Engineering and Scientific International Journal (ESIJ)
Volume 7, Issue 3, July – September 2020
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

A Theoretical Approach to Secure Medical Images by Combining Cryptography and Watermarking Techniques

K.Anusudha

Assistant Professor, Department of Electronics Engineering, Pondicherry University, Pondicherry, India

Abstract— Medical Imaging has remoulded the Healthcare system. It has become a vital tool for rapid diagnosis with visualisation of the interior of the body. Telemedicine is that the remote delivery of healthcare services over the telecommunication infrastructure. This paper aims at providing security to the medical images transmitted over public networks. It addresses the following traits of Medical Image Security namely: Confidentiality, Patient's control, Data Integrity and Consent Exception .The objective of the paper roots on providing theoretical ideas by combining Watermarking schemes with Cryptography techniques for developing enhanced security algorithms for transaction of medical images. The various parameters used for the measurement of the performance and effectiveness of the proposed algorithms such as Entropy, Number of Pixel Change Rate, Unified Average Change in Intensity, Correlation Coefficient, Mean Squared Error and Peak Signal to Noise Ratio are discussed. This paper provides a road map in constructing new algorithm by combining cryptography and watermarking technique for secure transaction of medical.

Keywords *— Power Factor Penalty; Time of Day Tariff; Demand and Energy Charges*

1. Introduction

Medical imaging has given healthcare a new up front. It has paved a way to improve physicians to diagnose, treat and to identify medical illness and conditions. The broad applicability of medical imaging has sprouted as a logical consequence of physicians integrating imaging into the quality treatment patterns. This has led to a rapid increase within the usage of medical images. Advances in electronics, miniaturization, visualization, acquisition and determination have made transaction of medical imaging faster, precise and mobile. Thus, the main transformation in healthcare is that imaging has become a typical aid for diagnosis and treatment of all major medical conditions and diseases.

Telemedicine is an innovative system of healthcare provision from distance utilizing the telecommunication and modern information technologies. Telemedicine has spread rapidly and has integrated into the functioning of hospitals, specialty departments, private physicians as well as consumer's homes and workplaces. It has provided the facility of providing health care independent of geographical distances. Telemedicine technology helps in connecting specialist in urban areas with the patients in non-developed areas, thereby making the health care system less complex and readily available. Though the technology adds to facilitating in reducing the patients' visit and home bound patients can seek help without moving to the clinic, but requires innovative techniques to prevent unauthorized and illegal intruders during the transaction of medical images. Therefore the most vital challenge is maintaining the integrity of medical images transferred over communication networks.

The Health Insurance Portability and Accountability Act (HIPAA) was established in1996 by the U.S Federal Law regulating healthcare industry for secure exchange of patient's information and to maintain the integrity of the information. In addition consumers have also demanded privacy and security of their health information that includes all forms of oral and electronic representations.
The following are the privacy and security rules of the Health Insurance Portability and Accountability Act:

- *Data Security Rule:* Will establish technical and administrative protocols for security and integrity of Electronic Health Data.
- *Privacy Rule:* Will establish guidelines for disclosure of patient's medical information.
- *Transactions and Code sets:* Will establish standard formats and coding of electronic claims and related transaction.

Telemedicine requires suitable techniques to support the above rules. Combining Digital Watermarking and Cryptography techniques provides copyright protection, authentication and integrity of medical images. Digital watermarking concentrates on hiding secret messages on the cover medical image. Cryptography adds more security to the watermarked image for safe transaction of medical images.

The paper gives a brief literature survey in section 2. Digital watermarking technique, various watermarking schemes are discussed in section 3. Section 4 gives a detailed process of cryptography techniques. Section 5 gives a new approach of combining Watermarking and cryptography techniques. The parameters used for the evaluation of the combined techniques are explained in section 6. Section 7 states the conclusion of the work.

