, but such devices have limited resources to enforce strong security measures and are easily vulnerable to attacks. In Tupakula and Varadharajan (2013), some techniques are presented for counteracting denial of service (DoS) attacks on mobile devices that are providing the user's health related information and for securing the communication between mobile nodes and healthcare service providers on the Internet. A DoS attack prevents access to resources by the legitimate users.

Evidence based medicine is emerging as a key process in health care to enable insights driven quality care for individual patients. The core of making evidence based medicine is information sharing between healthcare entities. However, the sharing of information across health care providers has security implications. The old methods of securing enterprises using perimeter defense models are likely to fall short; hence new innovative methods such as dynamic learning threat defense systems that perform rapid detection based on flow, signature, behavior, packet capturing techniques in addition to security policies and protection schemes are required to ensure security of the information exchanged as well as other threats to information and systems within the enterprise. Ensuring the confidentiality, integrity, and availability of the data is the foundation to enable such pervasive information sharing that is required for enabling evidence based care model to achieve better health outcomes (Varghese et al. 2014).

Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two subcategories. First, 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. On the other hand, some researches such as Calvillo et al. (2013) try to enhance the security through the access control mechanism. The second, security technique is hiding the sensitive information inside another insensitive host data without incurring any increase in the host data size and enormous computational overhead. These techniques are called steganography techniques. Digital steganography provides potential for private and secure communication that has become the necessity of most of the applications in today's world. A variety of multimedia carriers such as audio, text, video, and image can act as cover media to carry secret information (Ahmad 2014; Subhedara and Mankar 2014).

Most of the mentioned threats in healthcare systems is due to the plainness of the information that is communicated or the vividness of the cryptography algorithms which are employed to hide the content of the messages exchanged between the nodes of the network.

In this paper, we aim to survey all the published researches, which consider the security of the healthcare systems and medical applications by applying information hiding methods. We categorize these researches first based on the type of the used cover media and the second, based on the type of information hiding method. Our objective is to perform a systematic literature review (SLR) (Fernandez-Aleman et al. 2013) related to the security of medical and healthcare systems. The researches can be classified based on the applications, and the way of providing security. We will discuss about the advantages and disadvantages of each class and suggest the means for the feature systems.

We conclude from surveying the literature that, the recent years have witnessed the design of standards and the spread of directives concerning security and privacy of the patients' data. However, more attempts should be done to adopt these regulations and to deploy secure systems.

The organization of the paper is as the following. Section 2 describes the method of providing the survey. In Sect. 3, we review the researches, which used information hiding methods in medical science applications. In this section, the applications are grouped based on the type of the cover media and the employed information hiding method. In Sect. 4, we survey the methods for evaluating the employed information hiding methods and their outputs. Section 5 presents future of the data hiding techniques in medical science and provides a discussion and finally in Sect. 6 we conclude the paper.

## 2 Our method

In this section, different parts of the employed method to prepare the survey and the details of our exploring are presented.

### 2.1 Information source

To provide the survey, our data sources are articles written in English published in ACM, Wiley, IEEE, Elsevier, IOS Press, Taylor & Francis, Nature, InderScience and Springer Digital Library and our search was run between April 2015 and July 2015. We also scanned the reference lists included in the articles to ensure that this review would be more inclusive.

### 2.2 Systematic literature review

This article has used a systematic review to ensure that both the search and the retrieval process have been accurate and unbiased. A systematic review is defined as a technique that attempts to collect all empirical evidences in a specific field, to assess it critically and to obtain conclusions that summarize the research. The objective of an SLR is not only to collect all the empirical evidences of a research question, but also to support the development of guidelines, which can then be used by the professionals. This systematic review has followed the quality reporting guidelines set by the preferred reporting items for systematic reviews and meta-analysis (PRISMA) group (Liberati et al. 2009). A review protocol describing each step of the systematic review, including eligibility criteria, was developed before beginning the search for the literature and the data extraction.

### 2.3 Eligibility criteria

The following inclusion criteria were used: (1) articles that have been published in English and (2) articles those deal with the security and information hiding in medical and healthcare systems. The articles in English were considered because this language is favored by the scientific community in the publication of research studies.

### 2.4 Study selection

The study selection was organized in the following four phases:

1. The search for publications from electronic databases related to health and computer science. This step was performed by applying the following terms and operations: (“medical” OR “healthcare”) AND (“information hiding” OR “security”), which was adapted to the search engine of each digital library.
2. Exploration based on the title, abstract and keywords of the articles and selection based on the eligibility criteria.
3. Complete or partial reading of the articles that had not been omitted in the previous phase to determine whether they should be included in the review, according to the eligibility criteria.
4. Scanning the references of the articles to discover unseen studies which were then reviewed as indicated in Phases 2 and 3.

The study selection was developed in an iterative process of individual assessments.

### 2.5 Data collection process

Data collection was carried out using a data extraction form. Appeared articles were compared based on their titles. It was noticeable that, even though, different keywords have been used, some of the articles were duplicated. Therefore, we eliminated the copies. To identify the most relevant articles, the abstracts were considered by which 119 articles were selected. Each potentially relevant article was assessed by reading the full text. Afterward, our study selects only those articles dealing with the security of patients’ information endowed with information hiding methods. In data extraction, 69 articles were extracted using the predefined search string (which is defined in study selection) from 1990 to July 2015. The outcome was reviewed by the author. Finally, we found that only 29 articles have been used the information hiding methods for the purpose of privacy and security of patients’ data. Among these articles, 9 articles were about steganography and 14 articles employed watermarking techniques. The remaining is based on cryptography algorithms. Ten of these studies discuss about hiding information in ECG signals.

Table 2 shows the number of selected studies by the source of publication.

**Table 2** Number of selected studies, by the source of publication

| Source | Selected studies | Ref. no. |
|---|---|---|
| Journal of Biomedical Informatics | 1 | Sajedi and Jamzad (2009a, b) |
| IEEE Transaction on Biomedical Engineering | 1 | Traver et al. (2003) |
| IEEE Transactions on Information Technology on Biomedicine | 2 | Crichtona (2009), Kamal et al. (2017) |
| IEEE Transactions on Parallel and Distributed Systems | 1 | Fernandez-Aleman et al. (2013) |
| Journal of Visual Communication and Image Retrieval | 1 | Vleeschouwer et al. (2003) |
| Signal Processing | 1 | Zhou et al. (2001) |
| Journal of Medical Systems | 1 | Joseph and Remya (2014), Rubio et al. (2013) |
| Information Security Journal | 1 | Shapiro (1993) |
| Medical Informatics and the Internet in Medicine | 1 | Zhou et al. (2005) |
| Optik | 1 | Wang et al. ( 2010) |
| Journal of Dental and Medical Sciences | 1 | Vargheese et al. (2014) |
| Journal of Digital Imaging | 1 | Mazurczyk et al.( 2013) |
| Wireless Communications | 1 | Ahmad (2014) |
| International Journal of Engineering Research and Applications | 1 | Correa and Leber (2011) |
| IEEE International Conference on Engineering in Medicine and Biology Society | 2 | Lin (1999), Dao et al. (2015) |
| IEEE International Conference on Bioinformatics and Biomedicine Workshops | 1 | Tupakula and Varadharajan (2013) |
| IEEE International Symposium on Signal Processing and Information Technology | 1 | Gritzalisa et al. (1991) |
| IEEE International Conference on Computational Intelligence and Computing Research | 1 | Nambakhsh et al. (2006) |
| International Conference SPIE on Medical Imaging | 2 | Zehl et al. (2016), Istepanian and Petrosian (2000) |
| International Conference on Computational Intelligence and Security | 1 | Gritzalis et al. (1999) |
| International Conference on Computer, Control, Informatics and Its Applications | 1 | Li et al. (2013) |
| International Conference on Recent Trends in Information, Telecommunication and Computing | 1 | Subhedara and Mankar (2014) |

## 3 Past applications of data hiding techniques in medical science

The application of information technology to health care has grown concern about the privacy and security of medical information. Until now, different approaches have been employed to make medical applications more secure. Majorly the approaches are divided into two branches. One is using some modifications or mappings to provide privacy preserving. The other is using information hiding methods to hide patients' confidential data from third parties or unauthorized persons. In the sequel, we shortly investigate some privacy-preserving researches and in the next subsections, we review the information hiding methods.

E-health services operate in scenarios with a variety of different stakeholders: patients, relatives, paramedics, nurses, primary care doctors/general practitioners, surgeons, medical specialists and subspecialists, teachers and medical students, researchers, laboratories, insurance companies, governmental oversight agencies, and non-governmental oversight. For the same patient, the information that each user is allowed to access must depend on his role: e.g. if the patient has AIDS or venereal diseases, the nurses and the paramedics need to know, but probably not the researchers using his/her medical tests (Rubio et al. 2013). Attribute-level information hiding methods are effective ways to overcome this issue.

Electronic Medical Record/Electronic Health Record (EMR/EHR) systems are increasingly adopted to collect and store various types of patient data, which contain information about patients' medical histories, demographics, diagnosis codes, medication, allergies, laboratory test results, and billing records. Typically, an EHR system affords stable and protected storage for large volumes of health data. For example, the use of EMR/EHR systems, among office-based physicians, increased from 18% in 2001 to 72% in 2012 and is estimated to exceed 90% by the end of the decade (Gkoulalas-Divanis and Loukides 2014).

Security of medical database plays a vital role in the overall security of medical information systems and networks. This is because of the nature of this technology and its extensive use today. Security of databases not only involves fundamental ethical principles, but also essential prerequisites for effective and trustable medical care. Development of appropriate secure medical database design and implementation methodologies is a significant research issue in the area and a requirement for the successful development of such systems (Pangalos 1995).

The security requirements that must be fulfilled by multimedia medical data and the security measures used to satisfy these requirements are described in Tzelepi (2002). These security measures are based mainly on cryptography and watermarking approaches as well as on security infrastructures. In this research, an extended role-based access control model is introduced by considering the constraints that must be satisfied in order for the holders of the permission to use those permissions. Employing the constraints provides role-based access control to be tailored to specify fine-grained and flexible content-, context- and time-based access control policies. Other restrictions, such as role entry restriction also can be captured.

The study of Gkoulalas-Divanis and Loukides (2014) is a good survey of algorithms for publishing data from electronic health records while preserving privacy. Privacy threats, considering three various kinds of attributes, direct identifiers, quasi identifiers, and sensitive attributes. Direct identifiers are attributes that can explicitly re-identify individuals, such as name, mailing address, phone number, social security number, other national IDs, and email address. On the other hand, quasi identifiers are attributes, which in combination can lead to identity disclosure, such as demographics (e.g., gender, birth date, and zip code) and diagnosis codes. Sensitive attributes are those that patients are not willing to be associated with them. Samples of these attributes are specific diagnosis codes (e.g., psychiatric diseases, HIV, cancer, etc.) and genomic information (Gkoulalas-Divanis and Loukides 2014). The research in Crichtona (2009) defines high, medium, and low security in forensic mental health care. It proposes the Matrix of Security in Scotland.

Centralized storage simplifies routine operations of different health service providers and affords a perfect environment for supporting effective health data mining. The aim of health data mining is to efficiently and effectively extract hidden and valuable knowledge from a great volume of health data with the aim of improving the operations of health service providers or supporting medical research. Data mining on EHRs is beneficial to health service providers, researchers, patients, and health insurers (Khokhar et al. 2014). Some medical centers and hospitals outsource the data mining tasks to third party companies. In this situation, challenges about publishing the storages while preserving privacy are introduced.

Yang et al. (2015) proposed a mixture solution for privacy preserving data sharing in a cloud environment. Some methods are joined to support multiple paradigms of medical data sharing with dissimilar privacy strengths. A real world case study was to report the experimental evaluations of this research.

The research of Fernandez-Aleman et al. (2013) provides a summary of assessing authentication, access control models deployed, access management, what occurs in the case of an emergency, the training of EHR system users and information exchange techniques.

Investigating some privacy preserving systems and proposals, we can conclude that in privacy preserving algorithms some heuristics are employed to transform (maybe we can say a kind of information hiding) the original data to the one that can be published while preserving the privacy of patients. Usually, the heuristics include vertical or horizontal data partitioning, data clustering, space mapping, Space clustering, lattice search etc.

In the continuation, we categorize the applications of information hiding in medical application first based on cover medium and secondly based on the information hiding method.

## 3.1 Based on cover media

Data can be hidden in image, audio, video, signals (e.g. ECG) and text. We divide the methods based on the media that can cover the confidential data. In healthcare and medical application, mostly each research is placed in one of the two categories: first Biological signals and the second Medical Images. In the next two subsections, we shortly introduce these categories.

### 3.1.1 Biological signals

Biological signals usually acquired for diagnosis include the electroencephalogram (EEG), the electrocardiogram (ECG), the electromiogram (EMG), and the electro oculogram (EOG), the abdominal and thoracic breathings (Correa and Leber 2011), mechanomyogram (MMG), electrooculography (EOG), galvanic skin response (GSR), magnetoencephalogram (MEG), etc.

An electrocardiogram (EKG or ECG) is a test that has been used for detecting the problems with the electrical activity of the heart. An EKG converts the heart's electrical activity into line tracings on paper.

Electroencephalogram or EEG is related to the brain. The EEG is the equipment used for measuring electrical activities of the brain. An EEG tracks and records brain wave patterns. Small flat metal discs called electrodes are attached to the scalp with wires. The electrodes analyze the electrical impulses in the brain and send signals to a computer that records the results (Electroencephalogram (EEG) 2018). The electrical impulses in an EEG recording look like wavy lines with peaks and valleys. These lines allow doctors to assess whether there are abnormal patterns. Any irregularities may be a sign of seizures or other brain disorders.

