ROBUST WATERMARKING METHOD FOR SECURE TRANSMISSION OF MEDICAL IMAGES IN EHR SYSTEMS

Abderrahmane Daham and Mohamed ouslim

University of Science and Technology of Oran (USTO)

ABSTRACT

Confidentiality of Electronic Health Record (EHR) and privacy are two important security requirements for healthcare systems. Many devices on the EHR network utilize little or no encryption, which makes data in transit vulnerable to exploitative attacks, such as Man-in-the-Middle and other filtration methods. Recently, watermarking algorithms as an efficient response to these requirements is in the underline. In this paper, we present a robust watermarking method conceived as part of an Electronic Health Record platform. In this method a chaotic encryption and blind medical image watermarking technique was incorporated into the system as an authorization mechanism to ensure confidentiality and integrity of electronic health information. We present a hybrid watermarking method based on a combination of discrete wavelet transform (DWT), hessenberg Decomposition (HD), Singular value decomposition (SVD) and an original chaos crypto system based on the Arnold Transform (AT) of Singular Value Decomposition. In order to spread the robustness of our algorithm and provide additional security, an improved SVD-AT embedding and extraction procedure has been used to scramble the EHR data in the preprocessing step of the proposed method. In the process of watermark embedding, an R-level discrete wavelet transform was applied to the host image. The low frequency wavelet coefficients are selected to carry this scrambled-watermark. In extraction process, the stored used plain image is obtained from the trusted authority server to complete the verification process. The receiver should compare the unsigned watermark with the extracted watermark again. The verification can be done before clinical procedures and diagnosis. The proposed watermarking method endures entirety attacks and rightly extracts the hidden watermark without significant degradation in the image quality, thus, when the Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) performance of the proposed algorithm is performed.

KEYWORDS

Watermarking, medical image, discrete wavelet transform, singular value decomposition, Arnold Transform, e-health, chaos, hessenberg Decomposition, EHR Modeling.

1. INTRODUCTION

E-Health is the cost-effective and secure use of information and communication technologies (ICT) in support of health and health-related fields. The term was apparently first used by industry leaders and marketing people rather than academics. They created and used this term in line with other e-words; such as e-commerce, e-business, e-solutions, and so on, in an attempt to convey the promises, principles, excitement (and hype) around e-commerce (electronic commerce) to the health arena. Most hospitals and health care systems involve a lot of data storage and transmission, such as medical images, patient information, and administrative documents. Among these data, the patient information and medical images need to be protected against any malicious attempts. Three things are required to protect patients' information from being compromised: the integrity, privacy, and authenticity of medical images [1]. Digital

watermarking is a form of data hiding, describes the process of embedding information, for example, a number or a text or an image, into the digital media, such as a piece of audio, video, or image, to protect the copyright, benefit of the investor, and legal rights of owners. Today, with the rapid growth of the Internet, copyright laws are no longer effective, as many copyrighted products such as pictures, music, and videos are available in digital form. However, content owners also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high-capacity digital recording devices. The Internet is a great distribution strategy for digital media since it is inexpensive eliminates warehousing and stock, and delivery is almost immediate. Any unauthorized party that can produce identical copies of digital data without degrading the original content and distribute the copies on the network. Content owners also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high-capacity digital recording devices. When the only way the average customer could record a movie or a song was on analog tape, pirated copies were typically of a lower quality than the originals, and the quality of second-generation pirated copies (i.e., copies of a copy) was generally much reduced. However, with digital recording devices, songs and movies can be recorded with little, if any, degradation in quality. Using these recording devices and using the Internet for distribution, would-be pirates can easily record and distribute copyright protected material without appropriate compensation being paid to the actual copyright owners. As a result, there is a high demand for reliable and secure digital data distribution over networks. Such a technique designed to solve this problem is the digital watermarking. Digital watermark is a process in the digital domain that incorporates a watermark into copyrighted digital data to protect its value, so it cannot be used by unauthorized parties. The first owner of technological content turn towards is the cryptography. Encryption is probably the most common way to protect digital content. It is certainly one of the best developed as a science. The content is encrypted before delivery, and a decryption key is provided only to individuals who have purchased legitimate copies of the content. The encrypted file can then be made public on the Internet, but would be useless to a pirate without an appropriate key. Unfortunately, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. Encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. A hacker can actually buy the product, use the decryption key to get a non-protected copy of the content, and then proceed to distribute illegal copies. Therefore, cryptography can protect content in transit, but once decrypted, the content has no further protection. Thus, there is a strong need for an alternative or complement to cryptography: a technology that can protect content even after it is decrypted. Watermarking has the potential to fulfill this need because it places information within the content where it is never removed during normal usage. A watermark can be designed to withstand all of these processes: decryption, re-encryption, compression, digital-to-analog conversion, and file format changes. A watermark can be designed to survive all of these processes. Watermarking has been considered for many copy prevention and copyright protection applications. In copy prevention, the watermark could be used to inform software or hardware that copying should be limited. In copyright protection applications, the watermark may be used to identify the copyright holder and ensure proper payment of royalties. Although copy prevention and copyright protection have been major driving forces behind research in the watermarking field, there is a number of other applications for which watermarking has been used or suggested. These include broadcast monitoring, transaction tracking, copy control, and device control [2]. A medical image is a requirement for sharing in which the confidential data of the patient should be protected from unauthorized access, sharing them over the internet has become very popular nowadays for telediagnosis, telesurgery, and teleconsultation [2]. At present, medical images represent a significant percentage of the total medical information in hospitals, and digital information management systems are playing an increasingly important role in the modern medical system. However, with the popularization and application of the Internet, there are more and more information security problems. When we transmit the diagnosis medical images through the Internet, the patients' personal information recorded on the medical images is subject to

counterfeiting, tampering, or disordering. Digital watermarking of medical images, which involves encoding personal data as a digital watermark, can effectively solve this issue [3].

2. AN OVERVIEW OF DIGITAL WATERMARKING:

The watermark is closely related to the data, as opposed to simply being stored in the image's file's header. The watermarking embedder creates the watermarked image by fusing cover data with the watermark image (Data to hide). The purpose is the authenticity or copyright of this digital media [4]. The structure of a digital watermarking compose from two primary components: the first stage is the watermark embedding (marking), and the second is the watermark detection and extraction. The embedding algorithm takes the signature and the clear document in addition to generate the watermarked document. In this case, secret or public keys and other parameters like a scaling factor α (strong coefficient) can be used to extend the watermarking embedded. Figure (**1**) shows the embedding and the extraction operations.