DOI: **10.30726/esij/v7.i3.2020.73014**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

2. Literature Survey

Research activities in medical image security have been on the front end from the day of evolution of transmission of patient's information over public networks. In this thesis, robust digital watermarking algorithms are developed, to preserve the perceptual quality of the cover medical image with invisible watermarks. Digital watermarking may be a process whereby information is embedded into a picture in such how that the extra payload is imperceptible to image observers. Image watermarking has been proposed as an appropriate tool to spot the source, creator, owner, distributor, or authorized consumer of a document or a picture. It also can be wont to detect a document or a picture that has been illegally distributed or modified. Cryptography may be a process of obscuring information to form it unreadable to observers without specific keys or knowledge. This technology is usually mentioned as data scrambling. Watermarking complemented by cryptography can serve an outsized number of purposes including copyright protection, broadcast monitoring, and data authentication.

Confidentiality and Integrity are the important components within the maintenance of health record. Confidentiality refers to denial of access to unauthorized users during the transaction of medical records. Integrity implies that the pictures shouldn't be changed at any stage of the transmission process. Watermarking has been proposed as a security mechanism for improving medical image security. Digital watermarking can unnoticeably embed messages without altering image size or its format. Thus, it allows associating in protecting data with the information to be protected. Watermarking are often used for verifying the reliability of a picture by asserting its integrity and its authenticity. for instance , during a transaction, patient name and doctor's identity are often inserted within the image. Researchers have reported findings that watermarking techniques satisfy both confidentiality and integrity requirements (Shih et al, 2005; Zhou et al ,2001; Chao et al, 2002; Luo et al, 2003; Giakoumaki et al,2003;Cheng et al,2005; Acharya et al,2004; Nayak et al, 2004 and Srinivasan et al,2004). Hospital data system (HIS) and movie Archiving and Communication System (PACS) are initiated to supply confidentiality, integrity and authentication of health care information. Many applications of watermarking in medical images have been investigated extensively to assure secure (Cao et al, 2003; Coatrieux et al, 2000; Acharya et al, 2003; Fridrich et al, 2001 and Frank Y.Shih et al, 2005). These applications include data hiding, integrity control, protection, authenticity, invertible watermarks that can be completely erased after verifying image and interleaving patient information with medical images. Watermarks used for these applications got to be sensitive to any modifications to the pictures. The Digital Watermarking algorithms are often classified into two classes counting on the domain of watermark embedding. The first group belongs to the algorithms which use spatial domain for data hiding and the second group takes advantage of transformation domains like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) for watermarking purpose. Digital Watermarking can also be categorized into visible and invisible, fragile and robust, blind and non-blind with emphasis on authentication, rightful ownership and availability of the host image respectively.

Cryptography techniques can scramble secret information into an unreadable message. However, the unreadable message can easily attract unauthorized attention. Watermarking techniques can provide secure transmission by embedding secret information within covert carriers to avoid observations .The similarity between cryptography and watermarking techniques is that only an authorized person with right key can recover the secret information. Hence the best approach is to combine watermarking with cryptography techniques to protect the security of secret information.

Guo and Zhuang (2003) stated that digital watermarking applied to medical images should not impose visible changes on the watermarked medical image. Zhou et al (2001) have worked on maintaining authenticity and integrity of digital mammogram image using digital watermarking technique. The Least Significant Bit of randomly chosen pixel of the mammogram image is replaced with one bit of the Digital Envelope (DE) used as a watermark. But the method proposed can be applied only to a portion of the cover image.

Yusuk Lim et al (2001) projected a web-based image authentication system. The main purpose of this method is to verify the integrity and authenticity of medical images by a client server model in which the server performs watermark detection and client access server using internet. The proposed method uses bit plane slicing technique alongside hash function. A warning message is generated by the server if the transmitted message is distorted or modified. The proposed method has not been analyzed by subjecting to attacks and security of the watermarking scheme.

Chao et al (2002) proposed a Discrete Cosine Transform (DCT) based watermarking technique wherein Electronic Patient Record (EPR) is employed because the watermark. the first cover image obtained after the extraction process is claimed to be distorted. Cao et al (2003) worked on embedding the Digital Envelope within the selected Least Significant Bits of the duvet image. Since the proposed method is fully random, reconstruction of the embedded Digital Envelope wasn't successful.

