ENCRYPTION BASED WATERMARKING TECHNIQUE FOR SECURITY OF MEDICAL IMAGE

[1]B.Yugandhara Chary ,Assistant Professor, CSE(AIML), yugandhar.bandla@gmail,com
Swarna Bharathi institute of science and technology,
Khammam
[2]Dr.K.Spurthi, Associate Professor , CSE(AIML), Kolluspoorthy03@gmail.com
Swarna Bharathi institute of science and technology,
Khammam,
[3]P.Anusha, Assistant Professor, CSE, peddapakanusha@gmail.com
Swarna Bharathi institute of science and technology,
Khammam,

Abstract

An encryption-driven image watermarking method for medical images is executed by employing customized quantization of wavelet coefficients integrated with an individual Value Decomposition-based Confused encryption system. The technique enhances security through a refined Singular Value Decomposition-CHAOS embedding extraction Improve that scrambles the watermark in advance. During embedding, a multi-level Discrete Wavelet Transform is applied, and high-frequency bands are selected for watermark insertion using adaptive Lattice Boltzmann Model quantization. Experimental evaluations demonstrate greater robustness and high peak Quality *Ratio values* Relative to existing techniques.

KEYWORDS
Watermarking, medical image, discrete wavelet transform, singular value decomposition,

ABSTRACT
Postnatal stress is a significant psychological concern that affects the physical and emotional well-being of mothers and their infants. Understanding its prevalence and associated factors is essential for planning effective interventions to promote maternal mental health. **Objectives:** To assess the level of stress among postnatal mothers using the Perceived Stress Scale (PSS) and to describe the relationship between demographic and obstetrical variables with stress levels .**Methods:** A quantitative research approach with a descriptive research design was adopted for the study. The research was conducted at Coimbatore Medical College Hospital, Coimbatore. The study population comprised postnatal mothers who had delivered either vaginally or by lower segment caesarean section (LSCS). A non-probability purposive sampling technique was used to select 30 postnatal mothers based on inclusion and exclusion criteria. Data were collected using a structured questionnaire on demographic and obstetrical variables and the standardized Perceived Stress Scale (PSS). **Results:** Among the 30 postnatal mothers, the majority (70%) were aged between 21–25 years, 70% were Hindus, 44% had completed secondary education, and 60% were unemployed. Regarding obstetrical variables, 77% were multigravida, 67% had normal vaginal delivery, and 83% reported their child as healthy. The assessment of stress revealed that 67% of the postnatal mothers experienced moderate stress, while 33% experienced high stress. No participants reported low stress levels .**Conclusion:** The findings of the study indicate that all postnatal mothers experienced some level of stress, highlighting the need for continuous psychological assessment and supportive interventions during the postnatal period. The Perceived Stress Scale was found to be an effective tool for assessing stress among postnatal mothers..

Keywords:
Postnatal mothers, perceived stress scale, postnatal stress, descriptive study, psychological well-being, maternal health

quantization,
chaos cryptosystem.

INTRODUCTION

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. A medical I'm age is a requirement for sharing in which the confidential data of the patient should be protected f rom unauthorized access, sharing them over the internet has become very popular nowadays for telediagnosis, telesurgery, and teleconsultation [1]. Most hospitals and healthcare systems involve a large amount of data storage and transmission, such as medical images, patient information and administrative documents. Among this data, the patient information and medical images need to be protected against any malicious attempts. To prevent a patient's information from any attack, three things are required, i.e., integrity, privacy, and authenticity of medical images [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. This problem can be well solved through medical image digital watermarking [3–4], namely, embedding the personal information into medical images as a digital watermark. 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 [4-5].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]. The geometric attack is so far a major problem to be solved in the research field of digital watermarking for medical images. There is still no study about fighting against conventional and geometric attacks effectively. While in actual application, the medical digital watermark image often suffers from both kinds of attacks simultaneously. In addition, the study of medical images needs to tackle the problem of disclosing and changing patients' information or privacy in the process of watermark extraction. In light of the above problem, we may conduct some pretreatment, namely encryption, as secondary protection to enhance the security of the watermark information protection [7-8].Image watermarking can be applied to protect the copyright of medical images. Patient's information can be protected from illegal access by watermarking techniques. These applications include medical imaging, telehealth, and telemedicine, among others. Medical imaging visualizes tissues, organs, or some other parts of the body, by using information and communications technologies. In addition to the basic requirements of a typical watermarking system, as previously explained, some other specific features are needed for the medical watermarking system. These are explained below [9]. Image is called imperceptibility and can be measured by statistical standard metrics such as SSIM (Structural Similarity Index)[18], SSIM measures the perceptual difference between two similar images and gives a quality reference by comparing the original and modified images or :

Imperceptibility: The amount of invisibility of a watermarked image in comparison to none watermarked PSNR (peak signal-to-noise ratio). Reversibility: Due to the image quality, the applied method for medical watermarking should be reversible, meaning that one should be able to exactly recover the original image after extracting the watermark Integrity Control: The ability to verify that the image has not been modified without authorization. Authentication: Identification of the image source and verification that the image belongs to the correct patient.