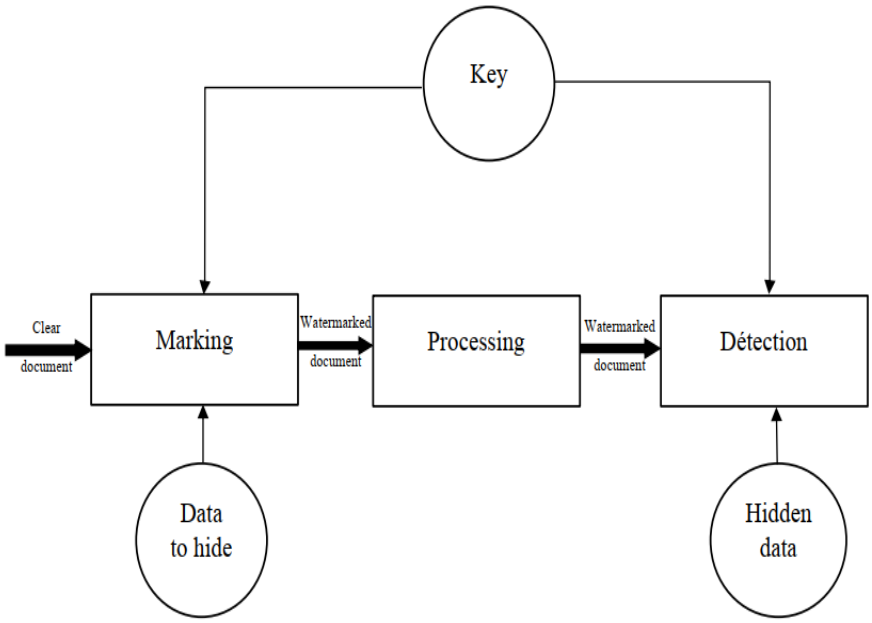

Fig 1. Watermarking system

2.1. The properties of a high-performance digital watermarking system

The transmission of medical images between hospitals, located at various locations and different administrative organizations has become common practice for many reasons. The security requirements for medical information derive mainly from legislative rules and strong security policy ethics, which the professionals and patients concerned, must follow [5]. The basic requirement of digital watermarking is closely linked to its purpose applications, different application has different request. In global, the requirements of a digital watermarking system, whose simultaneous presence distinguishes it from the other data hiding techniques, are as follows:

- Transparency: A prerequisite for any watermarking method is that it is transparent to the receiving user. Watermarked content must be properly visible on the device of the authorized user. The watermark is only visible in the watermark detector.

- Facility of embedding and retrieval: simplicity of integration and retrieval: preferably, the watermark on the digital media must be able to be performed automatically. The computational need for the selected algorithm must be reduced.

- Robustness: It represents the power to recover the inserted mark even if the watermarked image has been manipulated by attacks or unauthorized access. Any attempt, whether intentional or not, that has a potential to alter the data content is considered as an attack. Studies in this direction did not take into account the malicious nature of the attack, nor the means and determination of the attacker to want to destroy the mark or replace it. To this end, the concept of security has emerged.

- Security: Only authorized parties have access to the watermark information. The watermark information should only be available to them. The authorized parties have the authority to change the content of the watermark. Encryption is an effective way to prevent unauthorized access to watermarked data.

- Effect on bandwidth: Watermarking should be done in such a way that it does not increase the amount of bandwidth required for transmission. Watermarking will be refused if it becomes a burden on the available bandwidth.

- Interoperability: Digitally watermarked content must be interoperable so that it may be accessed effortlessly across heterogeneous networks and played on a variety of playback devices, both aware and oblivious of the watermark.

2.2. Classifications of Watermarking Systems

Watermarking can be applied to different types of data, such as text, image, audio and video. Watermarking approaches can be designed in the following domains: the spatial domain (array of pixels), the frequency domain (transforms) and hybrid. According to human perception, watermarking can be categorized into visible, invisible approaches

2.2.1. Classification based on visual perception

Besides watermark robustness, watermarks can be classified into some types. From the visibility point of view, watermarks can be clustered into visible and invisible types. Visible watermarks are perceptible to a viewer like logos, which are inserted into or overlaid on images. On the other hand, invisible watermarks are imperceptible and don’t change the visual appearance of the images. In our work, we are interested in invisible watermarks, taking into account the privacy of patient information; we have to embed the personal information into medical images as a digital watermark.

a) Visible watermarks

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image, but they are transparent. Such watermarks cannot be removed by cropping the middle part of the image. Furthermore, such watermarks are shielded from statistical analysis. The drawbacks of visible watermarks are that they degrade the quality of the image and can only be detected visually. Therefore, it's hard to locate them. by dedicated programs or devices. Such watermarks have applications in graphics, maps, and software user interfaces.

b) Invisible watermark

An invisible watermark is hidden in the content and designed to be beyond normal human observation. Normal human vision cannot distinguish between the original and the protected information. Diverse watermarks are used for content and/or author authentication and for detecting unauthorized copies. It is designed to be imperceptible to be undetectable by any unauthorized parties but detectable by an authorized agency only helping the owner to claim if a copyright infringement happens.

2.2.2. Classification according to the field of insertion

The insertion domain is defined as the digital representation of the image. Currently, the research in the field of medical image watermarking mainly revolves around two aspects: the spatial domain and the transform domain. Common transform domains include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), etc. They all embed watermarks through changing certain pixel gray levels or some of the coefficient values of the transform domain. Being small in calculation and compatible with international data compression standards (JPEG, MPEG), the DCT is now the hotspot in the research field of frequency domain digital watermarking algorithms. In view of the special requirements for the protection of medical image focal zones, general literature often chooses to embed watermark information into the Region of Non-Interest (RONI) of the image. The Region of Interest (ROI) of medical images refers to the focal zones of major pathological features or clinic information, and the embedding of watermark into the ROI may result in misdiagnosis. However, the identification of ROI often requires much time and energy, and a mistake in this process can negatively affect the doctor's diagnosis [6]. Finally the Techniques based on the combination of domains spatial and frequencies to provide more marks and minimize distortion of the watermarked image. They are based on brand insertion algorithms in the combination of two spatial and frequency domains. The principle is to partition the mark of the host image into two parts, respectively, for the spatial insertion and the frequency insertion which are carried out according to the user's preference and the importance of the data.

The remainder of this paper is organized as follows: Section 3 provides the related research that includes a brief summary of recent methods combining watermarking and cryptography. In Section 4 we present the basic theory methods which aims to build our system of watermarking. Use case modeling in analyzing and designing electronic health systems was examined; also the methods of watermark embedding and extraction procedures are discussed in Section 5. The experimental results are given in Section 6. Finally, Section 7 gives the conclusions.

3. RELATED WORK

There are techniques in the literature combining watermarking and cryptography to ensure a high level of security for the transmission of medical images. In this section, we present the state of the art of the different existing methods that combine watermarking and cryptography. The research of medical images needs to tackle the problem of disclosing and changing patients' information or privacy in the process of watermark extracting. The proposed algorithm mainly employs scrambling technology to provide secondary encryption to protect the medical watermark information and enhance the privacy of the watermark of a medical image. It also uses the image's phase properties to balance the watermark's invisibility and robustness. Given below is some of the related research:

Puech et al. [7] proposed a method that combines image encryption and watermarking techniques for secure transmission of medical images. This method is based on the combination of private keys, public keys, secret key encryption and watermarking. The encryption algorithm with a secret key is applied to the image. The secret key is encrypted with a key-based encryption public-private method then this secret key is embedded in the encrypted image using the discrete cosine transform watermarking method.

Macq [8] proposes using a hash function to obtain a header identifier. This identifier is then inserted into the image using a reversible marking method. This method is based on the use of an original, lossless multi-resolution transform by which a pair of pixels is bijectively transformed into a pseudo-sum/pseudo-difference pair. Macq inserts M bits (128 or 160, depending on the hash function used) in the domain resulting from this transform. Authentication itself is performed by recalculating the summary of the header and comparing it to that extracted from the image.

Ray et al. [9] proposed a watermarking technique based on the Rivest – Shamir – Adleman (RSA) algorithm. Using first level DWT, multiple frequency subbands of the host image are retrieved, whereas SVs of the watermark are attained, which are further encrypted with the help of the RSA algorithm. These encrypted SVs of watermark image are embedded into SVs of the transformed host image. Though it appears that the created method achieves minimal imperceptibility, the fact that it employs the RSA algorithm strengthens the security of the scheme.

