Watermark and Cryptography of Medical Images for Content Authentication

Huda Mohammed Alnoor¹, Saif Uldun Mostfa Kamal², Mohammed Jamal Almansor³
Rwaidah Aziz Abbas⁴, Ahmed Jamal Almansor⁵

¹Department of communication engineering, Iraq University College, Basra, Iraq.
²Department of Computer technology engineering, Iraq University College, Basra, Iraq.
³Department of communication engineering, Iraq University College, Basra, Iraq.
⁴Basra oil Company, Iraq, Basra.
⁵Department of Mathematical Sciences, Ministry of education, Basra, Iraq.

ABSTRACT

Medical images are often transmitted over insecure channel. Telemedicine enables medical diagnosis and Patient care using modern medical equipment’s. These equipment’s generate huge volume of data every day. Hence protection of medical image is very crucial. Many approaches like encryption, digital signature, watermarking etc. are spotted in the literature. Watermarking in medical images is commonly used for content authentication, effective data distribution and management, storage, security, safe archiving, controlled access retrieval, and captioning. Medical image is usually comprised of the region of interest (ROI) and non region of interest (NROI). ROI is the region that contains important information from a diagnosis point of view so it must be stored without any distortion. This paper develops an optimized embedding of payload in medical images by using genetic optimization. The goal is to preserve the region of interest from being distorted because of the watermark. By using this system there is no need to manually define the region of interest by experts as the system will apply the genetic optimization to select the parts of the image that can carry the watermark guaranteeing less distortion. The experimental results assure that genetic based optimization is useful for performing steganography with less mean square error percentage. This research develops an optimized embedding of payload in medical images by using watermarking and cryptography. The goal is to preserve the region of interest from being distorted because of the watermark.

Keywords: Medical Image Watermarking, DWT, Electronic Patient Record, Integrity, Authentication

1. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography (T. Morkel). The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” (T. Moerland).
Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is undetectable. The cover carrier can be different kinds of digital media such as text, image, audio and video (C. Liu and S. Liao). Many image steganography methods have been proposed. In these methods, the secret data is embedded into the cover-image by modifying the cover-image to form a stego-image. The most important requirement for a steganographic algorithm is to be imperceptible (M. Mohan and P. R. Anurenjan). Imperceptibility involves three features: **Invisibility** - The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

**Capacity** - Steganography aims at hidden communication and requires sufficient embedding capacity. Capacity is measured in bits per pixel (bpp) in images.

**Robustness** against statistical attacks and image manipulation - The amount of modification the stego amount medium can withstand before an adversary can destroy the hidden information.

Achieving all these requirements simultaneously is difficult to a great extend. Steganographic methods can be broadly classified in to 3 categories (A. Cheddad).

1. Spatial transform, 2. Transform domain, 3. Adaptive steganography methods. Common approaches in spatial domain include Least Significant Bit (LSB) manipulation. LSB insertion is the simplest method and very weak in resisting even simple attack such as transform, compression, etc. The transform technique involves modulating the coefficients of the cover data in the frequency domain. There are a few methods in fourier transform owing to it is not used for JPEG image format.

In contrast DCT is used extensively with image compression such as JPEG lossy compression. Although modification of properly selected DCT coefficient during embedding process will not cause noticeable visual artifacts, nevertheless they cause detectable statistical degradations. Various steganography methods like YASS (K. Solanki), MB, Outguess, Perturbed Quantization (PQ) have been proposed with the purpose of minimizing the statistical artifacts which are produced by modifications of DCT coefficients.

This paper proposes a method to embed data in DWT coefficients using a mapping function based on GA in 8x8 blocks on the cover image and, it applies the OPAP after embedding the message to maximize the Peak signal to noise ratio (PSNR). Only a few works on data hiding are done in DWT transform domain (H. Sajedi), (H. Sajedi and M. Jamzad), besides there are some image steganography methods that used GA (E. Ghasemi).