This paper presents a robust crypto-watermarking algorithm for medical images based on a DWT (discrete wavelets transform) and a Chaos cryptosystem-SVD (Singular value decomposition). The remainder of this paper is organized as follows: Section 2 gives an overview of digital Image watermarking. Section 3 provides the related research that includes a brief summary of recent methods. In Section 4 elaborates basic concepts of (DWT, SVD, and LBM quantization) and PROPOSED SHAOS-SVD CRYPTOSYSTEM. In section4 the methods of watermark embedding and extraction procedures are proposed in detail. The experimental results and

performance comparisons are given in Section 6. Finally, Section 7 gives the conclusions.

AN OVERVIEW OF DIGITAL WATERMARKING

Refers to the process of embedding a message into digital media, The watermarking embedder creates the watermarked image by combining cover data along with the watermark image. The purpose is the authenticity or copyright of this digital media. The structure of a digital watermarking compose from two primary components: the first stage is the watermark embedding, and the second is the watermark detection and extraction. To combine a watermark with a digital document, for example, images, you need an image (I), a watermark (W) that contains the secret information, a security key (K), and an embedding algorithm to create a watermarked image (IW). The embedding algorithm takes the signature and the cover image(I) and generates the watermarked image (IW), 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. The watermark is considered to be robust if it is embedded in such a way that the watermark can survive even if the watermarked image (IW*) go through severe distortions. The watermark must be very difficult to remove, or destruct from the media by the attacks. A watermark extractor or detector involves a two-step process. Watermark retrieval is the first step that applies some scrambling algorithms to extract a sequence referred to as retrieved watermarks. Then, in the second step, the embedded watermarks are detected and extracted from a suspected signal of containing watermarks. The second step normally requires the analysis and comparison of the unreliable watermark with the original one, and the consequences could be several kinds of confidence assessment displaying the similarity between the extracted watermark and the original one. The extraction loads the watermarked, normal or corrupted image (LW*) and extracts the hidden Watermark (W).

2.1. Digital Watermarking Requirements

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. 77 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022

- 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. Importance of Digital Watermarking

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. 78 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 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. 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 [1].

2.3. Classification of Digital Watermark

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 of the images. In our work, we are interested in invisible watermarks, taking into account the privacy of patient information; we have to embedding the personal information into medical images as a digital watermark.

2.3.1. Visible Watermarks

The 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 degrading the quality of 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 interface.

2.3.2. Invisible Watermark

Invisible watermark is hidden in the content and designed to be beyond normal human's observation. Normal human's vision cannot distinguish between the original and the protected information. Diverse watermarks are used for content and /or author authentication and for detecting unauthorized copier. 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.

2.4. Applications of Digital Watermarking Digital

Watermarks are potentially useful in many applications, including: 79 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022

2.4.1. Digital Watermarking Technology for Rights Management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. the content owners to the

receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment. The major technical requirements for this application are as follows:

- The watermark does not incur visible (or audible) artifacts to the ordinary users.
- The watermark is independent of the data format.
- The information carried by the watermark is robust to content manipulations, compression, and so on.
- The watermark can be detected without the un watermarked original content.
- The watermark can be identified by some kind of "keys" that are used to identify large number of individual contents uniquely.

2.4.2. Digital Watermarking

Technology for Authentication and Tamper Proofing Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/ Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a "sensor" to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications. The technical requirements for this application are as follows: 80 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 • Invisible to the ordinary users. • Applicable to compressed image format (most digital cameras use JPEG compatible format). • Sensitive to content manipulations, compression, and so on.