Rajendra Acharya et al [10] proposed a technique to interleave patient information text and graphic documents for efficient storage. The mark is designed to interleave patient information with medical images during JPEG compression, reducing storage and transmission overhead. Text data is encrypted using a logarithmic technique before being interleaved with images in the frequency domain to ensure greater security. Graphics signals are also interlaced with the image. The technique has been tested for different images.

Kaur et al. [11] proposed a new approach of image watermarking using the Arnold Transform and dual tree complex wavelet transform (DTCWT). DTCWT is used to decompose a host image into several sub-bands, and DTCWT is often used to decompose an encrypted watermark image in a similar way, whereas Arnold Transform is used to encrypt the watermark. Further embedding processes are done for all sub-bands especially while inverse DTCWT leads to the generation of a watermarked image. However, the developed technique turns out to be a non-blind scheme that requires the original host image in the extraction process. Where authors have highlighted the salient features of a variety of watermarking approaches, this actually aids researchers in providing a roadmap for developing new watermarking techniques.

Researchers have proposed a novel dual image watermarking technique in [12] where R Level DWT, the nonsubsampled contourlet transform (NSCT), Arnold Transform, and Singular Value Decomposition (SVD) transforms are effectively used. Dual image watermarks are embedded in this methodology, whereas set partitioning in a hierarchical tree (SPIHT) algorithm is employed successfully for compressing the watermarked image.

Naheed et al. [13] proposed a watermarking technique for medical image using interpolation and a genetic algorithm (GA). In this scheme, the watermark embedding locations were calculated using interpolation and a GA. After getting the best locations, the watermark image was inserted into those locations of the original medical image to achieve the watermarked image. In image encryption technology, the scrambling transform is the process to obfuscate or remove sensitive information, it is frequently deployed in the preprocessing stage of the watermark. A meaningful

watermark image will become meaningless after scrambling transformation. Without knowing the algorithm for scrambling or the key, the watermark can't be restored by the attacker even after successful extraction of water mark. Thus, the digital image is further secured by secondary encryption. Furthermore, after the scrambling transformation, the incidence relation between the positions of the pixel of the image will be evenly distributed in the carrier image space. In this way, we can improve the robustness of the algorithm. The two-level image scrambling algorithm using Arnold transform can be applied. The original image can be retrieved by applying the inverse Arnold transform to the scrambled image after a corresponding number of iterations. The Arnold transform is cyclical. That is to say, it can retrieve the original image at the certain of iteration. This number of iterations and order of scrambling increase the complexity of malicious decryption. Therefore, without the knowledge of its cycle and number of iteration, we will not be able to recover the original image. Through scrambling transformation, the key and the number of iteration can be turned into the private key. At the same time, the number of iteration in scrambling transformation depends upon the effect of scrambling and recovery required by different images [14].

Selecting Major Visual Feature Vectors against Geometric Attacks Currently, the main reason for the low resistibility of most medical image watermarking algorithms is the following fact: in the embedding process the digital watermark into pixels or transform coefficients, the slight geometric transformation of the medical image can cause a significant change in pixel values or transform coefficient values. Therefore, the inserted watermark would become vulnerable to attacks. If we can identify visual feature vectors reflecting the geometric characteristics of the image, the visual feature value of the image will not be seriously affected in the case of slight geometric transformation of the image. The study of Hayes showed that the phase is more important than the amplitude in terms of the image feature.

Such kind of watermark signal boasts cryptography security. Meanwhile, the embedded watermark is zero watermark in real sense and will not the quality of medical image, thus effectively solving the problems in embedding and extracting of medical image watermark. This method has no need for artificial selection of ROI, no capacity restriction, nor participation of original medical images in the watermark extraction process. It can successfully address both compression attacks and conventional attacks in the medical image application, thus further protecting the privacy of patient information. In a word, this method is easier and more practical.
After studying of plenty of the full graphic DWT data, we found that when we perform common compression transformation on a medical image, the value of the low frequency coefficient may be changed to certain degree but the sign of the coefficient remains basically unchanged.

Baoru Han et al. [15] proposed zero-watermarking algorithm for given medical applications to ensure robustness, security and invisibility. This technique is based on the three-dimensional discrete wavelet transform, the three-dimensional Fourier transform and the Hermite chaotic neural network. The new Hermite chaotic neural network is used to generate the pseudo-random chaotic sequence for scrambling. The three-dimensional medical image is transformed by the three-dimensional discrete wavelet transform and the three-dimensional discrete Fourier transform. Then, the low and intermediate frequency coefficients are se-selected as characteristics of medical data to create a zero-tattoo. This algorithm has good resistance to geometric attacks such as Gaussian noise, JPEG compression, shear tack and zoom attack

A novel zero-watermarking algorithm for medical Images based on dual-tree complex wavelet transform (DTCWT) is proposed in [16]. Unlike traditional watermarking schemes, the main idea of the zero-watermarking embedding in medical imaging is that the watermark is not inserted directly in the image itself, the watermarking process does not affect any modification to the image, Hidden features are extracted from the original image and combined with the watermark,

and then encrypted, and a key is produced, the extraction of internal representative feature information from the image data is the critical phase in the zero-watermarking approach. In this novel proposed algorithm, the DTCWT transform is used on medical images. Then, a visual feature vector of medical images against geometric attack is extracted from the low-frequency coefficients of DTCWT. Finally, combining with the concept of zero-watermarking, the watermark is encrypted by the logistic map. On this basis, the ordinary watermarking technology is combined with chaotic encryption. The secret key must then be kept for future watermark extraction.

In [17], the authors also proposed a dual approach of watermarking followed by encryption to prove the authenticity and integrity of medical images. The two-level DWT transformation is applied to the original data. The mark is inserted into the low-high sub-band based on the LSB technique where the low-high sub-band is again divided into several blocks, then the medical information (as the second mark) is inserted into these blocks using the LSB technique. Finally, the watermarked image is encrypted using RSA, Advanced Encryption Standard (AES), and Ron's Code (RC4) algorithms.

4. BASIC CONCEPTS

This part is a basic theory for the selected tools: Hessenberg Decomposition (HD), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and an original crypto system based on the Arnold's cat map (AT).

4.1. hessenberg decomposition

Hessenberg decomposition [18], is the factorization of a general matrix A by orthogonal similarity transformations into the form

$$A = QHQ^T . \quad (1)$$

Where Q is an orthogonal matrix and H is an upper Hessenberg matrix, meaning that $h_{ij} = 0$ whenever $i > j + 1$. Hessenberg decomposition is typically computed by Householder matrices.

4.2. Discrete Wavelet Transform (DWT)

DWT has excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system [19]. DWT decomposes the original image into four sub-band images: three high frequency parts (HL, LH, and HH, referred to as detail sub images) and one low frequency component (LL, named approximate sub-image). The fringe information is contained in the detail sub-bands, whereas the approximation sub-bands are the convergence of the original image's strength. The approximate sub-image is substantially more stable than the detail sub-images since the majority of image energy accumulates here. Images are obviously two dimensional data. To transform images we can use two dimensional wavelets or apply the one dimensional transform to the rows and columns of the image successively as separable two dimensional transform.