2. RELATED WORKS

This section presents Steganography is the art and science to hide data in a cover that it can be text, audio, image, video. Data hiding techniques are generally divided in two groups: **spatial** and **frequency domain** (Eswaraiah& Reddy, 2014), (M. almansor, 2017), (Jafari, Ziou, & Rashidi, 2013). The first group is based on embedding message in the least significant bit (LSB) of image pixel. The basic LSB method has a simple implementation and high capacity, however it has low robustness versus some attacks such as low-pass filtering and compression (Eswaraiah& Reddy, 2014). (Mohammed Al-mansor et al., 2017) developed a modified LSB method in which 8 bit ASCII codes of secret message are converted into 5 bit codes with the aid of encryption algorithm and then embedded in the cover image by using LSB method. Digital falsification of data aimed to succeed the counterfeiting syndicate these hidden plans. The falsification problem of digital data will from be resolved by applying the watermarking using LSB method (Least Significant Bit).
Different methodologies have been proposed in the literature for EPR authentication. Some methods have performed an integration between EPR encryption and hiding in the image under the concept of watermarking (Joint watermarking/encryption image for safe transmission) (Ajili, Hajjaji, & Bouallegue, 2014), (Rathi & Technology, 2012) EPR data are represented as ASCII of text files. In terms of watermarking, some researchers have used spatial domain based digital watermarking scheme for adding patient information to medical images. (Eswaraiah & Reddy, 2014), (Wu, Kao, & Hwang, 2011)

There are two types of LSB insertion methods, fixed-size and variable-size. In the fixed-size methods are embedded the same number of message bits in each pixel of cover image, and the variable-size embeds, the variant number of LSBs in each pixel used for message embedding depends on the image characteristics. A variant of LSB method can be found in (Chan & Cheng, 2004) that it proposes an optimal pixel adjustment process (OPAP) in which imperceptibility of the stego-image can be improved. Furthermore, this hiding method improved the sensitivity and imperceptibility problem found in the spatial domain.

The second group embeds the messages in the frequency coefficients of images. These hiding methods overcome the problem related to robustness and imperceptibility found in the spatial domain. JPEG, a standard image compression technique, employs discrete cosine transform (DCT). (M. almansor, 2017). Several steganography techniques for data hiding in JPEG have been proposed, recent researches apply discrete wavelet transform (DWT) (Manoj, Senthur, Sivasankaran, Vikram, & G, 2013) due to its wide application in the new image compression standard, JPEG2000. An example is the employment of an adaptive data embedding technique with the use of OPAP optimal pixel adjustment process to hide data in the integer wavelet coefficients of the cover image (El Safy, Zayed, & El Dessouki, 2009). (Sekra, Balpande, & Mulani, 2014) presented a genetic algorithm (GA) based steganography in discrete cosine transforms (GASDCT) domain and, GA based steganography using discrete wavelet transforms (GASDWT). GASDWT has an improvement in bit rate error compared to GASDCT. While others have used frequency domain such as discrete cosine transform (DCT) in (M. almansor, 2017) (Akter & Ullah, 2014)] based watermarking scheme which is capable of hiding EPR related data into a marked image (DWT) in (NileshRathi, 2014), (Hu & Hsu, 2015) and others used Two Label DWT and SVD (singular value decomposition) based watermarking technique for a more secure transmission of medical images (Conference & Group, 2014) Some have considered avoiding ROI region of interest in (Rathi & Technology, 2012), (Li & Kim, 2013).

The application of GA in steganography can increase the capacity and imperceptibility proposed a GA evolutionary process to make secure steganography encoding on the JPEG images. introduced a parameter optimization using GA that maximizes the quality of the watermarked image. Suggest by (Sekra et al., 2014)