MMG is the mechanical signal observable from the surface of a muscle when the muscle is contracted (Stokes and Blythe 2001). EOG/EOG is a technique for measuring the corneo-retinal standing potential that exists between the front and the back of the human eye (Bulling et al. 2009). GSR is the property of the human body that causes continuous variation in the electrical characteristics of the skin (Boucsein 2012). MEG is a functional neuroimaging technique for mapping brain activity by recording magnetic fields produced by electrical currents occurring naturally in the brain, using very sensitive magnetometers.

To provide metadata in an organized, accessible, also machine-readable way, Zehl et al. (2016) introduced odML (open metadata Markup Language) as a simple file format. All the signals can be stored in odML formats. Both the original raw data of the signal and metadata about the signal can be altered with a small invisible distortion to carry patient information or cover other secret information. Figure 1 shows the biological signals of EEG, ECG, and EOG.

About 20 million people over the world have abnormal electrocardiogram (ECG) signals, i.e., arrhythmias, each year. Most of the cardiac patients are elders. If they increasingly move to nursing homes, it is a necessary tendency to decrease 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 let the doctors to immediately detect the arrhythmia events of any patient without leaving their offices.

By increasing the number of aging people and a considerable portion of that suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as PoC applications in hospitals. For that reason, 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 and glucose level. and diagnosed by remote monitoring systems. It is quite important that patient confidentiality is protected while data is being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems.

So far, different applications related to biological signals have been proposed. In the subsequent, we mention to some samples of them.

A design method for an optimal zonal wavelet-based ECG data compression (OZWC) method for a mobile telecardiology model is proposed in Istepanian and Petrosian (2000). The hybrid implementation issues of this wavelet method with a GSM-based mobile telecardiology system are also presented in Istepanian and Petrosian (2000). The performance of the mobile system with compressed ECG data segments was evaluated and the compression performance analysis of the OZWC is compared with another wavelet-based approach. The optimal wavelet algorithm achieved a maximum compression ratio of 18:1. The mobile telemedical simulation results show the successful compressed ECG transmission at speeds of 100 (km/h) providing 73% reduction in total mobile transmission time with clinically acceptable reconstruction of the received signals. This approach provides a framework for the design and functionality issues of GSM-based wireless telemedicine systems with wavelet compression techniques and their future integration for the next generation of mobile telecardiology systems (Istepanian and Petrosian 2000).

Biological signals such as digital ECG data are huge enough to act as host to carry a tiny amount of additional secret data. For example, the research in AzamiSidek et al. (2014) investigates the robustness of performing biometric identification in a mobile environment using ECG signals. This method simplifies the process of biometric

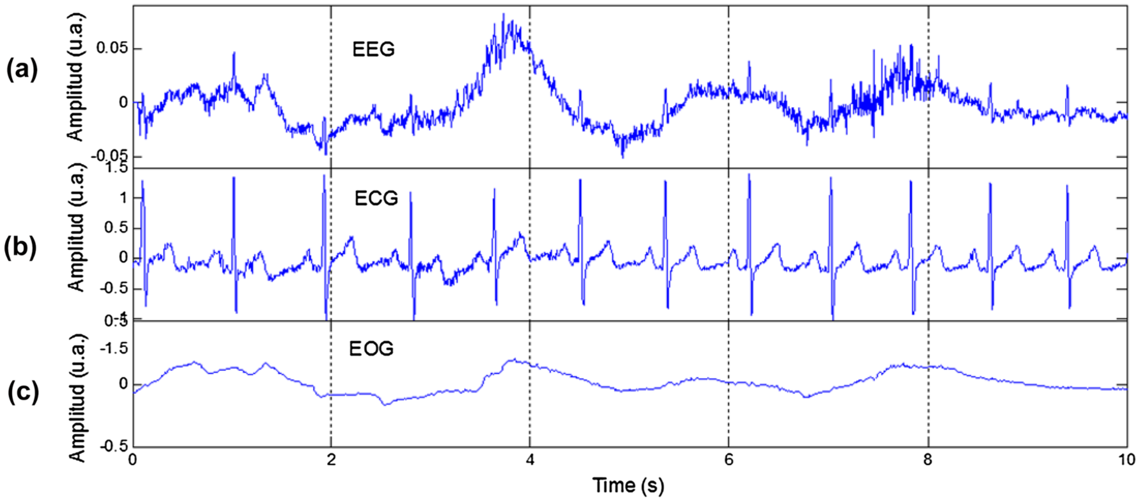

**Fig. 1** Examples of biological signals, **a** EEG recording, **b** ECG signal, and **c** EOG signal (Pangalosa 1993)

identification by reducing computational complexity when compared to other algorithms. This is evident when the total execution time (TET) values were significantly low on mobile devices as compared to a non-mobile device while maintaining high accuracy rates ranging from 98.30 to 99.07% in different classifiers. Consequently, these results support the usability of ECG based biometric identification in a mobile environment.

### 3.1.2 Medical images

Medical imaging plays an important role in monitoring the patient's health condition and providing an effective treatment. Knowledge extraction from biomedical data is one of the most challenging topics in the health engineering (Dao et al. 2015).

In the past years, many medical imaging studies have been conducted worldwide. Medical imaging techniques provide different type of images for diagnosis. Some of the well-known techniques are listed in the following (Eisenberg and Margulis 2011):

- Radiography: this imaging modality utilizes a wide beam of X rays for image acquisition and is the first imaging technique available in modern medicine
- Magnetic resonance imaging (MRI): similar to CT, MRI traditionally makes a two-dimensional image of a thin "slice" of the body and hence is considered a tomographic imaging technique. Modern MRI instruments are capable of producing images in the form of 3D blocks, which may be considered a generalization of the single-slice, tomographic, concept. Unlike CT, MRI does not involve the use of ionizing radiation and is, therefore, not associated with the same health hazards.
- Ultrasonography: medical ultrasonography uses high frequency broadband sound waves in the megahertz range that are reflected by tissue to varying degrees to produce (up to 3D) images.
- Echocardiography: when ultrasound is used to image the heart it is referred to as an echocardiogram.
- Functional magnetic resonance imaging (fMRI): fMRI is a functional neuroimaging procedure using MRI technology that measures brain activity by detecting associated changes in blood flow.
- Computed tomography (CT): a CT scan or computerized axial tomography scan (CAT scan), makes use of computer-processed combinations of many X-ray images taken from different angles to produce cross-sectional (tomographic) images (virtual 'slices') of specific areas of a scanned object, allowing the user to see inside the object without cutting.
- Positron emission tomography (PET): PET is a nuclear medicine, functional imaging technique that produces a three-dimensional image of functional processes in the body.

The amount of data achieved in a MR or CT scan is very extensive. Medical imaging techniques make very large amounts of data, especially CT, MRI, and PET modalities. Accordingly, storage and communication of electronics image data are prohibitive without the use of compression. JPEG 2000 is the state-of-the-art image compression, which is used in Digital Imaging and Communications in Medicine (DICOM) standard for storage and transmission of medical images.

## 3.2 Based on information hiding method

In the field of data hiding, many different techniques have been developed. As a good overview of the research area one can refer to Goljan et al. (2001). All the proposed approaches have in common the ability to store information into an object (called host), but the motivation and purpose of data embedding depends on the applications. For example, steganography requires that the presence of the stored data cannot be revealed (or statistically detected), whilst robust watermarking inserts data into a digital object in such a way that it is difficult to intentionally remove it without degradation. On the other hand, fragile watermarking is aimed at revealing if any modification has been made to the digital object, possibly localizing the modified area. When altering a digital object, reversibility is an issue as compression algorithms are classified as lossless or lossy. In the data-hiding context, the classification distinguishes between reversible and non-reversible. A reversible algorithm must store data and some additional information to recover the original host object, whilst a non-reversible algorithm deals with the issue of minimizing the embedding impact in terms of some measure, like the peak signal-to-noise ratio (PSNR). Generally, medical applications do not tolerate (also for legal aspects) any modification that does not allow us the recovering of the original host object, so reversible algorithms are required (Zhou et al. 2001). Alternatively, at list the modification can be somehow that it does not have influence on the diagnosis of medical experts and physicians.

We categorize the methods based on the type of information hiding methods, which are cryptography, steganography, and watermarking techniques. In the sequel, we describe the concept of each category and the published applications of this category in healthcare and medical systems.

### 3.2.1 Cryptography

In cryptography, security is usually provided by the use of secret keys. These can be thought of as more or less arbitrary sequences of bits that determine how messages are encrypted. In the simplest cryptographic systems, a message encrypted with a given key can only be decrypted with the same key.

Cryptography algorithms are lossless and after decoding if none noise encountered (e.g. during the transmission), the original data can be extracted without any changes. The cryptographed data takes the attentions and a third party can try to break the code and find the key of encryption.

Some well-known cryptography algorithms are ASCII coding and Huffman coding. Computers use binary data and cannot work directly with plain text characters. An ASCII table entry is composed of 8 bits, which allows $2^8 = 256$ different characters. The Huffman coding was developed in 1952 by David Albert Huffman. It is an algorithm that creates a binary tree based on the input data, which results in a lossless data compression. Figure 2 shows a sample of cryptography. In this example, the plaintext 'Information' is coded by Huffman and ASCII coding.

**3.2.1.1 Fundamental concepts** Growth in computation powers and parallelism technology are creating obstruction for credible security especially in electronic information exchanging under cryptosystems. Until now, a massive set of cryptographic schemes has been proposed in which each has its advantages and limitations. Some methods require the use of long bits key and some support the use of small key. Accurate selection of right encryption scheme is important for desired information exchange to achieved enhanced security objectives. The survey in Ali Shoukat et al. (2011) compares the encryption methods for convinced selection of both key and cryptographic scheme.

The general model of cryptography is shown in Fig. 3. In sender side, confidential data is encrypted based on the routine of the cryptography algorithm using a cryptography key. Encrypted data is sent through the communication channel. Receiver decrypts the encrypted data based on the decryption routine using its cryptographic key.

Well-designed cipher should consider some points as the following (Wu et al. 2015):

- Knowledge of the encryption and decryption algorithms should not compromise the security of the system.
- Security should be based on the use of keys.
- The keys should be selected from a large key space so that searching over the space of all possible keys is impractical.

Cryptography techniques can be divided into two groups; those are, based on symmetric key and based on asymmetric key. Based on symmetric key schemes, if an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be exposed. Asymmetric key-based schemes can provide more functionalities than symmetric ones, e.g., key distribution is much easier,

**Fig. 2** A sample of cryptography, **a** original data, **b** encrypted by Huffman coding, **c** encrypted by ASCII coding

| | | |
|---|---|---|
| Information | 001 011 1101 111 1010 1011 010 1001 1000 111 011 000 1100 | 01001001 01101110 01100110 01101111 01110010 01101101 01100001 01110100 01101001 01101111 01101110 00001101 00001010 |
| (a) Plain text | (b) Huffman coded text | ASCII coded text |

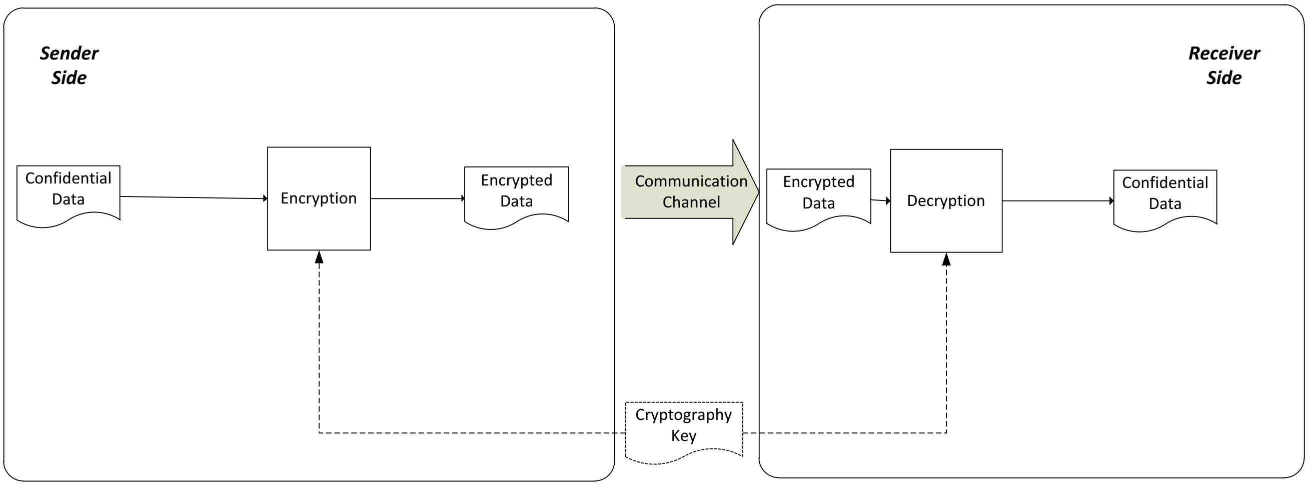

**Fig. 3** General model of cryptography

authentication and non-repudiation are available, and compromise of a private key of a user does not reveal messages encrypted for other users in the group. However, they are generally computationally expensive (Zhao et al. 2012).

Traditional asymmetric cryptography generally and effectively used in the Internet relies on a public key infrastructure (PKI). The success of PKI depends on the availability and security of a certificate authority (CA), a central control point that everyone trusts (Zhao et al. 2012). In general, Mobile Ad-hoc NETworks (MANET), applying PKIs by maintaining a central control point is clearly not always feasible. Another obstacle that impedes PKI's employment in MANETs is the heavy overhead of transmission and storage of public key certificates (PKCs).