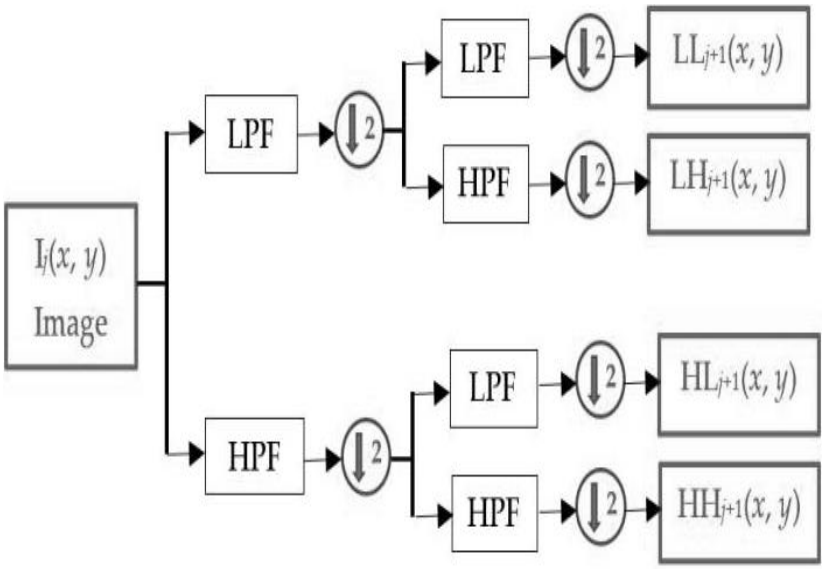

Fig 2. 2DWT of 'I' from level j to j + 1 produce sub-bands LLj+1, LHj+1, HLj+1, and HHj+1

4.3. Singular Value Decomposition

SVD is an effective numerical analysis tool used to analyze matrices [19]. In SVD transformation, a matrix can be decomposed into three matrices of the same size as the original matrix. From the view point of linear algebra, an image is an array of non-negative scalar entries that can be considered as a matrix. Also, singular value decomposition is defined for all matrices (rectangular or square). Let I be an image, with a size of M×N. The SVD of I defined as:

$$I=USV^{T}. \quad (2)$$

Where $(.)^{T}$: the elements of S are nonnegative values on diagonal representing singular values of I. the diagonal elements of matrix S = diag (s1, s2... sn) satisfy the order:

$$s1 \geq s2 \geq .... \geq sn. \quad (3)$$

It's crucial to keep in mind that, the nonnegative components of S represent the luminance value of the image. Modifying them slightly does not affect the image quality and they also don't change much after attacks;

The first columns of V are the right singular vectors, and the first columns of U are the left singular vectors. The SVD technique can be applied in digital image cipher and watermarking. The image can be split into three segments then secure them in a variety of ways so that only at the time all the three image segments come together and are multiplied with the right order the information could be retrieved.

4.4. Scrambling Transform Technology

There are two ways of digital image encryption which change the value of the pixel and the other one changes the position of the pixel (scrambling). The first focuses on altering the pixel value, rendering the original image illegible without knowledge of the encryption method used, such as Lorenz, Rössler, Chue and Nien. The other, such as Arnold transform Cat Map, focuses on

changing pixel positions for the purpose encryption. In order to expand the robustness of the algorithm and provide extra security to the embedded watermark, Arnold-SVD scrambling is employed in the pre-processing step of the proposed watermarking method.

The Arnold Transform (AT) is defined as the Cat's mapping. It aims to shift the pixel positions instead of changing their estimates. Recently, it was employed for image ciphering and watermarking [20]. The AT of a pixel (a,b) of an image f (a,b) of size NxN pixels is defined by f (a',b') and can be expressed mathematically by the standard Arnold cat map:

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = AT\left((a,b),N\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (\mathrm{mod}\, N). \quad (4)$$

Where (a, b) and, (a', b') represent the initial and the position of the shifted image pixel, respectively,„"Mod" defines the modular arithmetic operation. The parameter N is the target image size, which is used to determine the period of AT.

5. PROPOSED SCHEME

5.1. Modelling of Electronic Health Records system

An Electronic Health Record (EHR) is an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports The HER automates access to information and has the potential to streamline the clinician's workflow. The EHR also has the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting.[21]

The developed EHR System allows a doctor/user to securely receive a medical image through a trusted authority server. The doctor does not communicate directly with a medical image generator. Here, the server plays a mediator role in the EHR system. When a patient presents with undifferentiated symptoms, each stakeholder group performs different functions to support the care of the patient.

For Doctors: A doctor is an eligible user with an embedded data in his or her own device such as a computer or mobile. Each patient record contains the patient's medical images, and some information about their watermarked images.

Other roles of Doctor are:

- Registration in the system;
- Creating a record of the patient;
- Edit records: adding and modifying medical reports, e- prescriptions, required analyses, and certificates;
- Showing analyses results that were created by the laboratory;
- Show reports that added by other doctors (secondary): This means that another doctor can amend the record by adding a diagnosis or pictures. In general, this last one is a specialist.
- Watermarking.

The patient Provide and clarify information (including symptoms); negotiate a diagnostic, treatment

- Show all record created or modified
- Search for patient profiles.
- Search for patient records.
- The system should allow patients to create new accounts.
- Edit account information.
- Show his records.

Data requirements:

- Patient contact information.
- Emergency patient information.
- Medical records of patients.
- Medical records permissions for patients.
- Records of access to medical records of patients.

A model of a software system is made in a unified modelling language (UML). The model has both semantics and notation and can take various forms that include both pictures and text. The model is intended to be easier to use for certain purposes than the final system. The main difference between a method and a modeling language is that the modeling language lacks a process or instructions for what to do, how to do it, when to do it, and why it is done. [22]

5.1.1. Use case diagrams

A use-case diagram captures the activities performed by the system and the key players to the use cases that the system provides; these correspond to the functional requirements [22]. The use case is intended to include the following events: determining the target population criteria, querying the patient population, and interacting with patients. Each major event has specific data display requirements to support overall patient care. The use case does not include decision of a diagnosis, developing an initial treatment plan, or completing the visit because these activities are covered in the acute care use case. For treatment of chronic conditions, each stakeholder group performs different functions to support the care of the patient. Those roles include: Medical staff, patient.

Preconditions to this use case include, but are not limited to: the patient's condition being previously diagnosed and a treatment plan is in place. The tables below are designed to provide an illustration of the most common use cases function of doctor and Medical staff.

Table 1. Use case specification (1).

Uses case Name	Search for patient
Actors	Medical Staff
Description	Display medical information for the patient Add medical information to the patient Upload medical records to the patient
Précondition	A Medical staff should have an account The patient must have an account
Post-condition	The system displays existing record/create others (just

	For doctors).
Basic flow	The doctor only needs the patient's username to search. The patient should only give the username The system displays the required result for the selected Record type.

Table 2 illustrates the use case specification structure that stores patient records. Each patient's record contains the patient's medical images and some information about their watermarked images.

Table 2. Use case specification (2).

Uses case Name	Create record
Actors	Doctor
Description	Create record for patient Watermarking EPR
Précondition	A doctor should have an account Patient has created an account for use and updated his or her emergency contact information via the Update Emergency Info on Server
Post-condition	Doctor logs in with user name, password, ID. The system Verifies the username and password and access permissions and Display patient search window Doctor enters patient's ID in search screen A system Searches for patients by ID number and displays list of possible matches
Basic flow	The doctor create new record, watermark The system redirect the doctor to the record page
Other non-functional requirements	The confirmation page for the updated record will be shown to the patient Immediately after the "Save" button is clicked. The record listing should transmit to all concerned servers (update).