2.4.3. Visible Reversible Watermarking for Electronic Distribution

The visible reversible watermark, unlike the other digital watermarking systems listed above, is visible. It is available as a commercial product. This unique form of watermarking technology by IBM allows the content owners to embed a visible shape or logo mark such as company's logo on top of the image. The mark is removed (the watermark is reversed) only with the application of an appropriate "decryption" key and watermark remover software. This mark is inserted by modifying the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image according to a pre-defined rule and visual effect analysis result to make it half transparent, but not completely damaging. The key will be used in conjunction with the mark removal program to remove the mark from the image. The removal of a visible mark could be linked to the insertion of a second invisible mark for tracking purposes. Through this visible watermark on the image, the content becomes self-protective, and content owners can distribute the entire image as a sample to various open media or to the Internet. When a user wants to use a clean copy of the image, all he/she needs to be is to request a "decryption" key and you'll have to pay a price for it. This will reduce the security risk and the amount of the data transmission per each buy/sell transaction [5].

2.4.4. Watermarking as Communication System

Watermarking system can be viewed as some form of communication. The payload message P, encoded as a watermark W, is modulated and transmitted across a communication channel to the watermark detector. In this model, the cover work represents a communication channel and therefore it can be viewed as one source of noise. The other source of noise is a distortion generated by normal signal processing and attacks. Modeling watermarking as communication is

important because it makes it possible to apply various communication system techniques, such as coding, spread spectrum communication, modulation, error correction, matched filtering, and communication with side information, to watermarking. Those techniques could be used to help design key building blocks of a watermarking system which deal with the following: How to embedding and detect one bit. What processing/embedding domain to use. How to ensure imperceptibility by utilizing side information How to embed multiple bits using multiplexing and modulation techniques How to improve the robustness and security of my system, where robustness can be defined as a watermark resistance to normal signal processing, and security can be defined as a watermark resistance to intentional attacks [6].

2.5. Distortions and Attacks

First, we have to distinguish two reasons for an attack against a watermark image: Hostile or malicious attacks, which are an attempt to weaken, eliminate or alter the watermark image, and Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark. Loss image compression is considered the most common form of attack a watermarking scheme has to withstand. The harsh term "attack" can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information the 81 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 invisible watermark. A wide range of attacks has been described in the literature. The following four large categories of attacks can be invoked to penetrate a watermarking system: • Removal attacks • Geometrical attacks • Cryptographic attacks • Protocol attacks

2.5.1. Removal Attacks

Attacks that attempt to separate and remove the watermark are known as removal (simple) attacks. If someone tries to remove the watermark from the data, this is called a removal attack. The means employed most frequently are filter models taken from statistical signal theory. De noising the marked image through median or high-pass filtering as well as nonlinear truncation or spatial watermark prediction are methods considered very likely to succeed. The goal is to add distortion to the host image in order to render the watermark undetectable or unreadable [4]. The attack is successful if the watermark cannot be detected anymore, but the image is still intelligible and can be used for a particular determined purpose. Many such attack operations have been proposed: • Lossy image compression (JPEG, JPEG 2000) • Addition of Gaussian noise • Denoising • Filtering • Median filtering and blurring • Signal enhancement (sharpening, contrast enhancement)

2.5.2. Compression

The compression is generally an unintentional attack, which appears very often in multimedia applications. All images that are now being distributed over the Internet have been compressed. The watermark is required to resist different levels of compression; it is usually advisable to perform the watermark embedding in the same domain where the compression takes place. For example, image watermarking in the Discrete Cosine Transform domain is more robust to JPEG compression than the spatial-domain watermarking. Also the Watermarking in the Discrete Wavelet transforms Domain is also robust to JPEG 2000 compression.

2.5.3. Additive Noise

Unintentionally, a random signal with a specific distribution (e.g. Gaussian, uniform, Poisson, Bernoulli) is applied to the image. In certain applications the additive noise may originate from Analog to Digital Converter (ADC), or as a consequence of transmission errors. Though, an attacker may introduce perceptually shaped noise (image-dependent mask) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector operates. Denoising explores the concept that a watermark is a form of additive noise (which can be modeled statistically) relative to the original image. These attacks include the following: trimmed mean filtering, local median, midpoint, Wiener filtering, as well as hard and soft thresholding.

2.5.4. Filtering Attacks are Linear Filtering Filtering attacks

include image-processing manipulations such High-pass, low pass, Gaussian and sharpening filtering, etc. In watermarked image, low-pass filtering, does not cause significant 82 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 damage, but can radically affect the performance since spread-spectrum-like watermarks have non negligible high frequency spectral contents. To design Robust Filtering Schemes against filtering attacks that might be applied to the watermarked image, the watermark message should be inserted in such a way to have most of its energy in the frequencies which filters change the least.