Identity based cryptography (IBC) is a form of public key cryptography. It is an approach to eliminate the requirement of a CA and PKCs. Since 2001, IBC has attracted more and more attention from security researchers. Some properties of IBC make it especially suitable for MANETs. The advantages of IBC for MANETs are (Zhao et al. 2012):

- Easier to deploy without any infrastructure requirements. This saves certificate distribution, while bringing "free" pairwise keys without any interaction between nodes.
- Its resource requirements, concerning processing power, storage space, communication bandwidth, is much lower.
- The public key in IBC is self-proving and can convey much useful information.

IBC with its rapid development in recent years is a promising solution for MANET security issues. The study in Zhao et al. (2012) provides a survey of applications of IBC in MANETs.

**3.2.1.2 Applications in medical and healthcare systems** Encryption is the common approach to protect information confidentiality. Encrypting the patient confidential information prevents unauthorized persons from achieving the information and results secure transmission. A sample cryptography method encrypts the original text data with encryption key value generated from chaotic sequence with threshold function by bit xor operation. It is very useful to transmit the secret data through unsecure channel securely, which prevents data hacking (Joseph and Remya 2014).

Storing and sharing of medical data in the cloud environment, where computing resources, including storage is provided by a third party service provider, raise serious concern of individual privacy for the adoption of cloud computing technologies. Existing privacy protection researches can be classified into three categories, i.e., privacy by policy, privacy by statistics, and privacy by cryptography. However, the privacy concerns and data utilization requirements on different parts of the medical data may be quite different. The solution for medical dataset sharing in the cloud should support multiple data accessing paradigms with different privacy strengths. The statistics or cryptography technology alone cannot enforce the multiple privacy demands, which blocks their application in the real-world cloud (Yang et al. 2015a, b).

The study of Yang et al. (2015a, b) proposes a practical solution for privacy preserving medical record sharing for cloud computing. Based on the classification of the attributes of medical records, it uses vertical partition of medical dataset to achieve the consideration of different parts of medical data with different privacy concerns. It mainly includes four components, i.e., (1) vertical data partition for medical data publishing, (2) data merging for medical dataset accessing, (3) integrity checking, and (4) hybrid search across plaintext and cipher text, where the statistical analysis and cryptography are combined together to provide multiple paradigms of balance between medical data utilization and privacy protection.

The case study of privacy-preserving medical data sharing involves three parties, i.e., (1) community hospitals or senior people nursing centers with general medical practitioners, who have particular skills and practice a holistic approach for treating people with multiple health issues; (2) regional medical center or class A hospitals with domain specific medical doctors, who are experts of one or several diseases; (3) cloud service providers with the Regional Healthcare Collaboration Platform (RHCP) enabling the provision of collaborative medical care to the outpatients or inpatients of organizations (A) and (C). As a typical usage scenario, hospital A stores and shares the collected medical records of the patients on the RHCP, where the medical data storage is provided by a third party cloud provider. The shared medical data will be consumed by the general medical practitioner in hospital B. Here, A is the data owner, the RHCP serves the role of the cloud service of medical data storage, and B is the data recipient (Yang et al. 2015a, b).

The research in Rubio et al. (2013) proposes an encoding system for 1D biomedical signals that allows embedding metadata and provides security and privacy. The design is based on the analysis of requirements for secure and efficient storage, transmission, and access to medical tests in e-health environment. This approach uses the 1D SPIHT (Set Partitioning In Hierarchical Trees) (Said and Pearlman 1996) algorithm which is first presented as an efficient method for coding wavelet coefficients in image (2-D) compression, to compress 1D biomedical signals with clinical quality, metadata embedding in the compressed domain to avoid extra distortion, digital signature to implement security and attribute-level encryption to support role-based access control. Besides, the system is very efficient and secure, it permits embedding large amounts of additional information within the signal (e.g. ~ 3 KB per lead in resting ECGs, ~ 200 KB per lead in stress tests, ~ 30 MB per lead in ambulatory ECGs), detecting corruption of the signal or the information, and implementing different access levels for a variety of professional roles. The compression ratio achieved by the encoding is quite high, ranging from ~ 3 in real-time transmission to ~ 5 in offline operation, despite of the embedding of security elements and metadata to enable e-health services. In addition, this architecture could be extended to biomedical signals of higher dimension (e.g. 2D: MRIs, TACs, 3D: echocardiograms), since the encoding relies on the SPIHT algorithm. This would require changing to the adequate SPIHT modality (2D/3D), tuning the compression parameters, and establishing the distortion threshold for each new type of signal (Rubio et al. 2013).

A patient-identity security mechanism including an identity cipher/decipher and a user-authentication protocol, is proposed in Chaoab et al. (2005) to ensure the confidentiality and authentication of patients' electronic medical records (EMRs) during transit and at rest. To support the confidentiality of an EMR, the identity cipher/decipher uses a data-hiding function and three logical-based functions to encrypt/decrypt a patient's identifying data and medical details in an EMR. The cipher text of the patient's identifying data is patient-EMR related, whereas that of medical details is healthcare agent-EMR related. To support the authentication of an EMR, the user-authentication protocol based on a public key infrastructure uses certificates and dynamic cookies for verification/identification. The experimental results of Chaoab et al. (2005) show that healthcare agents can install large amounts of patients' encrypted EMRs in healthcare databases efficiently. In addition, separately storing the keys in a user's token and an EMR database for decryption increases the safety of patients' EMRs. For each user-authentication trail, the use of certificates and dynamic cookies for verification/identification ensures that only authorized users can obtain access to the EMR, and anyone involved cannot make false claims.

### 3.2.2 Steganography

Numerous security tools encrypt the information and prevent unauthorized access to the data exist. On the other hand, for hiding the very existence of these records steganography algorithms can be used. Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified, or even just to identify an image.

Generally, steganography techniques utilize redundancies in cover medias for embedding. However, they differ on their approach and the format (e.g., BMP, JPEG in case of image) they work on Sajedi and Jamzad (2010a, b). There have been a number of steganography techniques proposed over the past few years. The aim of image steganography is to hide data in an image with visual and statistical invisibility. In this fashion, hiding in other medias may demand other requirements.

There are many approaches to secure patient sensitive data (Rosa Algarin et al. 2012; Hu et al. 2007; Wang et al. 2010; Li et al. 2013). However, one approach proposed to secure data is based on using steganography techniques to hide secret information inside medical images like the methods of Zheng and Qian (2008), Golpira and Danyali (2010) and Kaur et al. (2010). The challenging factors of these techniques are how much information can be stored, and to what extent the method is secure. Finally, what will be the resultant distortion on the original medical image or signal? Embedding robustness is less important in many applications.

Each steganography method has its affirmative and feeble characteristics. For example, embedding data using the Pixel Difference Expansion involves computational overhead. It involves calculating the different values, partitioning difference values into four sets, creating a location map, collecting original LSB values, data embedding by replacement, and inverse integer transform. Another technique, the bit modification is least secure. The security lies on the presumption that no other parties are aware of this secret message. This method is easy to implement but very susceptible to data loss due to channel noise and resampling.

**3.2.2.1 Fundamental concepts** Cover object refers to the object used for carrying the embedded bits, embedded data is known as payload and the object with embedded data is called as stego object. The distortion induced on the host signal by the data embedding process is called the embedding distortion.

Imperceptibility is innocuousness of the stego object. For example, stego image should not have severe visual artifacts. Some of the major requirements of steganography include capacity and security. Capacity refers to the amount of information that can be hidden in cover medium without deteriorating the integrity of the cover object. Embedding operation needs to preserve the statistical properties of the cover object in addition to the perceptual quality.

Security means eavesdropper's inability to detect hidden information. Perceptual transparency ensures the retention of the visual quality of the cover after data embedding. Tamper resistance means to remain intact in the face of malicious attacks.

The embedding rate is measured as the number of embedded bits per carrier bit. The embedding efficiency is given by the expected number of embedded message bits per modified carrier bit. The change rate gives the average percentage of modified carrier bits (Subhedara and Mankar 2014).

Figure 4 shows the general model of steganography. In this figure, dashed-lines show the optional parts. The

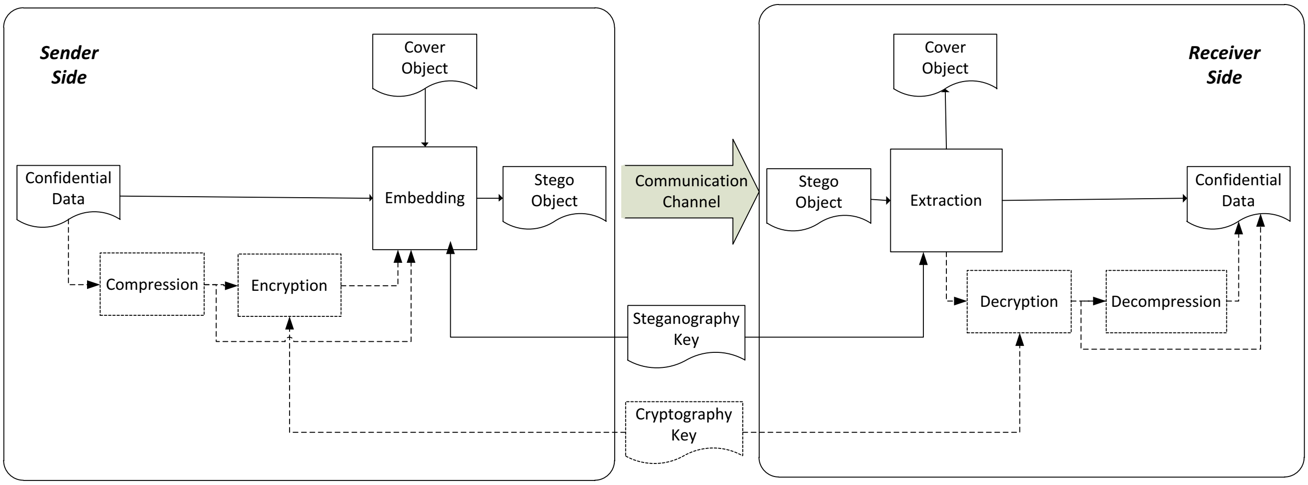

**Fig. 4** General model of steganography

confidential data before to be send through the communication channel, may be compressed and/or encrypted. After that, the embedding process hides this data into a cover object. A random cryptography key can be used in encryption process and similarly a key can be used for embedding data into the cover object. In server side, the same keys should be used for encryption and extraction.

Increasing the embedding capacity of cover objects reduces the detection risk of stego objects. In this respect, in Sajedi and Jamzad (2010) a boosted steganography scheme (BSS) is proposed that has a preprocessing stage before applying steganography methods. The goal of BSS is increasing the undetectability of stego images.

The development of steganography methods has led to an increased interest in steganalysis techniques. Most of the steganalysis methods attempt to estimate cover object statistics. One way to provide a secure steganography method is to disturb the estimation of steganalyzers. The main concern of Sajedi and Jamzad (2010a, b) is to resist against steganalysis methods and utilize a mechanism to securely embed more secret data into an image. Hybrid steganographic approach (HYSA), embeds secret data with randomized embedding algorithms in randomized regions of the cover image. HYSA embeds secret data in only some regions of the image not all over the image. In addition, HYSA can employ more than one steganography methods for embedding secret data in the image. Random selection of embedding regions and steganography methods leaves a combination of several types of distortion on the image, which are difficult to be recognized by the steganalysis methods (Sajedi and Jamzad 2010a, b).

The problem of spreading secret data to embed into multiple cover images is called batch steganography and has been theoretically considered recently. Few works have been done in batch steganography, and in all of them, the payload is spread between cover images unwisely. In Sajedi and Jamzad (2009a, b), adaptive batch steganography (ABS) approach is proposed which considers embedding capacity as a property of images. ABS is an approach to adaptively spread secret data among multiple cover images based on their embedding capacity. By splitting the payload based on image embedding capacity constraint, embedding can be done more secure than the state when the embedder does not know how much data can be hidden securely in an image.

Embedding capacity is the key measure to compare the performance of different data embedding algorithms. In a general sense, embedding capacity is the maximum data size that can be securely embedded in an object with respect to certain constraints (Sajedi and Jamzad 2009). By applying the steganography method proposed in Delbarpour and Sajedi (2017), the amount of distortion in cover images is low because an optimization method based on artificial immune system (AIS) tries to find places for embedding that cause low distortion.

In medical and healthcare applications, if a cover object is the subject of diagnosis by the physicians, minimum amount of perceptual distortion is a significant factor.

**3.2.2.2 Applications in medical and healthcare systems** In wireless tele-cardiology applications, ECG signal is widely used to monitor cardiac activities of patients. Accordingly, in most e-health applications, ECG signals need to be combined with patient confidential information. Data hiding techniques can play a crucial role in ECG wireless telemonitoring systems by combining the confidential information with the ECG signal. Some studies have been embedding information in ECG signal as a one-dimensional signal using Wavelet transform decomposition and then altering the wavelet coefficients. Wavelet transform decompose a signal to some subbands. For example, it decomposes an image as a two-dimensional signal to four types of subbands called HH, LL, LH, and HL in some levels of resolution. In the sequel, we describe these researches.

Electronic medical prescription is one of the areas benefiting from improvement in health care due to the introduction of information and communication technology. Within the overall context of protection of health care information, privacy of prescription data needs special treatment. The research of Omotosho et al. (2014) presents an e-prescription system that addresses some challenges pertaining to the prescription privacy protection in the process of drug prescription. The developed system uses spread spectrum image steganography algorithm with advanced encryption standard (AES) key implementation to provide a secure means of delivering medical prescription to the parties involved. The architecture for encoding and decoding was implemented with an electronic health record. The software development tools used were PHP and MySQL database management system for front end and backend data management, respectively. The designed system demonstration shows that the synergistic combination of steganography and cryptography technologies in medical prescription is capable of providing a secure transmission to properly provide security for patients' medical prescription (Omotosho et al. 2014). This study hides prescriptions in optional images using Spread Spectrum steganography algorithm.