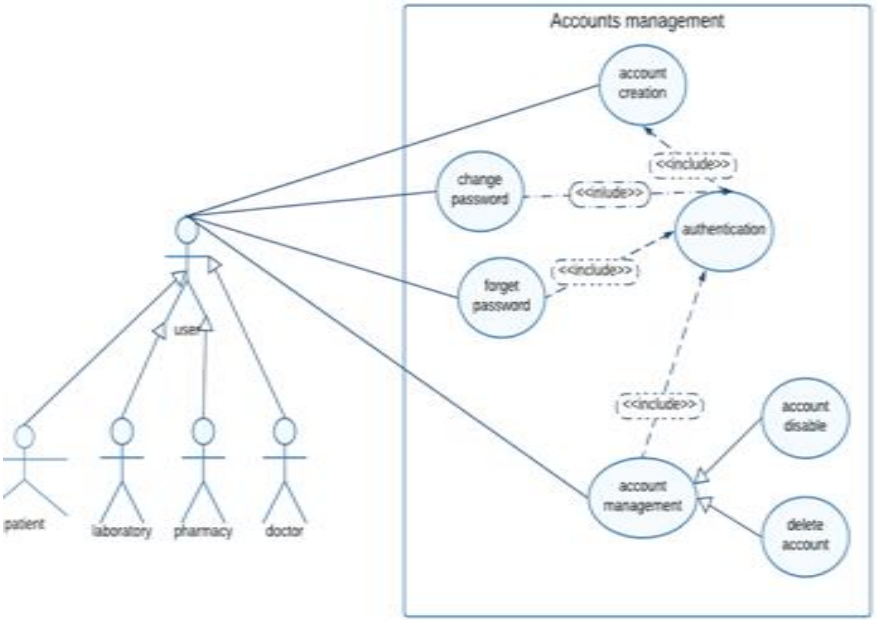

Fig 3. Use Case diagram for accounts management

5.1.2. Sequence diagrams

A sequence diagram shows a dynamic collaboration between a numbers of objects. The important aspect of this diagram is that it shows a sequence of messages sent between the players. It also shows an interaction between objects—something that happens at one specific point in the execution of the system. The diagram consists of a number of objects shown with vertical lifelines. Time passes downward in the diagram, and the diagram shows the exchange of messages between the objects over time. Messages are shown as arrows between the vertical lifelines. [22]

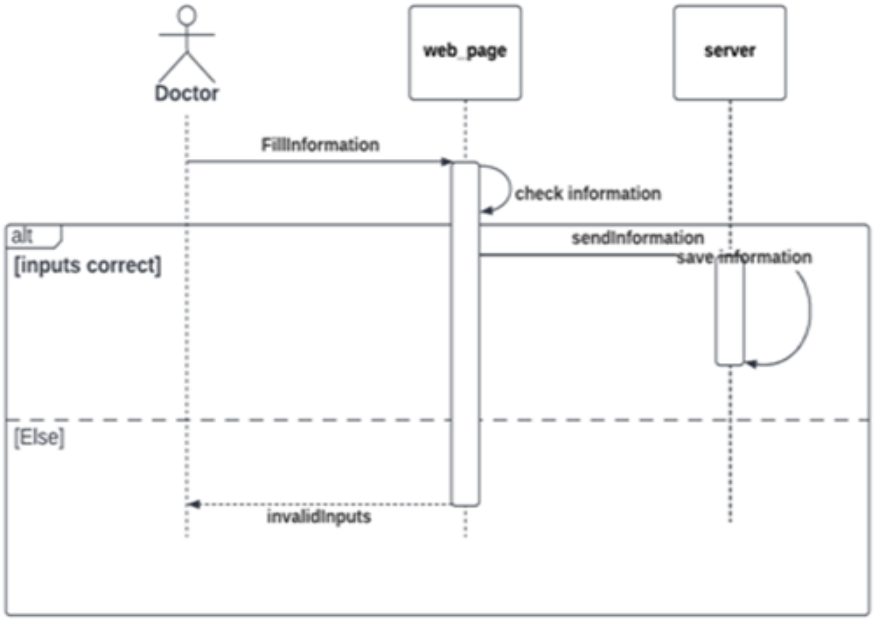

Fig 4. Sequence diagram (fill in the information)

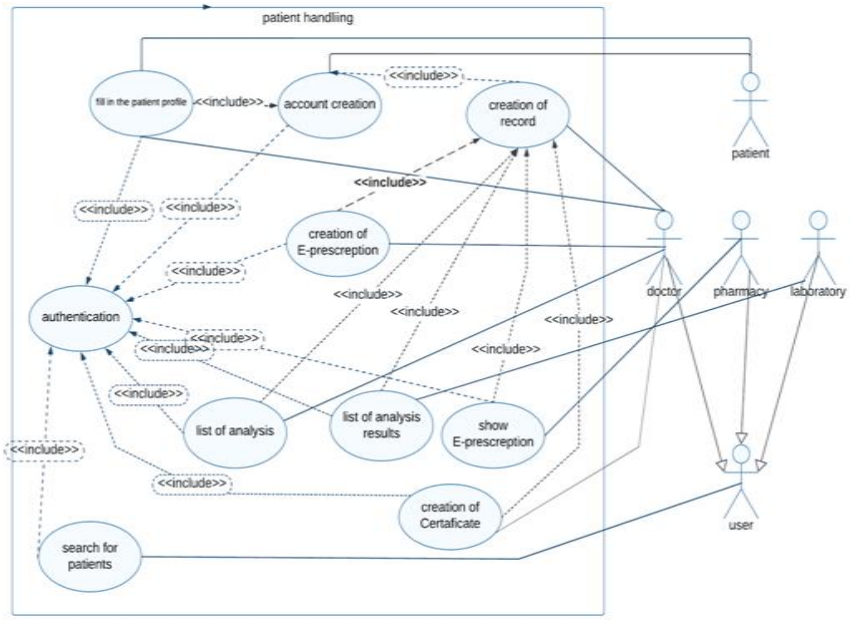

Fig 5. Use Case Modeling in Designing EHR Systems

The use case modeling method is useful for focusing on the start and analysis, better planning, repetition, and control of the issues with health and medical imaging information systems. We explained some functional and non-functional requirements of the EHR system.

5.2. Watermarking Method

In this part, we present a watermarking scheme that includes two main processes: watermark embedding and watermark extraction. Using watermarking techniques with the proposed AT-SVD and integrating the electronic patient report (EPR) into the medical images will not only guarantee the confidentiality and security of the sent data but also the integrity of medical images.

5.2.1. Insertion Algorithm

The watermarked image is transmitted to the receiver over EHR system. At the receiving end, watermark extraction and recovery is carried out. In the process of watermarking embedding, R level discrete wavelet transform was applied to the host image and a low-frequency sub-band was then obtained. The sub-band was further processed by HD and sub-band H was further processed by SVD. Plus the singular value of the sub-band and the scrambled watermark, and a new singular value was acquired. In the addition operation, a scaling factor was chosen to control the embedding strength of watermark, and an appropriate strength could be traded off between imperceptibility and robustness. This new value was decomposed once again to get a new singular value which was used to reconstruct a low-frequency sub-band. Finally, the watermarked image was formed by making use of the new sub-band after the process of inverse HD (of the new sub-band LL) at the end; an inverse discrete wavelet transform was applied to generate a Watermarked image. The details of watermark embedding are depicted in Figure 6.