3. APPLICATIONS OF MEDICAL IMAGE WATERMARKING

Medical Image watermarking has been used for different applications (gouenou et al., 2006) like Compact Storage, Saving Bandwidth, Avoiding Segregation, Tamper Proofing, Confidentiality and security, Indexing, Integrity Control, Captioning, Access Control and Origin Identification as discussed below. Huge amount of medical images are generated every day. Generation and managing the medical data is a challenging task faced by radiologist. In many hospitals electronic patient’s record (EPR) and medical images are stored separately. Requirement for memory for storage of images and patient record may increase rapidly. Hence embedding the EPR (meyer F.D et al., 1998) in the patient’s images may save lot of memory (Rajendra F.D et al., 2001) . And also if EPR and medical images are stored separately there is a chance for disconnection of patient data and image. Isolation or misplacing of patient data may create a problem in diagnosis which may lead to loss of money as well as life. To avoid segregation of EPR and medical images, (Aggeliki Giakoumaki et al. 2006) introduced watermarking technique to embed patient data & related information in the image itself. Transmission of multimedia data involves high bandwidth usage. Bandwidth is an important resource in network environment. Integration of EPR and the medical image saves the bandwidth requirement rather than sending EPR separately and medical image separately.
Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS) retrieve images based on querying mechanism (Johnson et al., 1999). As the communication of medical images extends beyond private network, there is a chance for casual or malicious tampering of medical image. Hence confidentiality and security of medical data is of paramount significance in medical data management systems. No patient likes to expose his/her medical report to public. Hence by imperceptibly embedding EPR data with advanced encryption techniques confidentiality and security may be maintained. To detect tampering, fragile watermarking techniques have been proposed. Fragile watermarking techniques embeds watermark that easily gets distorted in case on modification. Such watermarks can be used to authenticate the content. Works based on fragile watermarks even identifies the tampered regions, extent of tampering and even determines whether the data is truthful or not. Digital watermarks embed EPR in the image such that bandwidth and memory are utilized efficiently and effectively. It also provides a mechanism for storage of diagnostics data permanently into the image. Access to the images is made by proper keys only. For this reason watermarking is rising as a prospective tool for access control mechanism since different keys may disclose dissimilar information. Watermarks can also play the role of keywords or indices (e.g., ICD-10 diagnostic codes, image acquisition characteristics, patient demographics etc) for effective retrieval and archiving. Watermark can also be used for captioning. Caption or annotation watermarks can be used for providing additional information that is useful for diagnostics. Caption watermark includes health history of patient and diagnostics reports. Digital Signature or physician identification code is used as secret data in many reported works in the literature. In such cases the watermark can be used for origin identification. When watermarking combined with cryptographic technique complete protection is ensured.

4. REQUIREMENTS OF MEDICAL IMAGE WATERMARKING

Teleradiology is the transmission of radiological patient images from one location to another for the purposes of sharing studies with other radiologists and physicians. In particular medical image plays a vital role in telesurgery, telediagnosis etc. Security and privacy protection are critical issues to be considered in teleradiology. The security issues that need consideration are Confidentiality, Reliability and Availability.

- **Confidentiality**: It implies that only the authorized users can have access to the medical data.
- **Reliability**: It signifies two aspects a) Integrity - a proof that the information has not been altered or modified b unauthorized person. b) Authentication - a proof of the information origin and correct patient.
- **Availability**: It ensures access to medical information by the authorized users in usual conditions of access and exercise.

Security of medical images is very important when images are exchanged via Internet. In such cases, confidentiality and reliability are to be primarily considered. Digital watermarking techniques have the impending to act as a valuable tool for different range of security issues such as confidentiality, origin authentication, ROI protection, integrity and retrieval.

Watermarking techniques for medical health care applications differs from multimedia applications based on the properties of medical image and purpose of usage. The following requirements are specific to design authentication schemes for medical images.

**Reversible**: Medical images require intactness and good fidelity for diagnostic purpose. Hence it demands recovery of original image without any loss after removing the watermark. So the watermarking scheme should be reversible.

**Tamper detection**: Hospitals, insurance companies and even patients may alter the image for illegal purpose. Therefore the requirement is that when watermark is extracted the system should determine whether the image is tampered or not. In other word stamptering detection mechanism facilitates to identify whether the image is authentic or not.
**Localization:** When tampering is detected the scheme should be able to locate and recover the tampered region without any loss. That is the extraction and verification should be clever to reproduce and locate the illegally modified region of the image.

**Imperceptibility:** The watermark should not be noticeable under normal vision to the viewer nor should degrade the visual quality in the image. For medical applications visible watermarks are not encouraged.

**Robustness:** The watermark should resist attempts that were made to remove or destroy. They are mainly used for content tracking and copyright protection.