Medical images: In Srinivasan et al. (2004), an improved version of a high capacity data-hiding scheme, called bit-plane complexity segmentation (BPCS) steganography, is explained, and its effectiveness in hiding medical records in color cervical images is demonstrated.

In Ahmad (2014), a method is proposed to protect the medical data using the shared secret mechanism and steganography for 2 and 1 bit LSB. Its experimental results show that they produce relatively good quality (the similarity between the cover and the stego medical images).

ECG: ECG Steganography provides secured transmission of secret information such as patient personal information through ECG signals. A wavelet based steganography method is presented in Mu-Hsing and Kuo (2011), that combines encryption and scrambling method to safeguard patient confidential data. This method hides the corresponding patient confidential data and other physiological information of the ECG signal owner thus guaranteeing the integration between ECG and the rest. For evaluation of the effectiveness of this method on the ECG signal, two distortion criteria have been used: the percentage residual difference and the wavelet weighted PRD. It is found that ECG data remains diagnosable after hiding patient confidential data and as well as after hidden data are removed from the stego data (Mu-Hsing and Kuo 2011).

In Engin et al. (2005), after encryption of the private data, the ECG signal is broken down into frequency sub-bands, some carrying the meaningful data of the ECG and some carrying noise. A mathematical model identifies the different sub-bands and embeds the encrypted personal data in the noise bands. To embed the data securely, the model calls for two types of encryption. One relies on a key that the sender and the recipient both know. The other is based on a uniquely generated matrix that scrambles a key stored by both the sender's and recipient's computers. Once the data have been sent, the recipient's device must have the shared key, the scrambling matrix, and information about how the data was broken down into sub-bands to even prompt healthcare personnel for their credentials.

A steganography method is presented in Ibaida et al. (2010) which embeds confidential data of patients into specific locations (called special range numbers) of the digital ECG host signal which will make minimal distortion to ECG, and at the same time, any secret information embedded can be totally extracted. This research shows that there are 2.1475 × 10(9) possible special range numbers making it extremely difficult for intruders to identify locations of secret bits.

A steganography technique based on wavelet has been presented in Joseph and Remya (2014). It combines encryption and LSB embedding method to protect patient confidential data. Massive 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 and glucose level. and diagnosed by those remote patient-monitoring systems. An added benefit is the freedom of movement for patients due to the wireless networking technologies. A three-level wavelet decomposition is applied in this method.

The research in Edward Jero et al. (2014) presents a method, which employs discrete wavelet transform to decompose signals and singular value decomposition (SVD) to embed the secret information into the decomposed ECG signal. This method embeds the data 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 (by the measures introduced in Sect. 3.1) of the proposed approach allows understanding the suitable sub-band to hide secret data and the signal degradation that will affect diagnosability. In addition, a dynamic selection approach of location for embedding the singular values is proposed in Edward Jero et al. (2014). This approach is demonstrated on a database and the observations validate that HH is the ideal sub-band to hide data. In addition, it is observed that the signal degradation (less than 0.6%) is very less in this method even with the secret data being as large as the sub band size. Therefore, it does not have effect on the diagnosability and is reliable to transmit patient information (Edward Jero et al. 2014).

In Malashree et al. (2014), another wavelet based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data. This method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest (Malashree et al. 2014).

### 3.2.3 Watermarking

Systems for inserting data in objects are divided into watermarking systems, in which the message is related to the cover object, and non-watermarking systems, in which the message is unrelated to the cover object (Wu et al. 2015).

The advances in recording, editing, and broadcasting multimedia contents in digital form motivate to protect these digital contents from illegal use, such as duplication, manipulation, and redistribution. However, watermarking algorithms are designed to satisfy the requirements of applications, as different applications have different concerns.

Digital watermarking is used to provide evidence of ownership and tampering of digital contents. It has a broad range of applications, such as data authentication, copyright protection, device control, fingerprinting, media forensics, and information hiding. Digital watermarking is a process of embedding useful information into a digital cover (Naheed et al. 2014).

**3.2.3.1 Fundamental concepts** Reversible watermarking is a promising technique, which satisfies the requirements.

A watermarking algorithm is proposed in Naheed et al. (2014) for applications which require high embedding capacity and imperceptibility, to maintain the integrity of the host signal and also embedded information. This algorithm focuses on enhancing the watermark capacity and reducing the perceptual degradation of an image. This research investigated the additive interpolation-error expansion algorithm and enhanced it by incorporating with two intelligent techniques: genetic algorithm (GA), and particle swarm optimization (PSO). GA is applied to exploit the correlation of image pixel values to obtain a better estimation of neighboring pixel values, which results in optimal balance between information storage capacity and imperceptibility. PSO is also applied for the same purpose.

Goljan et al. (2001) introduced distortion-free data embedding in images. De Vleeschouwer et al. used a circular interpretation of bijective transformations of the histogram to embed data. In Vleeschouwer et al. (2003) and Tian (2003) proposed a reversible data-embedding method using the difference expansion of pairs of pixel values. To provide invertibility, a bi-level location map is compressed using JBIG2 method and transmitted as a part of the payload. Alattar generalized Tian's method to arbitrary vectors instead of pairs (Alattar 2004). Celik et al. (2005) presented a reversible data-embedding algorithm by compressing quantization residues.

The general model of watermarking is presented in Fig. 5.

Motivated by the advantages mentioned above, some researchers already applied watermarking technique to medical data.

**3.2.3.2 Applications in medical and healthcare systems** Nowadays, watermarking has become a technology of choice for a broad range of multimedia copyright protection applications. Watermarks have also been used to embed specified data in biomedical signals. Thus, the watermarked biomedical signals being transmitted through communication are resistant to some attacks.

Digital watermarking, which imperceptibly embeds information within a host signal (such as image, audio, or video),

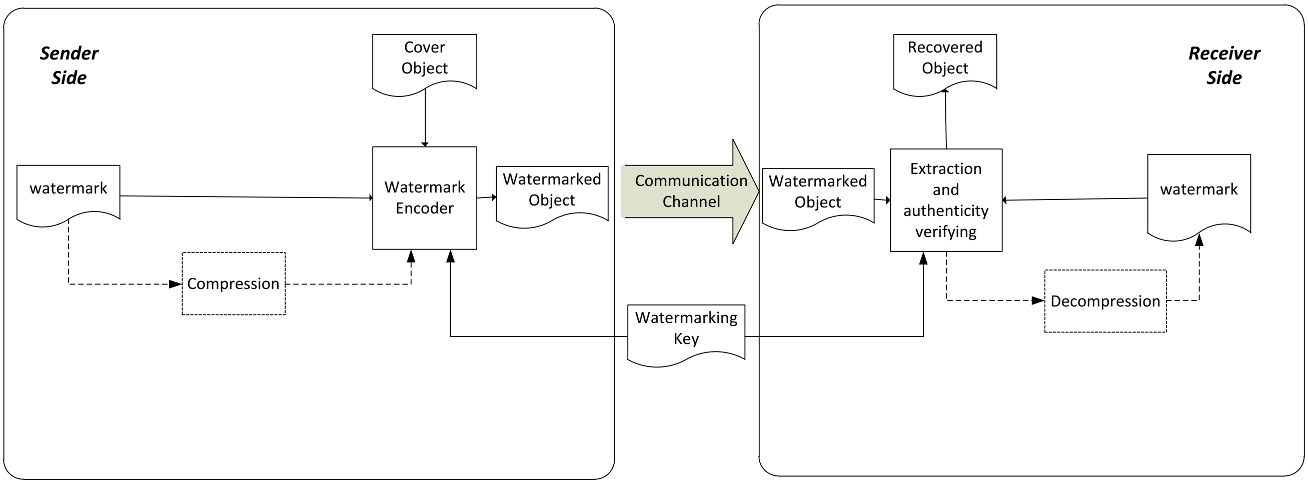

Fig. 5 General model of watermarking

is an emerging technique for protecting multimedia data. When applied to medical environments, the watermarked image can still conform to digital imaging and communications in medicine (DICOM) format. The security information can adhere to the image even if the image format is changed. Furthermore, the property of imperceptibility makes an unauthorized person more difficult to intercept or attack the watermark information hiding in the image.

Coatrieux et al. were one of the first researchers who examine the relevance of watermarking for medical images. They proposed an alternate approach by separating an image into a protection zone and an insertion zone to avoid compromising any diagnostic capability (Coatrieux et al. 2001). Lossless watermarking, which can recover the original image exactly, has drawn lots of interest recently (Goljan et al. 2001; Vleeschouwer et al. 2003; Tian 2003; Alattar 2004; Celik et al. 2005; Tzelepi 2002; Guo and Zhuang 2003).

With the rise in use of internet and multimedia the stealing of information from biomedical images, has become a major concern for healthcare professionals. Data hiding/watermark are added ownership to increase the level of security and to verify authenticity. Patients' information (electronic patient record), the logo of the hospitals or diagnostic centers can be inserted in the biomedical data as watermark to prove the intellectual property rights. Extraction is a most important process, as any kind of distortion during retrieval of the watermarked image will be unacceptable. After extraction of the watermark, it claims the original object, and thus data can be successfully hidden in an image. In other words, it can be said that watermark is actually a data, which is embedded within an object or image, and later it is extracted to recollect the required information (Chakraborty et al. 2013).

We split the researches base on the cover media, which can be medical images or ECG signal.

Medical images: The watermarking of digital images has an important role in the protection of digital content with respect to many aspects. Medical image watermarking has been widely recognized as a relevant technique for enhancing data security, image fidelity, authenticity, and content verification in the current e-health environment where medical images are stored, retrieved, and transmitted over networks. Medical image watermarking preserves image quality that is mandatory for medical diagnosis and treatment (Rao and Kumarib 2011).

The research of Guo and Zhuang (2009) presents a lossless watermarking method in the sense that the original image can be exactly recovered from the watermarked one, with the aim of verifying the integrity and authenticity of medical images. Furthermore, the scheme has the capability of not introducing any embedding-induced distortion in the region of interest (ROI) of a medical image. Difference expansion of adjacent pixel values is employed to embed several bits. A region of embedding represented by a polygon, is selected intentionally to avoid making embedding distortion in the ROI. Only the vertex information of a polygon is transmitted to the decoder for reconstructing the embedding region, which enhances the embedding capacity considerably. The digital signature of the whole image is embedded for verifying the integrity of the image. An identifier represented in electronic patient record (EPR) is embedded for verifying the authenticity by simultaneously processing the watermarked image and the EPR. Joining with fingerprint system, patient's fingerprint information is embedded into several image slices and then extracted for verifying the authenticity. The proposed watermarking method is a region-based lossless watermarking scheme, being capable of verifying authenticity and integrity of medical images is presented. Furthermore, the watermark encoder can choose embedding regions at will without introducing any distortion in the ROI. The watermarked image may be used for diagnostic purposes as well as other medical applications, provided that the embedding region does not intersect with the ROI. The experimental results demonstrate that such scheme can hide large amounts of data while keeping distortion level low enough. Any modification in the watermarked image can be detected.

Biometric information, such as fingerprint, is difficult to forge, providing concrete way for authentication. In Guo and Zhuang (2009), fingerprint authentication system is combined with the proposed watermarking scheme to further enhance the authenticity of medical images. A patient's medical image data often contains several slices of images for CT0 or MRI modality. First, the patient's fingerprint image is acquired via a standard fingerprint device. The device has output is a binary sequence (about 300 bytes) representing the fingerprint image's eigenvector. A dynamic bit allocation strategy is employed to embed such large information while keeping the total distortion level still very low. The embedding capacity of each slice is calculated before embedding. The fingerprint's eigenvector information is distributed to each slice, proportional to its embedding capacity; in general, given a distortion level, a slice with larger capacity will be embedded with more bits. In information extracting and authenticity verifying process, the watermark is first extracted from each slice. The fingerprint image's eigenvector is then reconstructed by combining all the pieces in inverse order and input to the fingerprint authentication system as a reference. During the verifying process, the fingerprint authentication system calculates the eigenvector of the input fingerprint's image and compares it with the reference to decide if the two are matching according to some suitable criteria. Experimental results show that such system can unambiguously identify the right person who is associated with the medical images (Guo and Zhuang 2009).

Zhou et al. (2005) presented two lossless data-embedding methods to embed digital signature to medical images. The first method was based on compressing the LSBs of randomly selected image pixels; the other method was based on a regular/singular (RS) approach that was introduced in the work of Goljan et al. (2001). However, current reversible watermarking methods did not have region-selecting capability (Goljan et al. 2001; Vleeschouwer et al. 2003; Tian 2003; Alattar 2004; Celik et al. 2005; Tzelepi 2002). The embedding-induced distortion was distributed in the whole image, instead of some region. If they were applied in medical environments, the watermark extraction and the original image restoration must be performed to ensure that the diagnostic accuracy in the region of interest (ROI) was not compromised by the embedding-induced distortion. This might bring great inconvenience in practical medical applications.

Zhou et al. (2001) presented a watermarking method for verifying the authenticity and integrity of digital mammography images. To embed the digital envelope into the image, the least significant bit (LSB) of one random pixel of the mammogram is replaced by 1 bit of the digital envelope bit stream. Instead of the whole image data, only partial image data (not including LSB plane) is used for verifying integrity. Other researchers adapted digital watermarking for interleaving patient information with medical images to reduce storage and transmission overheads. Again, the LSBs of image pixels are replaced for embedding.

Chao et al. proposed a discrete cosine transform (DCT)-based data-hiding technique, which is capable of hiding those electronic patient record (EPR) related data into a marked image. The information was embedded in the quantized DCT coefficients (Chao et al. 2002). The drawback of this watermarking approach is that the original medical image is distorted in a non-invertible manner, such as bit replacement, truncation, or quantization. It is impossible for the watermark decoder to recover the original image.