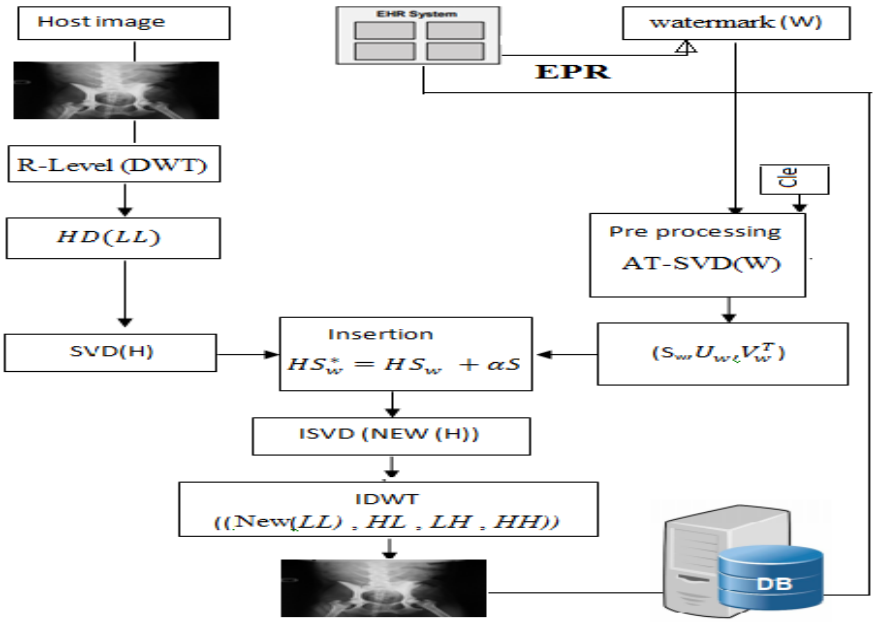

Fig 6. Extraction process

5.2.2. Extracting Algorithm

The extraction process doesn't require the original image. It is assumed that values of □, a and b, Uw1 and Vw1T for the AT transform are known for the extraction procedure, α being named often as the visibility factor. Indeed, α is an important factor in the watermarking system. If this factor is big, we win in terms of the robustness; however, we lose in terms of imperceptibility and vice versa. To construct the watermark, the DWT was applied to the watermarked image, and the low frequency approximate coefficient of which was further decomposed. We apply the HD method on LL, followed right away by SVD. The scrambled watermark was obtained under the utilization of the original host image and the newly formed singular value Snew. In order to construct the watermark, the following steps are performed:

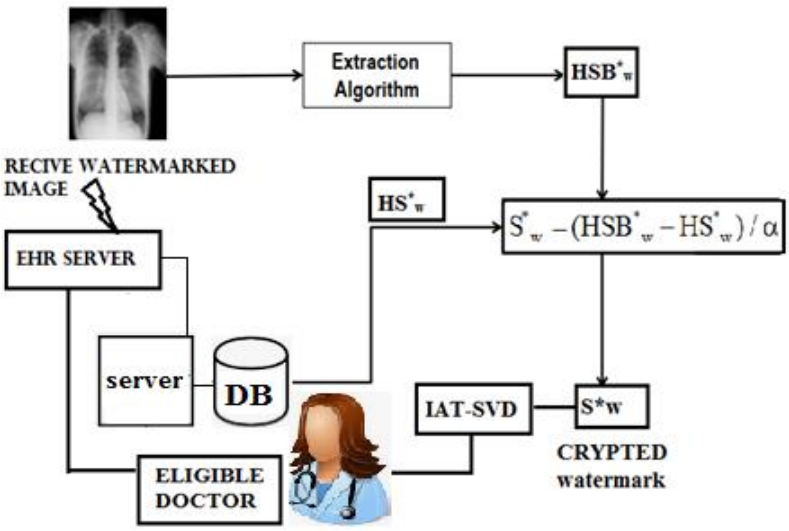

Fig 7. Extraction process

Step 1. The original watermarked image C* was decomposed by R level DWT into four sub-bands LL_w, LH_w, HL_w, HH_w.

Step 2. HD was performed on LL_w by the formula of:

$$P_w H_w P_w{}^T = HD(LL_w).(5)$$

Step 3. SVD was performed on H_w :

$$HU^*_w \cdot HSB^*_w \cdot HV^*_w{}^T = SVD(H_w).(6)$$

Step 4. We obtained the scrambled watermark image by the formula of:

$$S^*_w = (HSB^*_w - HS^*_w) / \alpha.(7)$$

In this process, the stored used plain image HS^*_w is obtained from the server to full the verification process. The receiver must compare the secret HS^*_w with the extracted HSB^*_w for a second time. The verification can be ready before clinical procedures and diagnosis.

Step 5. To obtain a watermark, decrypted Process of Proposed AT-SVD method was applied. The decryption process aims to derive the plain image watermark from the cipher image.

6. SIMULATION RESULTS

The PSNR (Peak Signal to Noise Ratio) is generally used to estimate the quality of the original image and watermarked. A higher PSNR value indicates that both images are more similar to each other. This metric is determined in decibels (dB)[18]. The PSNR is defined by:

$$PSNR=10\log_{10} XY \max_{x,y} p^2_{x,y} / \sum_{x,y} (p_{x,y} - \tilde{p}_{x,y})^2.(8)$$

The Normalized Cross-Correlation (NC) is defined as

$$NC=\sum_{x,y} p_{x,y} \tilde{p}_{x,y} / \sum_{x,y} p^2_{x,y}.(9)$$

Where, $p_{x,y}$ is the matrix of the original watermark and $\tilde{p}_{x,y}$ is the matrix of the extracted watermark.

To see the effectiveness of the suggested system, the experiment was carried out in MATLAB. Several tests are carried out on three standard grayscale benchmark images of types of medical images (MRI, radiography, ultrasound) from the kaggle database, these are coded on 256 levels of gray, in BMP format of size 256x256, and the watermark logo of size 64 × 64 was considered. The experiments are done in three steps, the first step is to apply our approach to a set of original images without attacks and to check if the key is well reconstructed on the receiver side. The second step consists in applying the approach on the same set of images while considering the attacks on the images during their transfer to the receiver

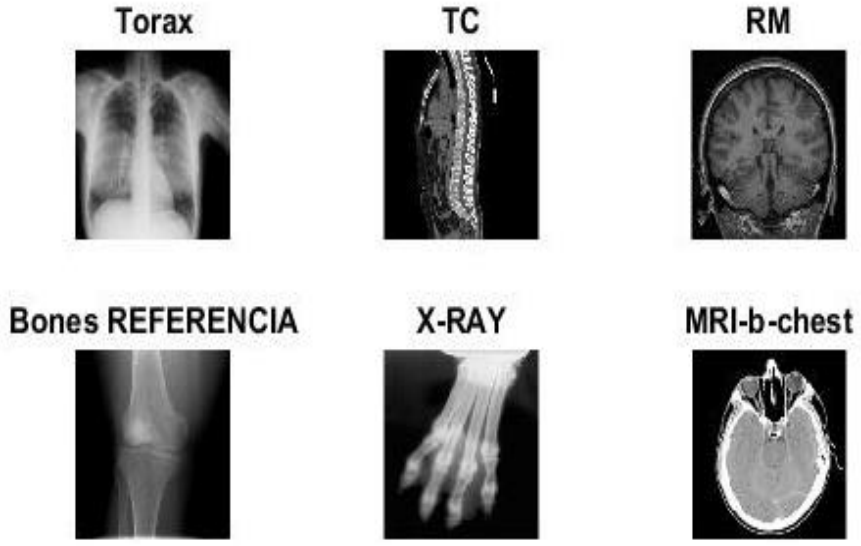

Fig 8. Types of medical images

Fig 9. Binary watermark image

6.1. Invisibility Analysis

Figure 10 shows the embedding and extracting procedures which result in test by images using proposed method. No degradation is noticeable on the watermarked medical image

Fig 10. Original and watermarked image

Figure 11 shows the embedding and extracting procedures which result in test by images using proposed method. No degradation is noticeable on the watermarked medical image α=0, 1, without attack.