**Capacity:** Capacity describes how many information bits can be embedded. Higher capacity is normally achieved at the expense of other two requirements, imperceptibility and robustness. Blind Detection: The extraction process should not require the original image and original watermark. This is very important requirement for medical images to guarantee better security.

**Fragility:** The scheme should be sensitive to the attacks, so that the watermark can be easily broken in order to authenticate.

**Security:** Security implies that the watermarks should be difficult to remove without altering the cover image. It can also be defined as the ability to ensure authenticity and integrity of the watermark under malicious attack.

**Time:** The time needed for embedding and extraction should be kept small. It should be possible for the doctors to have a fast access to stored images and to make a report.

5. **PROPOSED ALGORITHM**

In this part includes the procedure of the security system for safe transmission of medical image. The system consists of sender, and receiver. The electronic patient record EPR represents patient information to be inserted in an image for the patient. Patient information is encrypted for achieving first level of security by hiding the meaning of the information. Next, encrypted data is inserted in the medical image, which represents a host image for the patient information to achieve second level of security by hiding the existence of the information. The whole process is performed at the sender side. Next, the host image is transferred through a communication channel to another party of the medical service. The goal of this operation is to meet two requirements. The first one is to keep the patient information secured and inaccessible to a third party. The second one is to enable an authentication of the host image that it is clean from any possible attack or corruption during transferring. At the receiver side, the process is repeated in an inverted manner; the patient data is extracted. Next, the decryption of this data is applied in order to restore the plain patient information. The authentication can be called based on matching the restored plain text with the agreed format of the patient information message. This procedure represents the typical crypto-steganography system. In this methodology, and as it is stated in the statement of problem, the goal is to insert the patient information with lower effect on the imperceptibility. Therefore, the optimization process of inserting the patient information is performed through using an evolutionary cryptography AES. This security system is evaluated in terms of imperceptibility by using two statistical measures: Mean Square Error MSE and PSNR.

A. **AES (ADVANCED ENCRYPTION STANDARD)**

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text. (Manoj, Senthur, Sivasankaran, Vikram, & G, 2013), (Sekra, Balpande, & Mulani, 2014)
The main loop of AES performs the following functions:

**Sub Bytes**
Sub Bytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

**Shift Rows**
Shift Rows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

**Mix Columns**
Mix Columns () also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics.

**Add Round Key**
The actual ‘encryption’ is performed in the Add Round Key() function, when each byte in the State is XORed with the sub key. The sub key is derived from the key according to a key expansion schedule.

![AES Encryption Flowchart](image)

**Fig. 1 AES Encryption Flowchart**

**B. EMBEDDING STEGANOGRAPHY**

To embed the watermark inside the image, the watermark has to be converted to binary format (sequence of ones and zeros). Next, padding operation is performed on the host image to have a width and height divisible by 8. This is for converting it to 8 X 8 pixels length of blocks. Then, the blocks of the image are converted to discrete wavelet domain (DWT) are scanned sequentially and the watermark is inserted in the pixel (8,8) according to the following logic:

1- If the watermark bit is 1, then do a quantization to the nearest odd number.
2- If the watermark bit is 0, then do a quantization to the nearest even number.

The same procedure has been used (M. almansor, 2017) This quantization function is defined as :-
Assume that \( f(i,j) \) represents the pixel of medical image, \( w(i,j) \) represents the binary pixel of watermark and \( F_k(u, v) = DWT\{f_k(i, j)\} \),

If \( w(i,j) = 1 \) then
\[
\Delta Q_e \left( \frac{F(x,y)}{\Delta} \right)_{x,y \in H_k} \quad 1 \leq K \leq N_{HB}
\]
\[F_k(x,y) = \]
\[F_k(x,y)_{x,y \in H_k} \quad 1 \leq K \leq N_{HB}
\]

If \( w(i,j) = 0 \) then
\[
\Delta Q_e \left( \frac{F(x,y)}{\Delta} \right)_{x,y \in H_k} \quad 1 \leq K \leq N_{HB}
\]
\[F_k(x,y) = \]
\[F_k(x,y)_{x,y \in H_k} \quad 1 \leq K \leq N_{HB}
\]

Where \( Q_e \) is the quantization to the nearest even number and \( Q_o \) is the quantization to the nearest odd number, \( \Delta \) is a scaling quantity and it is also the quantization step used to quantize either to an even or an odd number.