Golpira and Danyali (2010) proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this work, medical images such as regional medical imaging (MRI) are used as host signal. A two-dimensional wavelet transform is applied to the image. Then, the histogram of the high frequency subbands is determined. Next, two thresholds are selected, the first is in the beginning and the other is in the last portion of the histogram. For each threshold, a zero point is created by shifting the left histogram part of the first threshold to the left, and shifting the right histogram part of the second threshold to the right. The locations of the thresholds and the zero points are used for inserting the binary watermark data. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithm is low. Moreover, no encryption key is involved in its watermarking process.

In Wu et al. (2015), a reversible data hiding method with contrast enhancement is presented for medical images. First, image background segmentation is performed and the principal gray-scale values in the segmented background are identified. By excluding the corresponding histogram bins from being expanded for data hiding, the contrast of ROI in medical images can be selectively enhanced. Considering the characteristics of pixel distribution, they develop a pre-processing strategy to reduce the visual distortions that may be caused. With this method, an original image can be exactly recovered from the corresponding enhanced image by hiding the side information within it. The experimental results on a set of medical images show that the visibility of ROI can be improved.

In Zhou et al. (2001), a reversible watermarking algorithm is presented for hiding information into medical images having luminance histograms with particular characteristics. Some radiographic images have the property that not all the gray levels are present; this leads to sequences of 0 values (0-runs) in the corresponding histograms. It is possible to use these 0-runs to encode information by modifying pixels having gray levels contiguous to these runs; by encoding also the run information it is possible to restore the original image after extracting the stored data. This watermarking technique is capable of exploiting all the 0-runs in the image histogram to achieve high capacity. Part of the watermark information may be devoted to a digital signature of the original image, whose authenticity may also be verified by a user.

In Nambakhsh et al. (2006), a blind watermarking method with secret key is presented by embedding ECG signals in medical images. The embedding is done when the original image is compressed using the embedded zero-tree wavelet (EZW) algorithm (Shapiro 1993). The extraction process is performed at the decompression time of the watermarked image. The proposed method is able to utilize about 15% of the host image to embed the mark signal. This marking percentage has improved previous works while preserving the image details.

Giakoumaki et al. (2006) propose a wavelet transform based watermarking algorithm for medical data. They got success to embed information relating patient's names and addresses, doctor's diagnosis and signatures into different frequency bands in the wavelet transform of ultrasound images. The main disadvantage of the method was that the original medical records or images were lost.

The research of Rao and Kumarib (2011) highlights essential needs of medical image watermarking with a review of developments from 2000 until 2010.

ECG: Zheng and Qian (2008) proposed a reversible data hiding technique based on wavelet transform. Their method is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex (Phukpattaranont

2015). The QRS complex is the combination of the Q wave, R wave, and S wave and represents ventricular depolarization. After detecting R waves (Bacharova et al. 2014), Haar lifting wavelet transform (Gavrovska et al. 2014) is applied again on the original ECG signal. Next, the non-QRS high frequency wavelet coefficients are selected by comparing and applying index subscript mapping. Then, the selected coefficients are shifted one bit to the left and the watermark is embedded. Finally, the ECG signal is reconstructed by applying reverse haar lifting wavelet transform. Moreover, before they embed the watermark, Arnold transform (Aburab 2013) is applied for watermark scrambling. This method has low capacity since it is shifting one bit. As a result, only one bit can be stored for each ECG sample value. Furthermore, the security in this algorithm relies on the algorithm itself; it does not use a user-defined key. Finally, this algorithm is based on normal ECG signal in which QRS complex can be detected. However, for abnormal signal in which QRS complex cannot be detected, the algorithm will not perform well.

The research in Engin et al. (2005) investigates a watermarking technique based on discrete wavelet transform for signal integrity verification in an electrocardiogram (ECG) coming from four ECG classes for monitoring application of cardiovascular diseases. This technique is evaluated under different noisy conditions for different wavelet functions. Daubechies (db2) wavelet function based technique performs better than those of Biorthogonal (bior5.5) wavelet function do. For the beat-to-beat applications, all performance results belonging to four ECG classes are highly moderate.

Kaur et al. (2010) proposed a digital watermarking of ECG data for secure wireless communication. A low frequency chirp signal is used to embed watermark which is patient's identification taken as 15-digit code. In their work, each ECG sample is quantized using 10 bits, and is divided into segments. The segment size is equal to the chirp signal that they use.

Finally, we summarize some selected studies in Table 3. The data that should be hidden in cryptography and steganography methods is listed in the third column and the cover type in steganography and watermarking method is mentioned in the fourth column.

### 3.3 Other applications of computer science algorithms in medical and bioinformatics science

Medical care and machine learning are associated together in the current era. For example, machine learning techniques support the medical diagnosis process/decision making on large scale of diseases. Advanced data mining techniques in diseases information processing context become essential. The study of Ghazvini and Shukur (2013) covered several aspects of large-scale knowledge mining for medical and diseases investigation.

Sometimes, existing mining approaches are not sufficient to handle large volume of datasets. Biological data processing also suffers for the same issue. In Nimmy et al. (2017), a classification process is carried out on large volume of exons and introns from a set of raw data. In Kamal and Khan (2014a, b), large data sets are subdivided into various segments to reduce the data sets as well as for efficient memory use. The integration of dynamic programming (DP) and Chapman–Kolmogorov equations (CKE) makes the analysis faster. The subdivision process is named data reducing process (DRP). DRP is imposed before DP and CKE. This approach needs less space compared with other methods and the time requirement is also improved.

Ongoing improvements in computational biology research result in different research works about protein–protein interactions (PPIs) and protein fold recognition. The availability of PPI data for several organisms provokes the discovery of computational methods for measurements, analysis, modeling, comparisons, clustering, and alignments of biological data networks. Nevertheless, fixed network comparison is computationally stubborn and as a result, several methods have been used instead. A probabilistic approach among proteins nodes that are part of various networks using Chapman–Kolmogorov (CK) formula is illustrated in Kamal et al. (2014). Large proteins have been mapped using self-organizing maps (SOMs). Neural network based SOMs has a significant role in reducing the irregular shapes of proteins interactions. Iterative checking enables the organizations of all proteins. In next stage, particle swarm intelligence is applied to classify the proteins' families. In Kamal et al. (2017), secondary (two-dimensional) and tertiary proteins (three-dimensional) proteins have been grouped. Two-dimensional proteins contain fewer hydrocarbons than three-dimensional proteins.

Markov Chain is very effective in prediction basically in long data set. In DNA sequencing it is always very important to find the existence of certain nucleotides based on the previous history of the data set. The research of Khan and Kamal (2015) imposed the Chapman Kolmogorov equation to accomplish the task of Markov Chain. Chapman Kolmogorov equation is the key to help the address the proper places of the DNA chain and this is very powerful tools in mathematics as well as in any other prediction based research.

Several protein structure prediction methods use neural network (NN). However, the Hidden Markov model is more interpretable and effective for more biological data analysis compared to the NN. It employs statistical data analysis to enhance the prediction accuracy. The work of Kamal et al. (2017a, b, c) proposed a protein prediction approach from protein images based on Hidden Markov Model and Chapman Kolmogrov equation.

**Table 3** Summary of the employment of information hiding methods in medical systems

| Ref. no. | Hiding methods | Embedded data | Cover type | Methodology |
|---|---|---|---|---|
| Omotosho et al. (2014) | Cryptography | Medical prescription | – | Advanced encryption standard (AES) key |
| Yang et al. (2015a, b) | | Medical records | – | |
| Rubio et al. (2013) | | 1D biomedical signals | – | |
| [110] | | Patient confidential data | – | |
| Correa and Leber (2011) | | Patient confidential data | – | |
| [110] | Steganography | Patient confidential data | ECG signal | |
| Edward Jero et al. (2014) | | Secret information | ECG image | |
| Ahmad (2014) | | Medical data | Medical images | LSB steganography |
| Engin et al. (2005) | | Encrypted personal data | ECG signal | |
| Sajedi and Jamzad (2010) | | Medical records | Color cervical images | |
| Ibaida et al. (2010) | | Confidential information of patients | ECG signal | |
| Malashree et al. (2014) | | Patient confidential data and other physiological information | ECG signal | |
| Joseph and Remya (2014) | | Patient information and diagnostics information | ECG signal | |
| (Omotosho et al. (2014) | | Medical prescription | Optional images | Hiding encrypted prescription using spread spectrum |
| Guo and Zhuang (2009) | Watermarking | Signature of the whole image for verifying the integrity of the image<br>Patient's fingerprint information is for verifying the authenticity | Medical images such as regional medical imaging (MRI) | |
| Naheed et al. (2014) | | Watermark | Medical images | Additive interpolation-error expansion algorithm and enhanced it by incorporating with GA and PSO<br>Data is embedded into high frequency coefficients of each block by applying the hiding technique based on bit shifting |
| Golpira and Danyali (2010) | | Binary watermark data | Medical images | |
| Zhou et al. (2001) | | Verifying watermark | Digital mammography images | |
| Chao et al. (2002) | | Electronic patient record | Medical image | |
| Tzelepi (2002) | | Digital signature | medical images | |
| Kaur et al. (2010) | | A low frequency chirp signal as the patient's identification | ECG signals | |
| Wu et al. (2015) | | A string of message bits | Medical images | |
| Cavagnino et al. (2015) | | Watermark | Radiographic images | |
| Chakraborty et al. (2013) | | Hospital logo or electronic patient record | Retinal images* | Spread spectrum image-watermarking algorithm using the Discrete Multiwavelet Transform |
| Rao and Kumarib (2011) | | Watermark | Medical images | |
| Nambakhsh et al. (2006) | | ECG signals | Medical images | |
| Zheng and Qian (2008) | | Watermark | ECG signals | |
| Engin et al. (2005) | | Watermark | ECG signals | |

*http://www.isi.uu.nl/Research/Databases/DRIVE/

Coding of biological data is a key area to get exact information on animals to discover the desired medicine. In Kamal et al. (2018), four different machine-learning approaches such as support vector machine (SVM), principal component analysis (PCA) technique, neural mapping skyline filtering (NMSF) and Fisher's discriminant analysis (FDA) were applied for data reduction and coding area selection.

Biological interaction mainly depends on the interactions of various genes and genomes. To identify actual meaning of interactions the facts and reasons for these interactions should be found out. Gene analysis allows verifying such environment. Gene annotation means to identify the exon regions in metagenomic samples. Accurate solution for large scale sequencing, trims space complexity and generates optimal gene annotation have tested in Kamal et al. (2016).

Protein fold recognition is considered as an essential step in determining the tertiary structure of proteins in bioinformatics. The most complex challenge in the protein folding problem is the high dimensionality of feature vectors and the diversity of the protein fold classes. In Ibrahim et al. (2018), deep kernelized extreme learning machine (DKELM) and linear discriminant analysis are employed to solve this problem.

One of the most challenging tasks in protein fold recognition problem is the extraction of efficient features from the amino-acid sequences to obtain better classifiers. In Ibrahim et al. (2017), six descriptors have been proposed to extract features from protein sequences.

In another application of computer science algorithms, for drug discovery purposes, a machine learning-based method was proposed in Sajedi et al. (2018). It simplifies the recognition of Actinobacteria, at different stages of the growth phase, from a mixed culture to facilitate the isolation of novel strains of these bacteria. This method is based on Gabor transform and employs k-Nearest Neighbors and Naive Bayes, Logitboost, Bagging and Random Forest classifiers to automatically categorize the colonies.

## 4 Evaluation

Different researches in medical data hiding employ various ways to evaluate their proposed information hiding methods. In this section, we review these methods.

### 4.1 Databases

Most of the studies of information hiding methods in ECG like Edward Jero et al. (2014), Istepanian and Petrosian (2000), Ibaida et al. (2010) use MIT-BIH arrhythmia database for evaluation.

This well-known ECG database is collected by the Massachusetts Institute of Technology (MIT)-Beth Israel Hospital (BIH) Arrhythmia (Rubio et al. 2013). This ECG database consists of 48 two-lead ECG registers of 30 min duration. The sampling rate is 360 samples per second with a resolution of 11 bits per sample. Although the database was originally created as standard test material for the evaluation of arrhythmia detectors, this database is by far the most used to test and compare ECG compression algorithms and hiding information in the ECG signals.

In Joseph and Remya (2014), various ECG signals are used for experimentation and 12 ECG samples is used for evaluation. The set of samples consist of four normal (NSR) ECG samples, 4 Ventricular fibrillation ECG samples and four Ventricular Tachycardia ECG samples. Each sample is 10 s long with 250 Hz sampling frequency.

To evaluate the performance of the data-embedding method in Guo and Zhuang (2009), first, medical images from three different modalities, i.e., CT, MRI, and Ultrasound have been collected. The size of CT, MRI, and US images are 512 × 512 (12 bits), 256 × 256 (12 bits), and 640 × 480 (8 bits), respectively. These images include head CT and MRI images, L-Spine CT images, kidney Ultrasound images, etc.

In Ahson and Ilyas (2010) eight Computed Tomography (CT) medical images downloaded from (National Biomedical Imaging Archive) with the size of 512 × 512 were used as test images.

The watermarking algorithm in Chakraborty et al. (2013) hides information in the retinal images of DRIVE database (Staal et al. 2004).

The research of Rubio et al. (2013) uses three ECG databases. The first one is MIT-BIH Arrhythmia (Moody et al. 1988). The second ECG database is MIT-BIH Compression (Moody et al. 1988). It is composed of 168 two-lead ECG records of 20.48 s duration. The sampling rate is 250 samples/s with a resolution of 12 bits per sample. This database was created to cover different challenges for ECG compressors, in particular for lossy compression methods. Despite this fact, it is scarcely used to test the ECG compression algorithms, being relegated by MIT-BIH arrhythmia. Since these ECG databases are composed of two-lead recordings, the entire evaluation has been done on both leads and the results represent the average.