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Frank Y. Shih and Y.T.Wu (2005) proposed a watermarking technique based on genetic algorithm. The watermark is embedded in Region of Non-Interest (RONI) of the cover medical image. Lossy and lossless compression techniques are used to achieve optimal compression. The proposed watermarking technique was a fragile technique which cannot be used for all applications.

Hyung et al (2005) introduced a digital watermarking technique for medical images to prevent illegal forgery caused while transmitting medical images over open network. In the proposed technique the medical image is divided into ROI and RONI .The ROI is embedded into the RONI portion. The complete process is done in wavelet domain. The main drawback of the proposed scheme is the computational complexity.

Cheng Ri Piao and Dond-Min (2008) proposed a combined Integer Wavelet Transform (IWT) and hash function based fragile watermarking for security of medical image. The cover medical image is subjected to first level Integer Wavelet decomposition. The hash values of the watermark content are embedded into the LSB bit of the Wavelet Transformed image. The proposed technique has stopped with the first level of decomposition, which can be extended to further levels to increase the level of security.

V. Fotopoulos et al (2008) proposed a method similar to Hyung et al (2005) method where in the scheme embeds the ROI of image into RONI portion of the cover image. A rectangular portion of the cover image taken as the ROI undergoes JPEG compression. At the receiver end, decompression is performed and compared with cover image portion to check the integrity of the image transmitted.

Wang Yan and Ling-di Ping (2009) proposed a spatial domain based steganography algorithm for color images. The secret data's are arranged to overcome distortion. Embedding is done completely based on the LSB substitution method, which cannot withstand hostile attacks .Mustafa Ulutas et al (2011) proposed a (k, n) secret sharing scheme which shares medical images among a team of n clinicians such that a smallest amount k of them must gather to reveal the medical image to be diagnosed. The proposed method overcomes the limitation on hiding capacity. But the proposed technique is not suitable for all situations of telemedicine diagnosis.

Wang Yan and Ling-di Ping (2009) proposed a spatial domain based steganography algorithm for color images. The secret data's are arranged to overcome distortion. Embedding is done completely based on the LSB substitution method, which cannot withstand hostile attacks. Mustafa Ulutas et al (2011) proposed a (k, n) secret sharing scheme which shares medical images among a health team of n clinicians such a minimum of k of them must group to disclose the medical image to diagnose. The proposed method overcomes the limitation on hiding capacity. But the proposed technique is not suitable for all situations of telemedicine diagnosis.

3. Digital Watermarking

Digital watermarking has a close relevance to steganography / Information hiding. In general, information hiding refers to hiding secret information. Based on the application, the secret information may be perceptible or copyright protection or imperceptible for integrity checking. Thereby, digital watermarking and steganography have similar approach, but the application ad solution makes it independent (Mauro Barni and Franco Bartolini, 2004). Watermark embedded on the cover data are commonly used for copyright protection. In addition, to prevention of illegal copyright, there are number of applications that forces to focus towards the research on digital watermarking. Watermarking varies from other conventional hiding techniques in three major ways First, Watermarking does not cause perceptible changes on the cover image. On transaction of watermarked images, attackers aim to distort the content of the watermarked image by introducing modifications such as additive noise, compression, rotation, cropping etc. Second, the watermark can be extracted / detected only with correct embedding key. Third, the watermarks undergo the same transformation as the cover image.

A watermarking system is much like a communication system consisting of three main elements: an embedding process, a communication channel and an extraction process. During the embedding process, the secret information is embedded in the host image using a secret key. Any processing applied to the host data after information concealment, along with the interaction between the concealed data and the host data, represents the transmission through a communication channel.