Fig. 2 Quantization Procedure
C. **EXTRACTOR**

Extracting of watermark is performed in an inverted way to the embedding procedure. That is, the host image is partitioned to 8 X 8 pixels lengths of blocks. Next, the blocks are scanned sequentially, and converted to DWT domain. Next, the pixel (8,8) in each block is checked, and the following logic is performed to extract the corresponding watermark bit:

1. If the value of the pixel is odd, then the corresponding watermark bit is 1.
2. If the value of the pixel is even, then the corresponding watermark bit is 0.

\[
\text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd when } w(i,j) = 0
\]

\[
\text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd when } w(i,j) = 1
\]
6. **AUTHENTICATION**

After extracting the watermark, and decrypting it, an authentication step is needed in order to validate that the host image has not been affected with any attack. In order to do this, the watermark plain data can be entered to a database in the system that includes information about all patient record number. The EPR should follow a predefined format. Any altering to the watermark bits will cause a change in the EPR format, and consequently, it can be used as a validation method for confirming that the image has not been exposed to any attack. The followed format in this thesis considers that the EPR consists of three types of fields: NAME, Date of Birth, and Record Number. A (#) delimiter separates each two consecutive field. Any violating to this format is used as an evidence of tampering the image.

7. **EVALUATION**

This research evaluates the performance of concealing data in the image using DWT applied to MRI, medical images based on statistical performance metrics like peak signal to noise ratio (PSNR), mean square error (MSE), normalized correlation (NC).
\[
\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j) - y(i,j))^2
\]

Where \(x(i,j)\) represents the original image and \(y(i,j)\) is represent modified image and \((i,j)\) are the pixel of position of the \(M*N\) , MSE is zero when \(x(i,j)=y(i,j)\).

\[
\text{PSNR} = 10 \log_{10} \frac{\text{Max}^2}{\text{MSE}}
\]

Where \(\text{max} I\) is the peak value of original image .The PSNR of an image is a typical measure used for assessing image quality by considering that the just noticeable distortions are uniform in all coefficients in a specific domain, such as special domain, frequency domain, or some transform domain. Since PSNR is more compatible and can be used to provide a generic bound for the watermarking capacity. So, we use the PSNR to analyze the watermark embedding distortions on images.

8. EXPERIMENTAL RESULTS

In order to validate the developed system, a set of 3 images with resolution of 3 has been used. Electronic records of 3 patients are encrypted by using advanced encryption system AES. Both embedding and extraction process are tested. After the patient electronic record is embedded in the image, a calculation of MSE and PSNR has been performed in order to verify the embedding quality or imperceptibility.

AES ENCRYPTION RESULT

As stated in chapter three, EPR has a predefined format. EPR starts with the patient name. Also, it contains the date of birth and record number. Each two fields are separated by # sign. AES algorithm has encrypted different EPR records. Table 1 shows the EPR plain texts and their encrypted results. This encryption step creates an initial security level before embedding the EPR in the patient image using the developed steganography.
Table 1 EPR plain text and cipher text

<table>
<thead>
<tr>
<th>EPR</th>
<th>ENCRYPTED EPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mohammed-almansor#04-12-1989-8483-8800-2020#</td>
<td>¦êfòûg·ÜûÖLÔöŽCôì ô @Fr¬Å%Y'gJGlâ$ôÖ&quot;,%ô«&quot;ë %dAYÉñªbl×0#</td>
</tr>
<tr>
<td>Huda-alnoor#15-08-1994#0182-8483-8800-2020#</td>
<td>ṮçFz&quot;³ô’NÔfì</td>
</tr>
<tr>
<td>Saifalsamer#24-09-1984#0569-0000-1456-4999#</td>
<td>½PYHˊˊ©</td>
</tr>
</tbody>
</table>