2.5.5. Statistical Averaging

This category includes the averaging and collusion attacks. Statistical averaging attacks are based on the fact that, if multiple images with the same embedded watermark are available, it is possible to estimate the watermark by averaging all those images, this is dangerous if the watermark doesn't depend substantially on data. This is reasonable grounds for using perceptual masks to create a watermark. Collusion attack is a malicious watermark removal

attack in which the hacker has access to multiple copies of the same content with a key or different watermark and essays to remove the watermark using averaging. The resulting signal may serve as a good estimate of the watermark, which can be used to remove it from the watermarked data.

2.5.6. Geometrical Attacks

Unlike to removal attacks, these attacks are not aimed at removing the embedded watermark, but try to distort the watermark detector synchronization with the embedded information. They attempt to break the correlation detection between the extracted and the original watermark sequence. The detector could recover the embedded watermark when perfect synchronization is regained. This can be accomplished by "shuffing" the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. These attacks can be subdivided into attacks applying general affine transformations and attacks based on projective transformation. Cropping is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place. Robustness to general geometric attacks often expect on the application of either a transform-invariant domain (Fourier-Melline) or an auxiliary template, or specially designed periodic watermarks whose auto-covariance function allows estimation of the geometric deformation.

2.5.7. Mosaic Attack

This point is emphasized by a "presentation" attack, which is of quite general applicability and which possesses the initially remarkable property that a marked image can be unmarked and yet still rendered pixel for pixel in exactly the same way as the marked image by a standard browser [24]. The attack was motivated by a fielded automatic system for copyright piracy detection, consisting of a watermarking scheme plus a web crawler that downloads pictures from the net and checks whether they contain a watermark. It consists of chopping an image up into a number of smaller sub images, which are embedded in a suitable sequence in a web page. Common web browsers render juxtaposed sub images stuck together. This attack appears to be quite general; all marking schemes require the marked image to have some minimal size (one cannot hide a meaningful mark in just one pixel). Thus by splitting an image into sufficiently small pieces, the mark detector will be confused. The best that one can hope for is that the minimal size could be quite small and the method might therefore not be very practical. 83 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022

2.5.8. Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks [24]. One such technique is brute-force search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks, which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key, it is very important to use keys with a secure length. Another attack in this category is so-called Oracle attack which can be used to create a non watermarked image when a watermark detector device is available.

2.5.9. Protocol Attacks

Protocol attacks neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather, they take advantage of semantic deficits of the watermark's implementation. The protocol attacks aim at attracting the concept of the watermarking application. The first protocol attack was proposed by Craveret al. They introduced the framework of invertible watermark and showed that for copyright protection applications watermarks need to be non-invertible. The idea of inversion consists of the fact that an attacker who has a copy of the stego-data can claim that the data contains also the attacker's watermark by subtracting his own watermark. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non invertability on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors proposed to make watermarks signal-dependent by using a one-way function. Consequently, a watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one image into another without knowledge of the secret key. It also belongs to the group of the protocol attacks. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data [7].

3. RELATED WORK

The research of medical images needs to tackle the problem of disclosing and changing of patient's 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: The goals of medical image watermarking (MIW) can be separated into two components, according to a survey report produced by Navas et al. [9]: (1) to control integrity and authentication and (2) to hide the electronic patient record (EPR) information. There is a need to embed watermark in the medical images. To fulfill the needs of privacy, integrity, and authenticity, we can use the digital watermarking scheme to receive correct information and provide proper treatment to patients. According to their applicability, another paper [13] categorized medical image watermarking methods into three categories: authentication, data concealing, and both authentication and data hiding combined. 84 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 El-Sheimy N. et al. [10] presented a new method for protecting patient information in which the information is embedded as a watermark in the discrete wavelet packet transform (DWPT) of the medical image. Wavelet packets are used to gain the advantage of better frequency resolution representation. One more advantage of wavelet packet is that it also adds the security as the basis is selected using the secret key. Rupinder K. in [11] Suggested a semi-fragile watermarking technique based on the Discrete Cosine Transform (DCT) domain to incorporate binary watermark into medical images. The binary watermark achieves a low amount of deterioration of the host image, resulting in a high level of quality. Ray et al. [14] 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 watermark are attained which are further encrypted with help of RSA algorithm. These encrypted SVs of watermark image are embedded into SVs of 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. Kaur et al. [15] proposed a new approach of image watermarking with the use of 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 process is done for all sub-bands especially while inverse DTCWT leads to generation of watermarked image. However, the developed technique turns out to be a non-blind scheme which requires original host image in extraction process. Where authors have highlighted the salient features of a variety of watermarking approaches, this actually aids researchers in providing roadmap for developing new watermarking techniques. Researchers have proposed a novel dual image watermarking technique in [16] where R Level DWT, The non sub sampled contour let 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 hierarchical tree (SPIHT) algorithm is employed successfully for compressing the watermarked image. Naheed et al. [5] 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 85 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 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 [17-18]. 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. A novel zero-watermarking algorithm for medical Images based on dual-tree complex wavelet transform (DTCWT) is proposed in [19]. 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.