The third one is STUDY dataset (Delorme and Makeig 2004; Ullsberger and Delorme 2007) from the Swartz Center for Computational Neuroscience (SCCN), composed of 10 recordings from 5 different subjects, with 61 channels per frame, 820 frames per epoch and 220–235 epochs. The sampling rate of these recordings is 200 samples/s and the resolution is 11 bits per sample.

As with lossy compression of radiology images (Wong et al. 1995), there exists no legal standards for regulating how much distortion induced by watermarking system can be accepted. To be acceptable, a watermarking system requires thorough clinical validation tests. Such tests must be carried out on a large number of images and should involve a large number of clinicians to assure that the diagnostic accuracy is not jeopardized by such distortion.

## 4.2 Evaluation measures

In general, information hiding systems should be tested on a large number of objects drawn from a distribution similar to that expected in the application. Although, the information hiding systems should provide security measurements against malicious attacks and stealing of patient information, they should have other characteristic to be applicable in practice:

- The systems can produce acceptable distortion in the cover media.
- The resultant cover media after embedding should be proper for diagnoses, if it is used for diagnosis.
- The hidden data should be completely extracted.

Modification of a signal might become an issue in a malpractice suit. For example, it might be easy to convince that embedding must not change a doctor's interpretation of an image (Cox et al. 2008).

Medical images are generally used to help diagnose illnesses and other disorders. If we disregard for the moment the legal issues regarding medical imaging, any distortion that will not affect a diagnosis can be considered legitimate.

In some cases, a modified work that appears to be an acceptable copy of the original might in fact lead to different conclusions. In a critical field such as medical imaging, therefore, the division of distortions into legitimate and illegitimate groups should be based on controlled studies, rather than on subjective judgment.

Cox et al. define 'Illegitimate distortion' a distortion that makes a work invalid for some application. An example in medical imaging is a distortion that might lead a doctor to an incorrect diagnosis. This is in contrast to 'legitimate distortion' (Wu et al. 2015).

### 4.2.1 Performance evaluation measures for steganography methods

In literature, many steganography schemes are presented based on variety of parameters. Some of them work in spatial domain and other in transform domain. Irrespective of the approach used for data embedding, some common attributes need to be defined to evaluate the performance. These features can get more or less important depend on the application. Some of them can be defined as follow:

- Security against attack: the steganographic system may suffer from different types of stego attacks, allowing eavesdropper to retrieve secret message bits embedded in cover media. The system is said to be γ-secure if TP Rate − FP Rate $\leq \gamma$, where $0 \leq \gamma \leq 1$, and is said to be perfectly secure if $\gamma = 0$ (Subhedara and Mankar 2014). TP rate is the true positive (detecting stegos as stegos) rate of steganalyzers in detection of objects, which may be clean (cover) or stego. FP rate is the rate of detecting covers as stegos incorrectly.
- Payload capacity: it is defined in terms of number of secret bits that can be embedded per bit or Byte. Ideally, it should be as high as possible while maintaining the acceptable quality of the stego object. It is also known as hiding capacity or embedding capacity and is measured in terms of bits per pixel (i.e. for image) or bits per coefficient (for spatial and transform domain approach, respectively).
- Imperceptibility: steganography system should have high embedding capacity and capability to withstand against stego attacks. For example, the stego image should not have severe visual artifacts. There is a need to make the stego object has an as good as possible quality.

### 4.2.2 Performance evaluation measures for watermarking methods

For some watermarking applications, fidelity is the primary perceptual measure of concern. In these cases, the watermarked object must be indistinguishable from the original. An artist may require this of a transaction watermark or a patient may require this of a watermark applied to his or her medical images. However, there are applications of watermarking for which quality, rather than fidelity, is the primary perceptual concern (Cox et al. 2008).

- Embedding effectiveness: the effectiveness is the probability of detection after embedding. This definition implies that a watermarking system might have an effectiveness of less than 100%.
- Fidelity: in general, the fidelity of a watermarking system refers to the perceptual similarity between the original and watermarked versions of the cover object.
- Data payload: refers to the number of bits a watermark encodes within a unit of time or within an object. For a photograph, the data payload would refer to the number of bits encoded within the image. For audio, data payload refers to the number of embedded bits per second that are transmitted.
- Robustness: refers to the ability to detect the watermark after common signal processing operations. Examples of common operations on images include spatial fil-

tering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and so on). In some cases, robustness may be completely irrelevant, or even undesirable. In fact, an important branch of watermarking research focuses on fragile watermarks. A fragile watermark is one designed so that it is not robust. For example, a watermark designed for authentication purposes should be fragile. For example, any signal processing application applied to the image should cause the watermark to be lost.

There are other criteria to evaluate the performance of a watermarking algorithm, for example to evaluate the enhancement effect as well as visual quality of the watermarked images, the relative contrast error (RCE) defined in Gao et al. (2013) and Structural SIMilarity (SSIM) defined in Wang et al. (2004) are calculated besides the PSNR value. The RCE values greater than 0.5 indicate the enhanced contrast. The more structural similarity between the original and contrast-enhanced images, the SSIM value is closer to 1.

### 4.3 Clinical validation tests

If a steganography or watermarking method is used to hide some information in cover media like an ECG signal or a MRI image and these covers should be used for diagnosis, clinical validation tests can be used to ensure that these covers still can be used for diagnosis without causing any artificial perceptual changes. Clinical validation tests provide a subjective evaluation measure.

In the process of clinical validation tests a few specialist doctors try to discriminate between the cover media before and after data hiding, the clinical validation tests are successful if physicians cannot be able to distinguish between the cover media before and after data hiding.

In Joseph and Remya (2014) to validate diagnosability of the digitally processed ECGs, two specialist doctors were consulted. Twelve ECG Segments for both normal and abnormal cases were shown to them before and after watermarking, and after the removal of watermarks. They were asked the following questions:

- How similar is the original and the watermarked ECG?
- Can the watermarked ECG be used for diagnoses?

Both the specialist doctors admitted that the similarity is so high that the difference is undetectable and the both the watermarked and unwatermarked signals can be used for diagnoses. As a result, the ECG signal can still be used for diagnoses purposes after removing the watermark.

### 4.4 Statistical measures

Some objective criterion can be used for measuring the performance of information hiding applications. In the following, we review some of them.

- Percentage residual difference (PRD): to measure the difference between the original signal and the resulting signal as shown in Eq. (1):

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=0}^{N} (x_i - y_i)^2}{\sum_{i=0}^{N} {x_i}^2}}, \tag{1}$$

  where $x$ represents the original ECG signal, and y is the watermarked signal.
- Percentage RMS distortion (PRD) (Rubio et al. 2013): to measure the difference between the original signal and the resulting signal as in Eq. (2):

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=1}^{N} (x(n) - \tilde{x}(n))^2}{\sum_{i=1}^{N} (x(n) - \bar{x})^2}} \times 100, \tag{2}$$

  where $x(n)$ is the original signal, $\tilde{x}(n)$ is the reconstructed, $\bar{x}$ is the mean of the original signal and $N$ is its length.
- Bit error rate (BER): it has been used to evaluate the reliability of the extracted information, as shown in Eq. (3):

$$\mathrm{BER} = \frac{B_{\mathrm{err}}}{B_{\mathrm{total}}} \times 100, \tag{3}$$

  where BER represents the bit error rate in percentage, $B_{\mathrm{err}}$ is the total number of erroneous bits and $B_{\mathrm{total}}$ is the total number of bits.
- Peak signal to noise ratio (PSNR): high value of PSNR means that the stego object has high similarity to the cover (carrier) object. The mathematical representation of the PSNR is as Eq. (4):

$$\mathrm{PSNR} = 20 \log_{10}\left(\frac{\mathrm{MAX}_f}{\sqrt{\mathrm{MSE}}}\right), \tag{4}$$

  where the mean squared error (MSE) is obtained by Eq. (5), if the cover object is an image:

$$\mathrm{MSE} = \frac{1}{mn} \sum_{0}^{m-1} \sum_{0}^{n-1} ||f(i,j) - g(i,j)||^2. \tag{5}$$

  The dimensions of the cover image and the dimensions of the stego image must be identical.
- Kullback–Leibler divergence (KL) (Kullback 1987): is a non-symmetric measure of the difference between two probability distributions P and Q.

- Root mean square error (RMS): is a frequently used measure of the differences between values predicted by a model or an estimator and the values actually observed.

$$\mathrm{RMS} = \sqrt{\frac{(x(n) - \tilde{x}(n))^2}{N}}, \tag{6}$$

where $x(n)$ is the original signal, $\tilde{x}(n)$ is the reconstructed, and $N$ its length.

PRD is used to evaluate the proposed model in Joseph and Remya (2014). To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics, the percentage residual difference (PRD) has been used. In Joseph and Remya (2014) PRD is reported from 12 to 43% for minimum data size to maximum data size for different ECG signals.

In Nambakhsh et al. (2006), the proposed algorithm has been tested on several CT and MRI images and the PSNR between the original and watermarked image is greater than 35 dB for watermarking of 512–8192 bytes of the mark signal.

The performance of the method proposed in Edward Jero et al. (2014) is measured using metrics such as Kullback–Leibler divergence (KL), PRD, PSNR and BER. The research of Rubio et al. (2013) uses RMS and PRD to measure the signal distortion. The performance of the method proposed in Istepanian and Petrosian (2000) is measured in terms of BER, PRD, and visual clinical inspection.

The steganography technique presented in Ibaida et al. (2010), embeds confidential information of patients into specific locations of digital ECG host signal that will cause minimal distortion to ECG, and at the same time, any secret information embedded is completely extractable. Experiments illustrate that percentage residual difference (PRD) of watermarked ECGs can be as low as 0.0247 and 0.0678% for normal and abnormal ECG segments (taken from MIT-BIH Arrhythmia database) respectively.

The wavelet based steganography technique that has been introduced in Mu-Hsing and Kuo (2011), 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 this technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference (PRD) and the wavelet weighted PRD (WWPRD).

In Nambakhsh et al. (2006), the maximum PSNR of watermarked images is about 25.

## 5 Future applications of data hiding techniques in medical science

Healthcare covers complex processes of the diagnosis, treatment, and prevention of disease, injury, and other physical and mental impairments in humans. The patients' consumption of products and services provided by hospitals and other institutions forms the healthcare industry, which is one of the largest and fastest-growing parts of a country's economy.

It is widely accepted that the high quality healthcare services lie in the effectiveness and efficiency of health problem detection, innovative solution identification, and medical resource allocation (Mu-Hsing and Kuo 2011; Ahson and Ilyas 2010), which in turn depend heavily on the proper collection, management and utilization of health information (Stansfield 2005). Considering the fact that the health information collection and utilization may be distributed in multiple organizations, the medical data sharing plays the critical role in enabling the medical information flow across these organizations and then improving the quality of healthcare services.

Storing and sharing of medical data in the cloud environment, where computing resources including storage is provided by a third party service provider, raise serious concern of individual privacy for the adoption of cloud computing technologies. Existing privacy protection researches can be classified into three categories, i.e., privacy by policy, privacy by statistics, and privacy by cryptography. However, the privacy concerns and data utilization requirements on different parts of the medical data may be quite different.

The solution for medical dataset sharing in the cloud should support multiple data accessing paradigms with different privacy strengths. The statistics or cryptography technology alone cannot enforce the multiple privacy demands, which blocks their application in the real-world cloud (Yang et al. 2015).

Both from security aspect and from non-security aspect several threads can be active in the future. For instance:

- Invention of proper and special data hiding approaches for each cover type. Due to the different characteristics of various mediums for example ECG, EEG, CT or MRI images, different methods can be proposed or different existing data hiding methods can be employed.
- In the hospitals, usually some persons have responsibility to enter clinical and administrate information of patient in a database. To omitting human mistakes in data entry and reusing of this information specially the information, which are determinant in diagnosis such as images and signals, steganography methods can be

employed to avoid interchanging the patients' information. For example, information of the diabetic patients can be hidden in their retinopathy images.
- Producing data hiding algorithms that can be resistant to compression techniques.

Table 2 shows that in the recent years the application of watermarking and steganography algorithm in medical and healthcare systems has been increased. Watermarking is used mostly for preventing from tampering the data and steganography is generally used for hiding the patients' information in the medical signals or images. In common, cryptography lonely is used for authorization. Although, we observe that in some researches the combination of cryptography and watermarking or steganography can be used to provide more security.

There are some researches, which investigate the application of information hiding methods for non-security viewpoint. Some metadata can be embedded in a medium to help retrieval services and facilitate advanced searches. Furthermore, hiding information for example, patients' information in an objective medium can prevent some humanoid errors. For example, the research of Giannetti (2003) examines the impact of medical errors upon health care practitioners. Medical errors are viewed from the perspective of extreme job related and personal stress. A transactional model of stress comprised of both situational and appraisal variables are utilized to explain the unique coping problems of health care professionals when dealing with serious medical errors. The culture of medicine, unique ethical requirements, and societal expectations are examined as an integral part of the context of coping with errors. The debilitating emotional impact of catastrophic medical errors is a function of a culture of perfectibility, blame and the myth of an error free practice of health care. The belief in the utilitarian value of blame and punishment inhibits the open discussion and processing of errors, which could lead to better data for process and system change. Change in the socialization of health care providers and the culture of medicine as well as a supportive environment for practitioners who err are needed to address the systems aspect of medical errors and to offer assistance to practitioners who inevitably will commit error as part of working in a complex, highly technological health care system.

Steganography methods can be employed to prevent some of the medical errors encounter to the mistake of personnel. For example, if the patients' ID is embedded in radiography image, the human mistake of swapping the images can be avoided.