3.1 Embedding Process

In watermark embedding an embedding function 'ε' takes the host image 'A', the watermark image 'w', key 'K', to generate the watermarked image 'A_w' such that

$$\varepsilon\,(A,\, w,\, K) = A_w \qquad (3.1)$$

Equation (3.1) represents the embedding process wherein the watermark is embedded into the selected features of the host image. Let $F(A)$ denote the selected features of the host image and the watermark embedding process can be performed as shown in equation (2.2) embedding rule:

$$F(A_w) = F(A) \oplus w \qquad (3.2)$$

DOI: **10.30726/esij/v7.i3.2020.73014**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

'⊕'denotes the watermark insertion operation. The main concern of the embedding part is to make the hidden data imperceptible. This task can be achieved, by properly choosing the set of host features and the embedding operation. After embedding, the watermarked image 'A_w' enters the communication channel and undergoes a series of attacks. Attackers may explicitly aim at removing the watermark from 'A_w', or may pursue a completely different goal, such as data compression, blurring, sharpening, cropping etc. The resulting image is denoted by the symbol '*A'w'*.

3.2 Extraction Process

The receiver end of the watermarking system can take any one of the two forms: According to first method, the detector receives the watermarked image '*A'w'* and 'b*' the watermark code as input. The host image '*A'* and the key *'K'* used for the embedding process may be provided to the detector. If the detector uses the host image for the detection, then it is termed as blind watermarking and the vice versa condition is termed as non-blind watermarking. The second method represents a watermark decoder that tries to obtain 'b*' from '*A'w'*. Similar to watermark detector, the host image and the key may be provided for the extraction process. These two forms leads to classification of watermarks whose presence can be read and those watermarks that can be detected.

The receiver part of watermarking scheme can assume two different forms namely blind and non-blind scheme. The distinction between readable and detectable watermarking can be further highlighted by considering the different form assumed by the decoding/detection function '*D'* characterizing the system. In blind, detectable watermarking, the detector P is a three- argument function accepting inputs such as watermarked image '*A'w'* , watermark '*w'*, and secret key '*K'*. '*D'* decides whether '*A'w'* contains '*w'* or not as given in equation (3.3).

$$D\,(A'w,\ w,\ K) = A \qquad (3.3)$$

3.3 Watermarking Schemes

3.3.1 Spatial Domain Watermarking

The most straight forward way of watermarking is to directly embed the watermark on the pixels of the cover image. It helps in controlling the maximum difference between the original image and the watermarked image. There has been two major ways by which the watermarking in spatial domain is performed.

3.3.1.1 Additive Watermarking

The most commonly used method for watermark embedding is to add some amount of watermark into a host image for embedding according to equation (3.4).The embedding process is given by the following equation

$$A_w(i,j) = A(i,j) + \alpha(i,j)\, w(i,j) \qquad (3.4)$$

Where '*A(i, j)'* denote the original image ' $w(i,j)$ ' denotes the watermark,' i 'denotes the location of the embedding and '$\alpha(i,j)$'denotes the strength factor whose value ranges from $0 \leq \alpha \leq 1$.Large value of ' $\alpha(i,j)$' will distort the host image to a large extent. In order to overcome this, block based additive watermarking (Lin and Delp, 1999) .Watermark extraction in spatial domain becomes a difficult process since the extraction requires the locations of the pixels where the watermark is embedded. Therefore it requires original host image to extract the watermark.

3.3.1.2 Least Significant Bit Modification

Least significant bit (LSB) modification for embedding the watermark in the host image is the most commonly used spatial domain watermarking. It is achieved by imperceptibly changing the LSB bits of the host image with the watermark bits. This method achieves significantly less distorted watermarked image. However the embedded watermark is not robust against attacks like lossy compression.