4. PLIMINARIES

4.1. 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 [15]. 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 86 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 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.

4.2. Quantization

Quantization is the process of mapping a large set of values to a smaller set. Quantization can be used to reduce the amount of data without affecting visual quality. Quantization techniques can be classified into scalar quantization and vector quantization techniques. Scalar quantization refers to quantization with scalar input and output, whereas vector quantization refers to quantization with vector input and output. [16].According to whether the quantization step is uniform or not, quantization techniques can be classified into uniform and non-uniform. In the uniform scalar quantizer, each cell is the same length, however in the non uniform scalar quantizer, cells are varied lengths.

4.3. Singular Value Decomposition

SVD is an effective numerical analysis tool used to analyze matrices [17]. 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 Where T (.) (1) : 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: $s1 \geq s2 \geq .... \geq sn$. 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. 87 International Journal of 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 [17].

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 [4-6]. The other, such as Arnold transform Cat Map, focuses on changing pixel positions for the purpose encryption. [7-8]. However, changing the value or the position of the pixel could be decrypted. The most crucial factor that can control the key space of the chaos system is the initial condition where it give theoretically infinite key space resulting in more immunity towards brute-force attack [9]. Many different forms of chaotic systems can be employed to generate encryption sequences. In this work we use a logistic map. The 1D Logistic Map is one of the most well-known and commonly utilized chaotic systems. It is defined as follows: X n 1 μx n ( ) . 1 . + = − x n) (2) where x takes values in the interval (0,1). x0 is the initial value for the sequence, μ is a parameter which is user defined and used to generate a chaotic sequence; and n is the number of iterations. When μ > 3:57, the curves complete chaotic periodicity. When 3:5699456 ≤ μ ≤ 4, logistic mapping will be in chaos condition. The main flaw in a 1D logistic map is the key sensitivity; which depends on a single system parameter μ and an initial condition x0. The statistical complexity decreases as control parameters are increased. Another disadvantage is occurrence of periodic sequences in chaotic region which is more vulnerable to differential attacks such as chosen plain text attack. A large amount of secret can be revealed under same conditions. To avoid this problem we use a logistic map which encompasses the chaotic characteristic to encrypt the binary watermark image and this feature ensures the confidentiality of the proposed scheme.

5. PROPOSED SCHEME

5.1. Proposed Chaos-svd Ciphering Method

The permutation process changes the pixel position inside the block/image under the test without changing its value. The permutation process of our suggested cryptosystem is based on the following equation. ( )

⎧ ⎪ + =⎨ ( ) a* y i * 1 y i (− ( )) y i 1 a* y i *1 y i b ⎪ ⎩ ( ) (( )) . − + (3)

Where a, b are real parameters according to the map's initial condition, x(1)∈ (0,1). Following that, a binary sequence is obtained with the help of the following equation: 88 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 89 ( ) ( ) 1,if y i z i 0,otherwise T ⎧ > =⎨ ⎩ . (4) T is a predetermined threshold value that is dependent on the real parameters a and b. Furthermore, T is proportional to a and b, meaning that as the values of a and b increase, the value of T also increases and vice versa. We use the binary chaotic sequence quantized to mask the watermark image and then using the following equation creates the masked watermark bits ( ) ( ) ( ) u i z i r i = ⊕ . (5) Where ⊕the exclusive-or (XOR) operation, ( ) r i is the watermark image. After this encryption process, ( ) u i cannot be found through random search. The pseudo code of the watermark preprocessing is presented in Algorithm