Figure 6 shows that body sensors collect different readings as well as ECG signal. This information can be sent in raw or after hiding information. The collected information can be sent to the network through the Bluetooth of the personal devices. The information hiding process is run in the

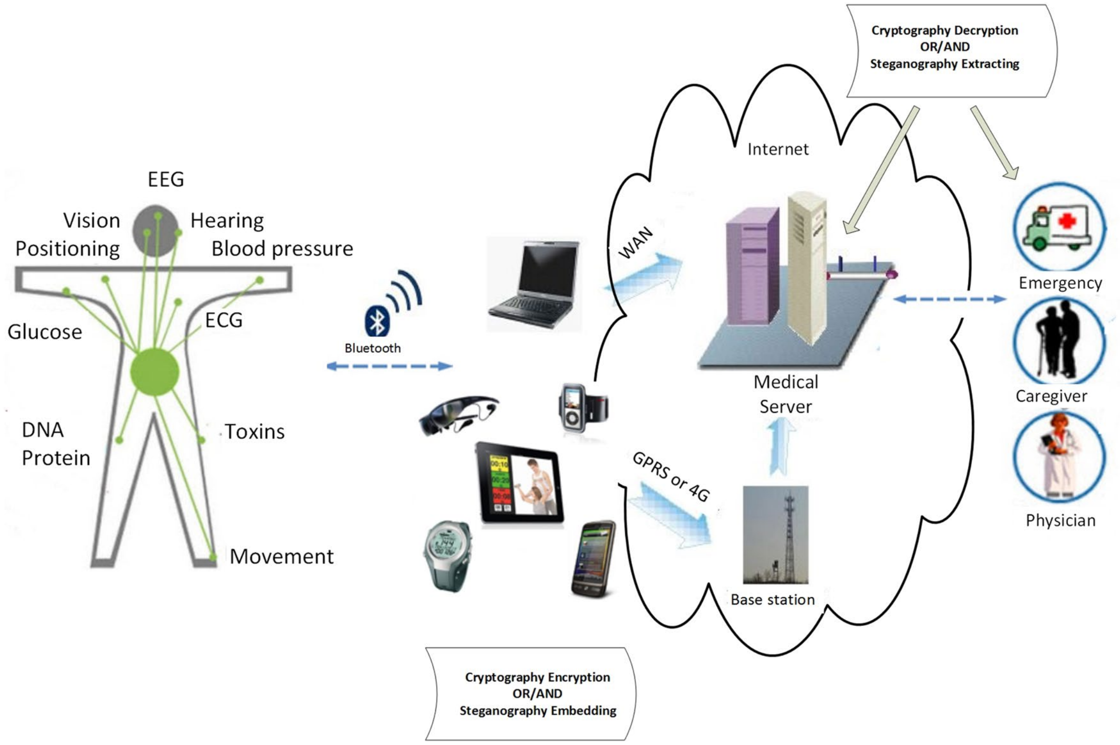

**Fig. 6** Body sensors collect different readings as well as ECG signal and the information hiding process implemented inside the patient's device

patient's device. This information can be stored in medical servers by the WAN or Internet technology of the mobile phones. The information can be extracted in the medical server and different action can be performed. For example, it can inform the emergency in case of obligation; call or inform the caregiver or report to the physicians. If a third party tends to sniff or manipulate the information (be passive or active attacker) transmits between patient's device and medical server, information hiding method can prevent it.

Authorization methods can be employed, usually by an encryption method, to prevent access of unauthorized person to the medical server information.

## 5.1 Challenges

The potential benefits of the e-health systems do not ignore the challenges that prevent the system from being fairly used. Security and privacy challenges of the e-health systems need to be understood and resolved. The potential advantages of the e- health systems have been considered over recent decades. However, because of its several challenges, the widespread usage of e-health systems is still at an early stage. Understanding the security as well as privacy issues are the key challenges in e-health systems. The principle that governs the patient–physician relationship is viewed as privacy. Patients are obligated to share required information with their physicians. However, they may decline to reveal important information as disclosure of some information may result in social stigma and discrimination (Kamal et al. 2017).

In case of using information hiding approaches, the selection of the right technique relies on time, memory, and security. Constraint about memory is highly important in case of small devices as they have low memory where the time is the most important factor for processing speed.

The constraints in medical and healthcare applications using steganography, watermarking, and cryptography are as the following:

- Time: how much time is needed for hiding and extracting the data and how much time is needed to fulfill the prerequisites before starting a hiding.
- Memory: the volume of the required memory is an important factor, especially in case of small devices such as PDAs, smart cards, RFID tags.
- Security: selected information hiding method scheme should meet one or more of the confidentiality, integrity (authentication, non-repudiation) and availability.
- Nature of data: it means how much the communicating information is confidential or important. If the size of information is small and the information is not much important; then any hiding scheme is suitable. If information is highly secret or important, then joint hybrid combination of schemes will be suitable.
- Type of data: for example, in case of video data, the privacy is more valuable and considerable constraint. If the data is small and in video format the previous described constrains (Time, memory, security) suggest the use of special mechanism. That is why the type of data constraint is a highly important constraint, which should not be neglected in the case of right selection of an information-hiding scheme.
- Volume of data: if the volume of data is large, high embedding capacity should be provided by the steganography methods and/or a large enough and proper cover media should be available.
- Transmission channel: some channels afford some security means. Based on the type of the channel a scheme for making secure communication can be designed.
- Sensitivity of the cover media: based on the significance of the data, different level of security can be developed.
- Cost: cost can be a combination of time, memory or other criteria.

Natural images, medical images, graphics, music, videos, and surveillance video all have very different statistics. The same is true of ECG, EEG, and EOG. Moreover, while these distributions are different from one another, they are also likely to be very different from the statistics of the watermark generation system. In the same way, the method of embedding by the steganography methods should be different.

## 5.2 Discussion

New innovative approaches in security that leverages big data analytics, learning models in combination with other technologies and policy best practices can help ensure information sharing across boundaries securely.

When an information hiding method is proposed for hiding a confidential data, the amount of the security should be measured. For example, it has been shown that in a modified image if the criterion PSNR is higher than 35 dB, the visual system of human cannot percept the changes enforced to the original image. In all the researches about hiding information in ECG signals, the security of the stego ECG signals is not evaluated.

Compression is a technique to reduce the size of data. Compression methods are divided to two categories: lossless and lossy. Increasing use of computerized ECG processing systems requires effective electrocardiogram (ECG) data compression techniques, which aim to enlarge storage capacity and improve data transmission over phone and internet lines. Some researchers studied compression of ECG signals (Ahmed et al. 2007). The research in Ahmed et al. (2007)

presents a compression technique for ECG signals using the Singular Value Decomposition (SVD) combined with Discrete Wavelet Transform (DWT). The central idea is to transform the ECG signal to a rectangular matrix, compute the SVD, and then discard small singular values of the matrix. The resulting compressed matrix is wavelet transformed, thresholded and coded to increase the compression ratio.

Many conventional watermarking/steganography algorithms introduce distortions in the original signals and suffer from the problem of low embedding capacity. Although, many established techniques have suppressed distortions. Modifications remain unacceptable for medical, military, and important records, where one wishes to maintain the original copies. Reversible watermarking, also called lossless data embedding, is developed for such sensitive applications. The reversible data hiding technique enables the exact recovery of original contents upon extraction of embedding data (Naheed et al. 2014).

Two main characteristics used to measure the performance of a reversible watermarking algorithm are watermark capacity, and imperceptibility. Watermark capacity is the amount of watermark information stored in the digital media, usually measured in bits or bits per pixels/time. Imperceptibility is related to the quality of cover. The watermark should be embedded in such way that it has no perceptible effect on the cover media. These two characteristics oppose each other, i.e. increase in one will decrease the other. So an optimum balance is needed between them.

Nowadays, it is widely accepted that the application of Information and Communication Technologies (ICT) in the healthcare environment leads to the improvement of care delivery, not only enhancing citizens' health but also including well-being and social care. Moreover, it increases the subjects' quality of life and independence as well as reducing rising healthcare costs in an ageing society (Calvillo et al. 2013).

### 5.3 Implementation considerations

If we used cryptography, the time complexity is high. In case of steganography or watermarking, the time complexity is lower than the cryptography. To increase the security a combination of cryptography and steganography/watermarking can be used. To increase the speed hardware accelerators can be employed.

If information hiding should be done on the patients' devices, the limitation in memory should be considered. Since the current tendency is building portable medical devices and wearable sensors, which often mount low power processors, the algorithms for encoding and protection should be as simple as possible to not overload them with complex calculations and reduce demand on the energy consumption of the battery. Moreover, rapid execution and transmission are the necessities to maintain the availability of the services at good levels and provide real-time services.

## 6 Conclusion

In this paper, some issues that endows with further attention on improving information security in healthcare are emphasized. Refining and improvement of healthcare outcomes is a key concern and focus for the healthcare industry. The healthcare industry is faced with important challenges resulting from the growing costs due to the rising of the number of patients, an aging population with a high incidence of chronic disease, the substantial shortage of medical professionals, process inefficiencies, and wastage. New healthcare approaches are trying to address many of these concerns.

In a applicable integrated healthcare environment, digital information systems such as a Hospital Information System (HIS), picture archive and communication systems, and EPR system play a more vital role than ever. Compared with its analogy counterpart, the digital representation of medical data has many advantages, such ease of compression and transmission, or image and signal enhancing. On the other hand, with current techniques, it is fairly straightforward for a malicious adversary to intercept or tamper sensitive medical data or confidential information when the public network (e.g., the Internet) is being used for telemedicine. It is a common view that there is a critical need of security measures in medical information systems.

Information security remains to be one of the critical issues facing any organization worldwide including health care. Information hiding techniques are in the initial of the path in medical applications. With the increasing number of aged population and the significant portion of that suffering from cardiac diseases, it is believable that remote ECG patient monitoring systems are expected to be used widely as point-of-care applications in hospitals. Consequently, enormous amount of ECG signal obtained and compiled by Body Sensor Networks from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature and glucose level. and diagnosed by those remote patient-monitoring systems. It is utterly important that patient confidentiality be protected while data is being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems.

These systems are designed to provide security measurements against malicious attacks and stealing of patient information. These techniques will provide privacy protection of medical data for telemedicine applications. These techniques have to be designed in such a way that guarantees least acceptable alteration in the medical data such as ECG signal or medical images.

## Compliance with ethical standards

**Conflict of interest** Author declares that they have no conflict of interest.

**Studies with human participants or animals** This article does not contain any studies with human participants or animals performed by the author.

## References

Aburturab M (2013) Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain. Opt Laser Technol 4:525–532

Ahmad T (2014) Shared secret-based steganography for protecting medical data. In: Proceedings of international conference on computer, control, informatics and its applications (IC3INA), pp 87–92

Ahmed SM, Al-Zoubi Q, Abo-Zahhad M (2007) A hybrid ECG compression algorithm based on singular value decomposition and discrete wavelet transform. J Med Eng Technol 31(1):54–61

Ahson SA, Ilyas M (2010) Cloud computing and software services theory and techniques. CRC Press, Boca Raton

Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Processing 13:1147–1156

AzamiSidek K, Mai V, Khalil I (2014) Data mining in mobile ECG based biometric identification. J Netw Comput Appl 44:83–91

Bacharova L, Bang L, Szathmary V, Mateasik A (2014) Imaging QRS complex and ST segment in myocardial infarction. J Electrocardiol 47(4):438–447

Boucsein W (2012) Electrodermal activity. Springer, Berlin, p 2 **(ISBN 978-1-461-41126-0)**

Bulling A et al (2009) Wearable EOG goggles: seamless sensing and context-awareness in everyday environments. J Ambient Intell Smart Environ 1(2):157–171

Calvillo J, Roman I, Roa LM (2013) Empowering citizens with access control mechanisms to their personal health resources. Int J Med Inf 82:58–72

Cavagnino D, Lucenteforte M, Grangetto M (2015) High capacity reversible data hiding and content protection for radiographic images. Sig Process 117:258–269

Celik MU, Sharma G, Tekalp AM, Saber E (2005) Lossless generalized-LSB data embedding. IEEE Trans Image Process 14:253–266

Chakraborty S, Samanta S, Biswas D, Dey N, Chaudhuri S (2013) Particle swarm optimization based parameter optimization technique in medical information hiding. In: Proceedings of IEEE international conference on computational intelligence and computing research

Chao HM, Hsu CM, Miaou SG (2002) A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6:46–53

Chaoab H, Twua S, Hsu C (2005) A patient-identity security mechanism for electronic medical records during transit and at rest. Med Inf Internet Med 30(3):227–240

Coatrieux G, Maitre H, Sankur B (2001) Strict integrity control of biomedical images. In: Proceedings of SPIE security and watermarking of multimedia

Correa MAgustinaG, Leber EL (2011) Noise removal from EEG signals in polisomnographic records applying adaptive filters in cascade, adaptive filtering applications, Chap. 8. InTech, Croatia

Cox IJ, Miller ML, Bloom JA, Fridrich J (2008) Ton Kalker digital watermarking and steganography. Morgan Kaufmann, Burlington

Crichtona JHM (2009) Defining high, medium, and low security in forensic mental healthcare: the development of the Matrix of Security in Scotland. J Forensic Psychiatry Psychol 20(3):333–353

Dao T, Pouletaut P, Charleux F, Lazáry Á, Eltes P, Varga P, Ho Ba Tho M (2015) Multimodal medical imaging (CT and dynamic MRI) data and computer-graphics multi-physical model for the estimation of patient specific lumbar spine muscle forces. Data Knowl Eng 96–97:3–18

De la Rosa Algarin A, Demurjian S, Berhe S, Pavlich-Mariscal J (2012) A security framework for xml schemas and documents for healthcare. In: Proceedings of IEEE international conference on bioinformatics and biomedicine workshops, pp 782–789