3.3.2 Frequency Domain Watermarking

Frequency domain watermarking helps in achieving better robustness and imperceptibility compared to spatial domain watermarking (Nickolaidis and Pipas, 1998). It is also termed as multiplicative watermarking technique. Conventional transforms namely Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) are commonly used for frequency domain watermarking. Watermarking in frequency domain is achieved through three stages: i) Image is transformed to frequency domain ii) Embedding phase and iii) Detection / Extraction phase. Transformation can be applied on the complete image or on selected block of the image. Watermarking in frequency domain modifies the selected co-efficient which is represented as:

$$I_i' = I_i + \alpha . I_i . W_i \qquad (3.5)$$

Where, I_i and I_i' represents the original and watermarked images respectively, 'W_i' denotes the watermark and 'i'represents the position to be embedded and 'α' is the watermark strength factor. A correlator helps in complete extraction of the watermark.

4. Cryptography Techniques

Cryptography is the technique of converting the readable information into non-readable form, using a secret key. Cipher text refers to encrypted form of the plaintext.

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Histograms are frequency distributions, and histograms of images describe the frequency of intensity values that occur in a picture. Mathematical expressions and algorithms are used to scramble the data into unreadable form. It can be decoded or decrypted only with the authentication key (William Stallings, 2005).

Hu et al (2009) used cryptography technique on medical images. However encrypted image may attract hackers and the issue related to key sensitivity were not discussed. Puech et al (2004) proposed an asymmetric encryption algorithm by performing the encryption twice. Acharya et al (2003) proposed a spatial domain watermarking technique, wherein the secret text is encrypted before being embedded into the cover medical image. The effectiveness of the proposed algorithm was not verified.

Cryptography addresses the following desirable properties:

- *Confidentiality:* Only the sender and receiver are allowed to access the message.
- *Authentication:* The receiver can identify the authenticated owner of the message.
- *Integrity:* The receiver should be able to identify any change in the transmitted message.
- *Nonrepudiation:* The sender cannot deny the transmission of the message.

All these properties are also addressed by the watermarking technique. Symmetric-key cryptography, Asymmetric-key cryptography, One-way hash functions and Cryptographic signatures are the four basic classifications of cryptography techniques.

4.1 Symmetric Key Cryptography

Symmetric-key cryptography or secret-key cryptography shares the secret key used for the encryption process. The key 'K' is used in the encryption function as denoted by $E_K(.)$ and a decryption function D_K (.). The plaintext is denoted as 'm' and its encrypted cipher text as 'm_c'.The encryption operation is as follows:

$$m_c = E_K(m) \tag{4.1}$$

Similarly, the cipher text 'm_c' is decrypted to obtain the plain text 'm' by

$$m = D_K(m_c) \tag{4.2}$$

The main drawback of this technique lies in the secret sharing of the key used for the encryption. It becomes complex when more number of people are involved in the communication.

4.2 Asymmetric Key Cryptography

Asymmetric-key cryptography was introduced to overcome the drawback of symmetric key cryptography, using different keys for encryption and decryption. A pair of keys, 'K_E' and 'K_D', the message can be encrypted using K_E, and decrypted using K_D and vice versa as given below:

$$m_c = E_{K_E}(m) \tag{4.3}$$
$$m = D_{K_D}(m_c) \tag{4.4}$$

For each encryption key, there is a corresponding decryption key for obtaining the plaintext. The main advantage of the asymmetric key is a knowledge any one of the key does not allow to detect the other key. Distribution of the public key does not cause any risk on the encryption technique. Asymmetric key can be implemented in a number of ways. That is, either a public key or private key can be used for the encryption process.

4.3 One-Way Hash Function

A one-way hash function is one of the function that is simple to calculate, but the inversion operation is more complex. It is easy to find the corresponding output for the given input, but the vice versa is not possible. Common one-way hash functions are MD5 and Secure Hash Algorithm (SHA). One-way hash functions is for checking the integrity of a message. This can be checked if the sender can compute a hash 'H'of the message 'm' with a secret key 'K'as,

$$H = h(m + K) \tag{4.5}$$

Where, '$m + K$' indicates the string concatenation of 'm'and 'k'. $H(.)$ is a one-way hash function. The hash value is often referred to as a Message Authentication Code (MAC), or Data Authentication Code (DAC).