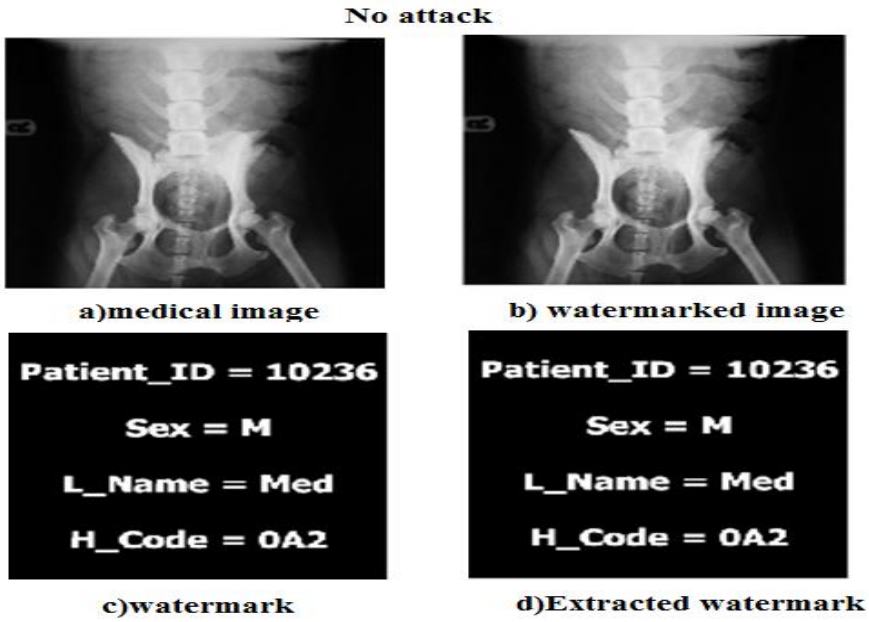

Fig 11. Invisibility tests

6.2. Robustness Analysis

The watermark should be robust against attacks (the distortions due to attacks should remain minimal). In our experiments, we consider some geometric and non-geometric attacks. These attacks consist of median filtering, salt-and-pepper, average filter, cropping, contrast

enhancement, scaling, Gaussian filtering, low pass filtering, histogram equalization, noise, rotation, sharpening, and translate attacks.

Detailed results of NC are summarized in Figure 12. This graph displays the comparison results with a scale factor $\alpha = 0.05$, the NC values are in the range [0 1]

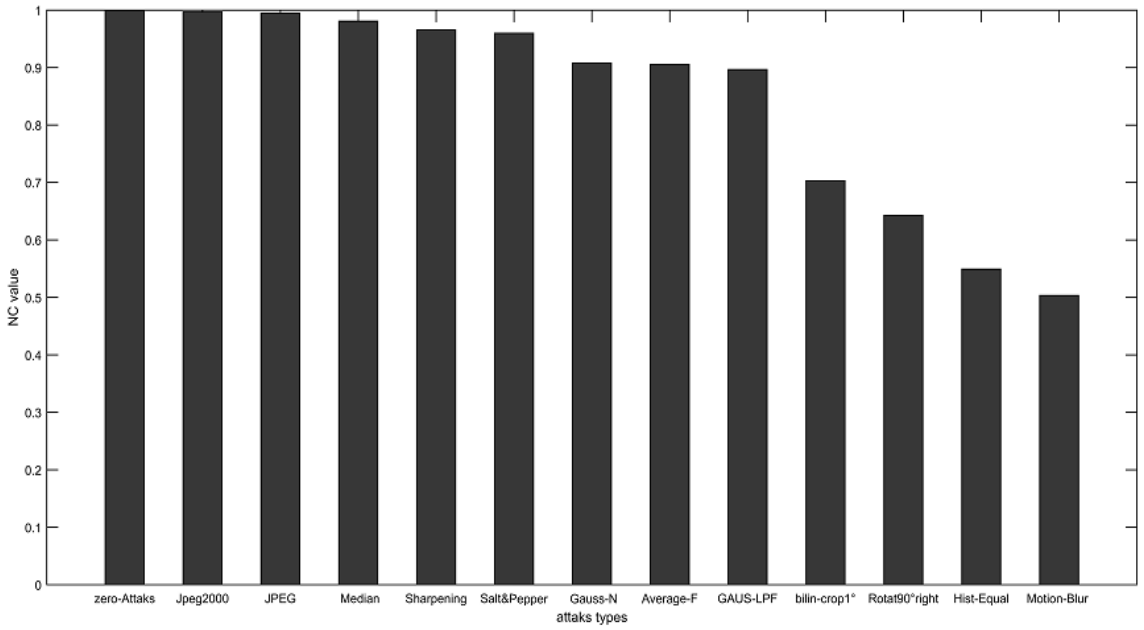

Fig. 12. Robustness NC values against attacks

In our case the NC = 0.99901 without attack. With the exception of the histogram equalization the NC = 0.54937, we can see that not only the visual quality of the extracted watermark is acceptable, but that the NCs are also relatively high. The NC of the proposed method for various attacks varies from 0.95981 to 1, Compression attacks in the field of watermarking of digital images affect and significantly alter watermarked images and generally the detection of the mark after compression becomes very sensitive, because the compression algorithms only keep from the watermarked image the essential components of the watermark. It is often said that a good watermarking pattern resists compression well, which is presented by very acceptable values: NC = 0.97965 for Jpeg and NC = 0.99462 for Jpeg2000.

6.3. Imperceptibility Analysis

Watermark's imperceptibility is evaluated by calculating PSNR between original and watermarked images. To quantitatively evaluate the performance of the proposed scheme, the peak signal-to-noise ratio (PSNR) was adopted to measure the image quality of a watermarked image. There is a trade-off between invisibility and robustness in image watermarking. To maintain a good balance between these qualities, a suitable gain index (α) value should be selected for embedding. The results of PSNR values (between host and watermarked images), and values adaptive strength factors alpha are shown in Figure 13.

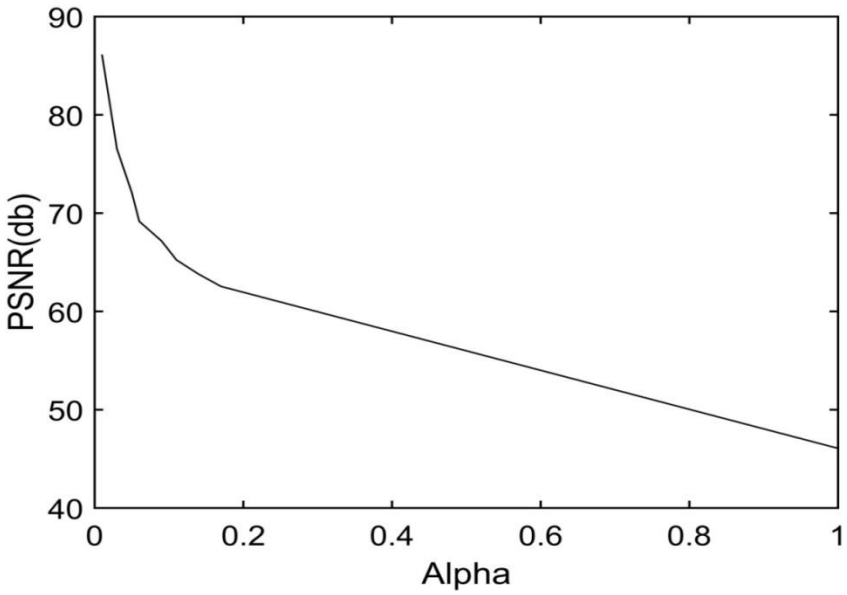

Fig. 13. Peak signal to noise ratio as a function of for different values of α

The proposed watermarking scheme achieves the lowest distortion in the watermarked images. All the PSNR values in [0, 1] exceed 45 (high PSNR quality). Higher PSNR values indicate higher imperceptibility and less distortion. For the watermarking, a PSNR value greater than 40 dB is an indicator of good quality image reconstruction [25]. The PSNR values are comparatively lower for higher gain index values.