9. STEGANOGRAPHY PERFORMANCE

In order to evaluate the performance of the steganography, PSNR and MSE measures are generated for every image after inserting the EPR. PSNR is a good measure for imperceptibility while MSE is a measure for the amount of the noise that is interfered in the image. Table 2 shows each EPR, encrypted EPR, and its corresponding PSNR, MSE measures. In addition, the algorithm has been compared with (a method from the literature) in order to observe the relative performance with respect to the State of the Art methods. Figure 5 shows results PSNR and MSE Figure 6-7 Embedding process .Table 3 the comparison results between my study and others (add some comment, better or less) Lastly, Figure 8 comparison results PSNR .
Fig 6. Embedding DWT

Fig. 7 Embedding DWT
### Table 2 Encryption EPR and measures PSNR , MSE

<table>
<thead>
<tr>
<th>EPR</th>
<th>Encrypted EPR</th>
<th>PSNR</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mohammed-almansor#04-12-1989#0182-8483-8800-2020#</td>
<td>[êfòûg©U ù ÔLå Ö®Ž C £î û @ F r¬Â% Yi °GJg ìbSôÎ%,‰ &lt;&lt;œ‰Í ãÝÉººbÎ x0#</td>
<td>74.7231</td>
<td>0.0022</td>
</tr>
<tr>
<td>Huda-Alnoor#15-08-1994#0182-8483-8800-2020#</td>
<td>³ë©n•N Ô¶-¼ŷ³ôLå gååãï RMÜ•4+• ç^ÆhÚ</td>
<td>74.7121</td>
<td>0.0021</td>
</tr>
<tr>
<td>Saifalsamer#2 4-09-1984#0569-0000-1456-4999#</td>
<td>½²PYH´©,ëC¬qSéJz]sHS% Y¬E,n</td>
<td>73.4303</td>
<td>0.0015</td>
</tr>
</tbody>
</table>

![EPR Evaluated](image)

Fig. Evaluated EPR
<table>
<thead>
<tr>
<th>Author -Year</th>
<th>Objective</th>
<th>Domain</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Method -2020</td>
<td>Authentication</td>
<td>Encryption and DWT watermark</td>
<td>74.7231 dB</td>
</tr>
<tr>
<td>Sudeb Das &amp; Malay</td>
<td>Authentication integrity</td>
<td>Spatial</td>
<td>43.5-44.8 dB</td>
</tr>
<tr>
<td>Kumar Kundu [22] (2013)</td>
<td>and data hiding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dalel Bouslimi et al. [8] (2012)</td>
<td>Reliability</td>
<td>Spatial Encryption</td>
<td>53.9dB-60.15dB</td>
</tr>
<tr>
<td>Marco Fontani et al. [21] (2010)</td>
<td>Reliability</td>
<td>Frequency (Wavelet)</td>
<td>66-84dB</td>
</tr>
<tr>
<td>Viswanathan &amp; Venkatakrishna</td>
<td>Confidentiality</td>
<td>Spatial Encryption biometric</td>
<td>45-62dB</td>
</tr>
<tr>
<td>[23] (2013)</td>
<td>Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3 PSNR Results between my study and others

Fig.8 PSNR Results between my study and others
10. AUTHENTICATION

As stated in chapter three, different types of attacks are applied on the images. Next, the algorithm has been used to perform an authentication by extracting the EPR from the image after applying the attack, decrypting the EPR, and comparing the format with predefined format of the EPR. Figure 9-11 shows watermarked images and their corresponding attacked images. All authentication process has been applied successfully.

![Fig.9 Gaussian noise attack](image)

![Fig.10 salt and pepper attack](image)

![Fig.11 Rotation attack](image)
11. CONCLUSIONS

Steganography that is a branch of information hiding technology aims to hide a secret data securely in a cover media for transmission. Hiding EPR and stego-image quality are two important criteria in evaluating a steganography method. This paper presents a novel algorithm for embedding and extracting data in DWT domain. We employ a cryptography AES algorithm based mapping function to embed data in DWT Transform coefficients in 8x8 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. This research develops an optimized embedding of payload in medical images by using watermarking and cryptography. The goal is to preserve the region of interest from being distorted because of the watermark therefore improving the hiding capacity with low distortions. This work is more suitable for low or medium size of images while big size images cause a relatively high computational complexity for executing the optimization.

References