Delbarpour S, Sajedi H (2017) Image steganography with artificial immune system. In: 7th joint conference on artificial intelligence and robotics and the 9th RoboCup IranOpen International Symposium

Delorme A, Makeig S (2004) EEGLAB: an open source toolbox for analysis of single trial EEG dynamics including independent component analysis. J Neurosci Methods 134:9–21

Edward Jero S, Ramu P, Ramakrishnan S (2014) Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. J Med Syst 38(10):132–140

Eisenberg RL, Margulis AR (2011) A patient's guide to medical imaging. Oxford University Press, Oxford **(ISBN 978-0-19-972991-3)**

Electroencephalogram (EEG) (2018). http://hopkinsmedicine.org/healthlibrary/test_procedures/neurological/electroencephalogram_eeg_92,p07655/. Accessed 4 Aug 2018

Engin M, Cidam O, Engin EZ (2005) Wavelet transformation based watermarking technique for human electrocardiogram (ECG). J Med Syst 29(6):589–594

Fernandez-Aleman JL, Carrion Seor I, angel Oliver Lozoya P, Toval A (2013) Security and privacy in electronic health records: a systematic literature review. J Biomed Inform 46:541–562

Gao MZ, Wu ZG, Wang L (2013) Comprehensive evaluation for HE based contrast enhancement techniques. Adv Intell Syst Appl 2:331–338

Gavrovska A, Bogdanović V, Reljin I, Reljin B (2014) Automatic heart sound detection in pediatric patients without electrocardiogram reference via pseudo-affine Wigner–Ville distribution and Haar wavelet lifting. Comput Methods Programs Biomed 113(2):515–528

Ghazvini A, Shukur Z (2013) Security challenges, and success factors of electronic healthcare system. In: Proceedings of 4th international conference on electrical engineering and informatics (ICEEI 2013), pp 212–219

Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Multiple image watermarking applied to health information management. IEEE Trans Inf Technol Biomed 10:722–732

Giannetti V (2003) Medical errors: the hidden victim. Clin Res Regul Affairs 20(4):425–432

Gkoulalas-Divanis A, Loukides G, Sun J (2014) Publishing data from electronic health records while preserving privacy: a survey of algorithms. J Biomed Inform 50:4–19

Goljan M, Fridrich J, Du R (2001) Distortion-free data embedding for images. In: Proceedings of 4th information hiding workshop, pp 27–41

Golpira H, Danyali H (2010) Reversible blind watermarking for medical images based on wavelet histogram shifting. In: Proceedings of IEEE international symposium on signal processing and information technology (ISSPIT), pp 31–36

Gritzalis S, Iliadis J, Gritzalis D, Spinellis D, Katsikas S (1999) Developing secure web-based medical applications. Med Inf Internet Med 24(1):75–90

Gritzalisa D, Katsikasa S, Keklikoglou J, Tomaras A (1991) Data security in medical information systems: technical aspects of a proposed legislation. Med Inf 16(4):371–383

Guo X, Zhuang T (2003) A lossless watermarking scheme for enhancing security of medical data in PACS. In: Proceedings of SPIE and medical imaging, pp 350–359

Guo X, Zhuang T (2009) A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64

Hafizah Hassan N, Ismail Z (2012) A conceptual model for investigating factors influencing information security culture in healthcare environment. International Congress on Interdisciplinary Business and Social Science

Hu F, Jiang M, Wagner M, Dong D (2007) Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/software code sign. IEEE Trans Inf Technol Biomed 11(6):619–627

Ibaida A, Khalil I, Al-Shammary D (2010) Embedding patients confidential data in ECG signal for healthcare information systems. In: Proceedings of IEEE engineering in medicine and biology society

Ibrahim W, Saniee M, Abadeh (2017) Extracting features from protein sequences to improve deep extreme learning machine for protein fold recognition. J Theor Biol 421:1–15

Ibrahim W, Saniee M, Abadeh (2018) Protein fold recognition using deep kernelized extreme learning machine and linear discriminant analysis. Neural Comput Appl 1–14. https://doi.org/10.1007/s00521-018-3346-z

Istepanian RS, Petrosian AA (2000) Optimal zonal wavelet-based ECG data compression for a mobile telecardiology system. IEEE Trans Inf Technol Biomed 4(3):200–211

Joseph T, Remya UL (2014) ECG steganography based privacy protection of medical data for telemedicine application. J Dent Med Sci 13(8):85–94

Kamal S, Khan M (2014a) An integrated algorithm for local sequence alignment. Netw Model Anal Health Inf Bioinf 3:68

Kamal Md, Khan M (2014b) Chapman–Kolmogorov equations for global PPIs with discriminant-EM. Int J Biomath 07(05):1450053

Kamal MdS, Khan M, Dev K, Chowdhury L, Dey N (2016) An optimized graph-based metagenomic gene classification approach: metagenomic gene analysis, classification and clustering in biomedical signal processing, IEG Global Publisher, pp 290–314

Kamal MdS, Chowdhury L, Khan M, Ashour AS, Tavares J, Dey N (2017a) Hidden Markov model and Chapman Kolmogrov for protein structures prediction from images, Comput Biol Chem 68:231–244

Kamal MdS, Sarowar MdG, Dey N, Ashour AS, Ripon SH, Panigrahi BK, Tavares JRS (2017b) Self-organizing mapping based swarm intelligence for secondary and tertiary proteins classification. Int J Mach Learn Cybern:1–24

Kamal MdS, Dey N, Ashour AS (2017c) Large scale medical data mining for accurate diagnosis: a blueprint, handbook of large-scale distributed computing in smart healthcare. Scalable computing and communications. Springer, Cham

Kamal MdS, Dey N, Nimmy S, Ripon S, Ali N, Ashour A, Karaa W, Nguyen G, Shi F (2018) Evolutionary framework for coding area selection from cancer data. Neural Comput Appl 29(4):1015–1037

Kaur S, Singhal R, Farooq O, Ahuja B (2010) Digital watermarking of ECG data for secure wireless communication. In: Proceedings of international conference on recent trends in information, telecommunication and computing, pp 140–144

Khan M, Kamal MS (2015) Performance evaluation of Warshall algorithm and dynamic programming for Markov chain i0 local sequence alignment. Interdiscip Sci 7(1):78–81

Khokhar RH, Chen R, Fung BCM, Man Lui S (2014) Quantifying the costs and benefits of privacy-preserving health data publishing. J Biomed Inform 50:107–121

Kullback S (1987) Letter to the editor: the Kullback–Leibler distance. Am Stat 41(4):340–341

Li M, Yu S, Zheng Y, Ren K, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute based encryption. IEEE Trans Parallel Distrib Syst 24(1):131–143

Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gotzsche PC, Ioannidis JPA et al (2009) The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. J Clin Epidemiol 62(10):e1–e34

Lin JC (1999) Applying telecommunication technology to health care delivery. IEEE Eng Med Biol Mag 18(4):28–31

Malashree KS, Jagadish KN, Suma M (2014) Confidential data hiding using wavelet based ECG steganography. Int J Eng Res Appl 4(5):84–88

Mazurczyk W, Szczypiorski K, Lubacz J (2013) 4 new ways to smuggle messages across the internet. IEEE Spectr 50(11):42–4523

Moody G, Mark R, Goldberger A (1988) Evaluation of the 'TRIM' ECG data compressor. In: Proceedings of computers in cardiology, pp 167–70

Mu-Hsing A, Kuo (2011) Opportunities and challenges of cloud computing to improve health care services. J Med Internet Res 13(3):e67

Naheed T, Usman I, Khan TM, Dar AH, Shafique M (2014) Intelligent reversible watermarking technique in medical images using GA and PSO. Optik 125:2515–2525

Nambakhsh MS, Ahmadian A, Ghavami M, Dilmaghani RS, Karimi-Fard S (2006) A novel blind watermarking of ECG signals on medical images using EZW algorithm. In: Proceedings of IEEE engineering in medicine and biology society, pp 3274–3277

National Biomedical Imaging Archive. http://imaging.nci.nih.gov. Accessed 28 Apr 2018

Nimmy S, Kamal MdS, Hossain MI, Dey N, Ashour AS, Shi F (2017) Neural skyline filtering for imbalance features classification. Int J Comput Intell Appl 16(03):1–25

Omotosho A, Adegbola O, Olayemi Mikail O, Emuoyibofarhe J (2014) A secure electronic prescription system using steganography with encryption key implementation. Int J Comput Inf Technol 3(5):980–986

Pangalos GJ (1995) Design, and implementation of secure medical database systems. Med Inform 20(3):265–277

Pangalosa GJ (1993) Medical database security evaluation. Med Inform 18(4):283–292

Phukpattaranont P (2015) QRS detection algorithm based on the quadratic filter. Expert Syst Appl 42(11):4867–4877

Poremba S (2015) Cyber security is growing importance for medical devices too. Forbes magazine. 1/19/2015

Rao NV, Kumarib VM (2011) Watermarking in medical imaging for security and authentication. Inf Secur J 20(3):148–155

Rubio OJ, Alesanco A, Garcia J (2013) Secure information embedding into 1D biomedical signals based on SPIHT. J Biomed Inform 46:653–664

Said A, Pearlman W (1996) A new fast and efficient image codec based on set partitioning in hierarchical trees. IEEE Trans Circ Syst Video Technol 6(3):243–250

Sajedi H, Jamzad M (2009a) Adaptive batch steganography considering image embedding capacity. Opt Eng 48(8):1–10

Sajedi H, Jamzad M (2009b) Secure steganography based on embedding capacity. J Inf Secur 8(6):433–445

Sajedi H, Jamzad M (2010a) HYSA: hybrid steganographic approach using multiple steganography methods. Secur Commun Netw 4(10):1173–1184

Sajedi H, Jamzad M (2010b) BSS: boosted steganography scheme with cover image preprocessing. Expert Syst Appl 37:7703–7710

Sajedi H, Mohammadipanah F, Shariat Panahi HK (2018) An image analysis-aided method for redundancy reduction in differentiation of identical actinobacterial strains. Future Microbiol 13(3):313–329

Shapiro JM (1993) Embedded image coding using zerotrees of wavelet coefficients. IEEE Trans Signal Proces 41(12):3445–3462

Shoukat IA, Bakar KA, Iftikhar M (2011) A survey about the latest trends and research issues of cryptographic elements. Int J Comput Sci Issues 8(3):140–149

Srinivasan Y, Nutter B, Mitra S, Phillips B, Ferris D (2004) Secure transmission of medical records using high capacity steganography. In: Proceedings of 17th IEEE symposium on computer-based medical systems

Staal JJ, Abramoff MD, Niemeijer M, Viergever MA, van Ginneken B (2004) Ridge based vessel segmentation in color images of the retina. IEEE Trans Med Imaging 23:501–509

Stansfield S (2005) Structuring information and incentives to improve health. Bull World Health Organ 83(8):562

Stokes M, Blythe M (2001) Muscle Sounds in physiology, sports science and clinical investigation. Medintel, Oxford **(ISBN 0-9540572-0-1)**

Subhedara MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13(14):95–113

Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circ Syst Video Technol 13:890–896

Traver V, Monton E, Bayo JL, Garcia JM, Hernandez J, Guillen S (2003) Multiagent home telecare platform for patients with cardiac diseases. In: Proceedings of computing in cardiology, pp 117–120

Tupakula U, Varadharajan V (2013) security techniques for counteracting attacks in mobile healthcare services. In: Proceedings of 3rd international conference on current and future trends of information and communication technologies in healthcare, pp 374–381

Tzelepi S, Pangalos G, Nikolacopoulou G (2002) Security of medical multimedia, medical informatics and the internet in medicine. Taylor & Francis, London, vol 27, no 3, pp 169–184

Ullsberger P, Delorme A (2007) EEGLAB study set. http://tinyurl.com/bsdkyaj. Accessed May 2012

Vargheese R, Prabhudesai P (2014) Securing B2B pervasive information sharing between healthcare providers: enabling the foundation for evidence based medicine. International Workshop on Privacy and Security in HealthCare (PSCare14), pp 525–530

Vleeschouwer C, Delaigle JF, Macq B (2003) Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans Multimed 5:97–105

Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error measurement to structural similarity. IEEE Trans Image Process 13(1):600–612

Wang H, Peng D, Wang W, Sharif H, Chen H, Khoynezhad A (2010) Resource-aware secure ECG healthcare monitoring through body sensor networks. Wirel Commun 17(1):12–19

Wong S, Zaremba L, Gooden D, Huang HK (1995) Radiologic image compression—a review. In: Proceedings of the IEEE, vol 83, no 2, pp 194–219

Wu H, Huang J, Shi Y (2015) A reversible data hiding method with contrast enhancement for medical images. J Vis Commun Image Retriev 31:146–153

Yang J, Li J, Niu Y (2015a) A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Syst 43:74–86

Yang J, Qiang Li J, Niu Y (2015b) A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Systems 44:74–86

Zehl L, Jaillet F, Stoewer A, Grewe J, Sobolev A, Wachtler T, Brochier TG, Riehle A, Denker M, Grun S (2016) Handling metadata in a neurophysiology laboratory. Front Neuroinform 10:26

Zhao S, Aggarwal A, Frost R, Bai X (2012) A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Commun Surv Tutor 14(2):380–400

Zheng K, Qian X (2008) Reversible data hiding for electrocardiogram signal based on wavelet transforms. In: Proceedings of international conference on computational intelligence and security

Zhou XQ, Huang HK, Lou SL (2001) Authenticity, and integrity of digital mammography images. IEEE Trans Med Imaging 20:784–791

Zhou Z, Huang HK, Liu BJ (2005) Digital signature embedding (DSE) for medical image integrity in a data grid off-site backup archive. In: Proceedings of SPIE and Medical imaging, pp 306–317