Our extraction scheme is very difficult to break; therefore, the security of the proposed embedding and extraction algorithms is greatly improved. Furthermore, the watermark can be extracted without the original image; this allows for blind extraction, which broadens the range of watermarking applications and improves security. Therefore, compared with the traditional embedding techniques of watermarks, the proposed scheme not only realises the complete imperceptibility of the watermark but also causes minor damage to the watermarked image. Thus, the problem of image degradation does not exist, so it maintains the integrity of the original image and the imperceptibility of the watermarked image. So that even if the attacker extracts the watermark, the original watermark image cannot be obtained if the encryption method or encryption key is not known. However, the proposed method does not maintain the quality of watermarked images against attacks such as histogram equalisation and motion blur attacks.

7. CONCLUSIONS

The proposed watermarking technique finds its potential application in the field of medical health care where a patient record bearing vital information can be transmitted as watermark beside with medical image. The proposed system has two main phases: Utilizing use case modeling approach for modeling the problems of health and Electronic Health Record systems towards understanding, focusing on the start, analysis, and control. Second we talked in detail about a proposed watermarking scheme for secure transmission of medical image and patient record information. Our watermarking system consists of a hybrid combination of the three methods, HD, SVD, and DWT. DWT is further applied to the reflectance component resulting in frequency sub bands (LL) of host image which are transformed by HD and SVD. Two image watermarks are selected for embedding process whereas security of proposed algorithm is strengthen by

performing scrambling of watermark through AT-SVD, and additional parameters (a, b, alpha), these parameters are used as secret keys to extract watermark in the process of watermark extraction, which can be obtained from the embedding process, without the correct initial condition, the watermark cannot be successfully detected. The method endures several attacks and rightly extracts the concealed watermark without major degradation in the image quality of the watermarked image, thus when the Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) performance of the proposed algorithm. The experimental results show that after all attacks the extracted watermarks are visually recognizable and all extracted watermarks are similar to the original watermark, the average NC value is greater than 0.9 which is a good ratio and the PSNR on average is equal to 53.45 dB. Future work will focus on the current artificial intelligence methods for the extraction of robust features from the original image in order to generate a strong brand. This study will allow us to assess the potential benefits of artificial intelligence approaches for an overall improvement of watermarking systems.

REFERENCES

[1] Joint NEMA/COCIR/JIRA Security and Privacy Committee,2003. "Defending Medical Information Systems Against Malicious Software," National Electrical Manufacturers Association-USA.

[2] Umamageswari A., Ferni U., Suresh G.R. ,2011."A Survey on Security in Medical Image Communication, «International Journal of Computer Applications, Vol. 30, no.3.

[3] Ravi Shah, Abhinav Agarwal and Subramaniam Ganesan, "Frequency Domain Real Time Digital Image Watermarking", Oakland university, MI-48309, 1998.

[4] Husrev T. Sencar, Ali N. Akansu, in Data Hiding Fundamentals and Applications, 2004.

[5] Frank Y. Shih, Scott Y. Y. Wu, "Combinational Image watermarking in the Spatial and Frequency domain", Pattern Recognition, volume 36, Number 4, April 2003, pages 969-975.

[6] Jiwu Huang, Yun Q. Shi, Yi Shi, "Embedding image watermarks in DC components", IEEE Trans. CSVT 10 (6) (2000) 974–979.

[7] William Puech et Jose M Rodrigues, A new crypto-watermarking method for medical images safe transfer, 2004 12th European Signal Processing Conference,2004, p. 1481-1484.

[8] B. Macq, F. Dewey, Trusted Headers for Medical Images in Proceedings of the DFG VIII-DII Watermarking Workshop, Erlangen, Germany, Oct. 1999.

[9] A.K. Ray, S. Padhihary, P.K. Patra and M.N. Mohanty, Development of a new algorithm based on SVD for image watermarking, in: Computational Vision and Robotics Springer, New Delhi, pp. 79-87, 2015.

[10] Rajendra Acharya et al., « Simultaneous storage of patient information with medical images in the frequency domain », in : Computer methods and programs in biomedicine 76.1 (2004), p. 13-19.

[11] S.Kaur and R. Talwar, Arnold transform based Security Enhancement using Digital Image Watermarking with Complex Wavelet Transform, International Journal of Electronics Engineering Research.9 (2017), pp. 677-693.

[12] C. Kumar, A. K. Singh, P. Kumar, R. Singh and S. Singh, SPIHT-basedmultiple image watermarking in NSCTdomain, Concurrency and Computation: Practice and Experience. (2018), e4912.

[13] Abderrahmane Daham and Mohamed ouslim ,Encryption Based Watermarking Technique For Security Of Medical Image , International Journal of Computer Science & Information Technology (IJCSIT), February 2022, Volume 14, Number 1.

[14] S. M. Haque, (2008),"Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking", Master's Thesis, Computer Science, Blekinge Institute of Technology, Sweden.

[15] Rupinder K., 2013. "A Medical Image Watermarking Technique for Embedding EPR and Its Quality Assessment Using No-Reference Metrics," I.J. Information Technology and Computer Science, vol. 2, pp. 73-79.

[16] Chauhan, D.S.; Singh, A.K.; Kumar, B.; Saini, J.P. Quantization based multiple medical information watermarking for secure e-health. Multimed. Tools Appl. 2019, 78, 3911–3923

[17] Zain JM, Clarke M. Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. Int J Comput Sci Netw Secur. 2007;7(9):19–28.

[18] Dagadu, J.C.; Li, J. Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimed. Tools Appl. 2018, 77, 24289–24312.

[19] A. Daham, M. Ouslim, Y. Hafed and W. Djaber, "Robust Watermarking Method to Secure Medical Images Applied to Ehealth," 2022 13th International Conference on Information and Communication Systems (ICICS), 2022, pp. 379-385, doi: 10.1109/ICICS55353.2022.9811160.

[20] Ashraf Afifi Efficient Arnold and Singular Value Decomposition based Chaotic Image Encryption International Journal of Advanced Computer Science and Applications, Vol. 10, No. 3, 2019.

[21] Thakur, S.; Singh, A.K.; Ghrera, S.P.; Elhoseny, M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed. Tools Appl. 2019, 78, 3457–3470.

[22] S.A. Parah et al. Parah, S.A.; Sheikh, J.A.; Ahad, F.; Loan, N.A.; Bhat, G.M. Information hiding in medical images: A robust medical image watermarking system for E-healthcare. Multimed. Tools Appl. 2017, 76, 10599–10633.

[23] M. Kutter and F.A. Petitcolas, Fair evaluation methods for image watermarking systems, Journal of Electronic Imaging. 9 (2000), 445-456.

[24] Mayssa Tayachi et al. Tamper and Clone-Resistant Authentication Scheme for Medical Image Systems, 2020.

[25] Huang, H.-C.; Chu, S.-C.; Pan, J.-S.; Huang, C.-Y.; Liao, B.-Y. Tabu Search Based Multi-Watermarks Embedding Algorithm with Multiple Description Coding. Inf. Sci. 2011, 181, 3379–3396.