1. Algorithm

1: Watermark Preprocessing Variable Declaration: ( ) W i = 1, 2, ..., M; j = 1, 2, ..., M:The watermark image ( )( ) y i + 1 i = 1, 2, . . . , M × M:Logistic mapping parameter, a, b: real parameters ( )( ) z i i = 1, 2, . . . , M × M :Binary sequence T: predetermined threshold value ( )( ) r i i = 1, 2, . . . , M × M :New one dimensional sequence from watermark (Wi). ( ) u i : encrypted watermark sequence Watermark Preprocessing Procedure: Let y(1)∈ (0,1) for i = 1: M do Calculate y(i + 1) with Equation (3) Calculate z(i) with Equation (4) Calculate u(i) with Equation (5) End for return encrypted watermark sequence The suggested Chaos- SVD image cryptosystem will be defined in terms of processes. The watermark (w) can be split into three segments: UW is an m×n matrix with orthonormal columns watermark. Sw is an n×n diagonal matrix with non-negative entries VwT is an n×n orthonormal matrix A three matrix was first scrambled by using a Logistic algorithm1 to generate a new UW Sw VwT. The original binary watermark image W is converted into an one dimensional sequence r, where r ={r(i), i = 1, 2, 3, . . . , M × M}. Then, in the final stage of preprocessing, r(i) is encrypted using z(i) with Equation (5), y(1), a, and b can be used as a secret key K. 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. International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 Fig 3: the proposed chaos-svd ciphering method Figure 4, show original and scrambled watermark with chaos-svd cryptosystem.

Fig 4: scramble watermark

5.2. Embedding Algorithm

The embedding algorithm makes use of DWT along with a chaos-SVD watermark to enhance the security. In the procedure of watermark embedding, a watermark image is first scrambled by using our chaotic algorithm before being embedded into the transformed domain of the host image. Step1: In the procedure of watermark embedding, a watermark image W was first scrambled by using our chaotic algorithm before being inserted into the transformed domain of the host image: Uw . Sw . Vw = CHAOS-SVD (w). Step2: The host image C was decomposed To R level DWT into four sub-bands using Daubechies-4 wavelet filter. C = LL, HL, LH, HH. Where M, N size of image and watermark. = M R log .N 2 Step3: Calculation of the threshold for each sub-band: (6) The approximation coefficients are a (m, n) and the detail coefficients of the level of resolution l and the sub-band s are ds, j (m, n) or s ∈ {HL, LH, HH} and l∈{1… L}. Furthermore, an 90 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 embedding location selection method is exploited to select blocks with small modifications as the embedding locations. This can reduce the embedding distortion and greatly improve the imperceptibility of our scheme. s,l T =qmax{d (m, n)}. l s, j (7) For each subband, if the detail coefficient is greater than or equal to the threshold calculated above, the bit of the watermark is inserted. Each bit of the brand is inserted directly into the LSB of each coefficient. To quantify the result, we will use an LBM, that is, a quantification followed by an insertion into the LSB. The quantifier operates on integers with an area set aside for coefficients that are too low to be zero. In LBM quantization, the least significant bit in the binary representation of a coefficient is replaced by the message bit (quantize-and-replace). While the generalized systems of LBM apply a vector generalization of this insertion strategy: = ( ) S q x .d m. +α ( ) (8) To adjust the embedding strength of the watermark, a scaling factor α was employed, q (x) represents the raw quantization which determines the significant bit, and d is determined only by the least significant (modulated) bit. The insertion by LBM never changes the significant bits of the source image; this is expressed by the strength of the quantization we used: ⌊ ( ) E q x x 0. –⌈ ⌉⌋ = (9)

Figure 4 shows the Q-DWT technique based on setting the least significant bit to 1 or 0 after quantization to insert the information(scrambled watermark). Δ being the quantization step.

Fig 5: LBM quantization

Step 4. Obtained the watermarked image C* by performing inverse DWT with the modified coefficient.

5.3. Extracting Algorithm

The extraction process require the original image, we use the wavelet coefficients, which should contain a watermark, only the coefficients with a value above the calculated threshold. 91 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 To extract the mark from the marked signal,. It is assumed that value of alpha, y(1), a and b for logistic scrambling technique are known for extraction procedure. To construct the watermark, the operation of DWT was applied to the watermarked image, and the high frequency approximate coefficient of which was further decomposed. The scrambled watermark was obtained under the utilization of the original host image and the wavelet coefficients, which should contain a watermark. Step1:S1 is detail coefficients of original image S1=q(x) +d1 (m). Step2:S2 is detail coefficients of watermarked image (S2- q(x))/ α = d2 (m). W= d2 (m) - d1 (m). Step3: The inverse Chaos-SVD is implemented to the resulted cipheredW1=Inverse-SHAOS SVD (W) 6. SIMULATION RESULTS Peak signal to noise ratio (PSNR), normalized correlation (NC) [18], are the parameters which are employed for evaluating performance of the proposed technique. PSNR=10log XYmaxp / (p-p) .(10) 10 ∑ 2 2 x,y x,y x,y x,y The Normalized Cross-Correlation (NC) is defined as 2 x,y NC= p p / p .(11) x,y x,y ∑ ∑ x,y x,y Where y x p , x,y is the matrix of the original watermark and y watermark. ~ p , x is the matrix of the extracted 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.

Fig 6. Types of medical images 92 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022

Fig 7: Binary watermark image.

Figure 8 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, Y(1), a=1,b=0.5.

Fig 8: original and watermarked image As the results are shown in Figure 9, the histogram of the encrypted image has a regular intensities' distribution. In fact, on comparing the histogram of the watermarked encrypted image with the histogram of the host image, therefore, the experimental results recommend that the encryption process can generate reliable results and is highly secure for medical imagery with a uniform distribution and maximum dissimilarity of

pixel values without leaving any clue for statistical analysis and attacks. In the absence of any type of attack, the PSNR equal to 45.73, it is important to get an NCC = 1 (without attacks) and a good value of PSNR. 93 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022

Fig 9: embedding crypto-watermarking system (PSNR = 45.73). 6.1. Robustness Analysis The watermark should be robust against attacks (the distortions due to attacks should remain minimal). The robustness of our proposed algorithm has been evaluated using normalized correlation (NC). To test and verify the robustness of our algorithm after extraction, the following attacks were applied to the protected medical image: Gaussian Noise (0, 0.01) Sharpening Average Filter (2×2) Median Filter (2×2) Cropping (1°) JPEG Compression (80) Salt & pepper Noise (0.05). Detailed results of NC in an average for all images are summarized in

Figure10. Fig 10: Robustness NC values against attacks. 94 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 95 To demonstrate the effectiveness of the proposed method, comparisons with other works are presented in Tables 1. Symbol '-' means NC values were not reported for these attacks. On observing Table 1 it can be easily interpreted that proposed scheme is superior as it offers better robustness in comparison to other reported techniques. Table 1. Comparison of the average NC value of the proposed method with [23, 22, 21, 19, 20]. Attacks [23] [22] [19] [21] [20] Proposed method Cropping left top corner 25% 0.8445 0.9997 - - 0.9966 - Noise attack (0.01) 0.9114 0.9589 - - - - Salt and pepper noise 0.9099 0.9589 - 0.9758 0.97572 Sharpening 0.9852 - 0.9018 0.9977 0.8898 0.97570 Gaussian filter 0.9488 - 0.9322 - - - Median filtering 2x2 0.9494 - - - 0.6973 0.98093 JPEG80 - - - - - 0.99468 Average filtering 0.9407 - - 0.9354 - 0.95643 Gaussian noise(0.01) 0.9114 - - 0.9144 0.93589 Rotation 1◦ 0.9881 - - 0.9728 0.9460 - bilin-crop1° - - - - - 0.90069 NC values are quite high for proposed technique as they are ranging from 0.999 to 0.90069 which is quite remarkable. Comparing our method with that of Mayssa Tayachi et al. [23] In the cases of Gaussian noise attacks, selt and paper noise, median filtering, and average filtering attacks, our strategy appears to be more effective against these four types of attacks. However, when we consider the Sharpening attack, the method of S.A. Parah et al. [21] has a higher NC value than the other methods. When we compare the results of our method with the method of S.Thakur et al. [20] in terms of NC, we can see that the results achieved after applying median filtering, sharpening and average filtering attacks to the watermarked image are less with our method however, in the instance of attacks such as selt and paper noise, There isn't much of a difference in the case of these attack. The method of Dagadu, et al. [22] has only been tested for cropping, noise attack (0.01) and selt and paper noise. Therefore, this method is very robust and performs well against these three types of attacks; while in the case of median filtering the normalized correlation coefficients of the attacked image and the original image of our method is more robust than other method (see column 8 of Table 1). The median is the central value. Median filtering reduces blurring of edges. The idea is to replace the current point in the image by the median of the brightness in its neighborhood. It is well known that in a set of ordered values. Sharpening spatial filters are used to highlight fine detail in an image or to enhance detail that has been blurred, either in error or as a natural effect of a particular method of image acquisition. Comparing our results with [19], our NC values between the original watermark and the extracted watermark in the case of sharpening is better than the results of [19]. A comparison of the proposed technique with [23,20].When adding the Gaussian Noise to the watermarked image, and fix the value of the variance to 0.01 and changed the value of mean; the results of the proposed algorithm are more robust than Mayssa Tayachi et al. [23], S.Thakur et al. International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 A few algorithms can fully resist strong compression JPEG and Jpeg2000. This forces the user to check whether his Watermark has been always present and limits it in its choice of compression levels. The results of the proposed algorithms under compression attacks give best correlation between original and extracted watermark. This is due to the fact that embedding is carried out in the low frequency sub-band which is less affected by compression attack.

6.2. Security Analysis

In order to provide more security, increase the power of the algorithm and preserve the watermark, the proposed AT-SVD system is used in the pre-processing step of the proposed method, we used a logistic map that includes the chaotic property of binary encryption of the watermark image and this feature will ensure the confidentiality of the proposed method: First, we used SVD and logistic mapping to encrypt the watermark, with a key K(x (1), a, b) used for both encryption and decryption. Second, there is another parameter, alpha (strong coefficient), which is used in the embedding process. Different values of alpha show different experimental results. A best strong coefficient was used for both embedding and

blind extraction. Therefore, without these parameters, it is difficult to detect the embedded watermark.

7. CONCLUSION

In the proposed watermarking scheme, the watermark is inserted in best dwt blocks which again helped the scheme in achieving high robustness by preserving the image quality intact. The security of watermarking is greatly improved when SHAO-SVD is administered. The experimental results of our method show that after several 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 when correlated with other related techniques, and the PSNR on average is equal to 53.45 dB. Therefore, our method is robust against different attacks. The evaluation results exhibit the high results of the proposed technique respect with fidelity of medical image.Due to limited bandwidth and illegal eavesdropping, future work will focus on the current intelligent algorithms, such as deep neural networks or the Hybrid Chaotic method, to encrypt the watermark images and create a distinct and selective joint encryption-compression system to simultaneously achieve the security and excellent compression performance of medical image transmission.

REFERENCES

[1] [2] [3] [4] [5] [6] 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. Joint NEMA/COCIR/JIRA Security and Privacy Committee,2003. "Defending Medical Information Systems Against Malicious Software," National Electrical Manufacturers Association-USA. Ravi Shah, Abhinav Agarwal and Subramaniam Ganesan, “Frequency Domain Real Time Digital Image Watermarking”, Oakland university, MI-48309, 1998. O. Bruyndonckx, J. -J. Quisquater, B. Macq, “Spatial method for copyright labeling of digital images”, Proceeding of IEEE Workshop on Nonlinear Signal and Image processing, Neos Marmaras, Greece, 20–22 June 1995, pp. 456–459. P. Moulin, M. K. Mihcak, “The data-hiding capacity of image sources”, IEEE Trans. Image Process, 2002. Jiwu Huang, Yun Q. Shi, Yi Shi, “Embedding image watermarks in DC components”, IEEE Trans. CSVT 10 (6) (2000) 974–979 96 International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 1, February 2022 [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] 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. Romualdas Bausys, Arturas Kriukovas, “Reversible Watermarking Scheme for Image the International Symposium ELMAR -2006, 07-09 Authentication in Frequency domain”, 48, June, Zadar, Croatia. Mandeep K. and Rupinder K.2012. "REVERSIBLE WATERMARKING OF MEDICAL IMAGES: AUTHENTICATION AND RECOVERY-A SURVEY," Journal of Information and Operations Management, vol.3, Issue 1, pp-241-244. El- sheimy N., Salwa A.K., Tolba A.S., Abdelkader F.M. and Hisham M. E., 2010."Wavelet Packets-Based Blind Watermarking for Medical Image Management," The Open Biomedical Engineering Journal, vol.4, pp.93-98. 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. 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. 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. 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. 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. X. G. Xia, C. G. Boncelet, G. R. Arce, (1997),“A Multi-Resolution Watermark for Digital Images”, in Proceedings of the IEEE International Conference on Image Processing, vol. 1, pp:548-551. F. Yu, Z. Lu, H. Luo, and P. Wang, (2001), “Three-Dimensional Model Analysis and Processing”, Springer-Verlag, Berlin Heidelberg. S. M. Haque, (2008),“Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking”, Master's Thesis, Computer Science, Blekinge Institute of Technology, Sweden. M. Kutter and F.A. Petitcolas, Fair evaluation methods for image watermarking systems, Journal of Electronic Imaging. 9 (2000), 445-456. 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 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. 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. Dagadu, J.C.; Li, J. Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimed. Tools Appl. 2018, 77, 24289–24312. Mayssa Tayachi et al. Tamper and Clone-Resistant Authentication Scheme for Medical Image Systems, 2020 Andreja S. and Jan .T.2008."ATTACKS ON DIGITAL WAVELET IMAGE WATERMARKS", Journal of ELECTRICAL ENGINEERING, VOL. 59, NO. 3, 2008, 131–138.