4.4 Cryptographic Signature

A Cryptographic Signature uses asymmetric key cryptography technique to solve key exchange and authentication problem. It can also be used instead of Message Authentication Code. To produce a cryptographic signature, a one-way hash of the message is computed and encrypted using a private key as shown in the below equation:

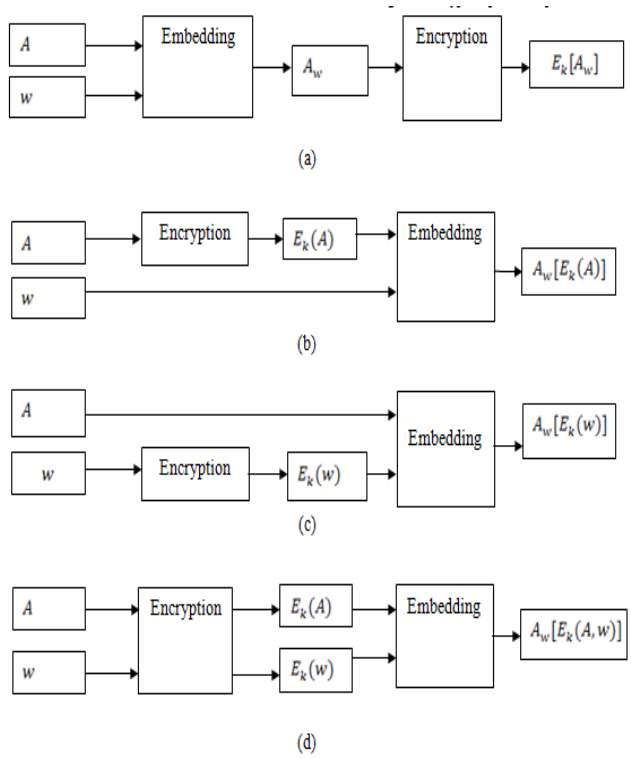
$$S = E_{K_E}(h(m)) \tag{4.6}$$

5. Combined Watermarking with Cryptography Techniques

This section focuses on the idea of combined watermarking with cryptography techniques. It is a known fact that both the techniques are widely used as a means of transmitting data more securely.

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)



a, b, c & d are four methods

Fig.5: Block diagram for combined watermarking with cryptography systems

The common applications of both the techniques are copyright protection, authentication and integrity. The combined system is expected to perform better than when operated separately. Table1 shows different ways of combining watermarking with cryptography techniques. The combination can be performed by changing the order of the technique in the system. From Table 1, it can be inferred that the system generates an encrypted watermarked image or watermarked encrypted image based on which four types can be formulated. In addition to varying the ordering of the technique, the system can also be constructed by combining watermarking techniques operating in different domains with cryptography techniques belonging to different classes. Although cryptography techniques provide secure data exchange, the decryption process depends on the secret key used for the generation of the cipher text that is not tampered. Similarly in Watermarking techniques, the cover image embedded with the watermark appears imperceptible to the Human Visual System, but this form of transmission is not suitable for all conditions of Public networks.

Let A denote the cover image and w represents the watermark image. The watermarked image is denoted as A_w and the encrypted watermarked image as $E_k[A_w]$.$E_k(A)$ denotes the encrypted cover image and $E_k(w)$ denotes the encrypted watermark image. The watermarked encrypted image is denoted as $A_w[E_k(A,w)]$.

Table 1. General Methodology for Combining Watermarking and Cryptography System

Methods	Input to Encryption	Input to Embedding	Remarks
Method I	A_w	A and w	Encrypted Watermarked Image
Method II	A	A' and w	Watermarked Encrypted Image
Method III	w	A and w'	Watermarked Encrypted Image
Method IV	A and w	A' and w'	Watermarked Encrypted Image

Figure 5 depicts possible types of Combined Watermarking and Cryptography techniques as described in Table 1.In Method I, as shown in Figure 5 (a), the cover image and the watermark image are fed directly into the embedding system whose output namely the watermarked image is fed as input to the Encryption system to generate the Encrypted Watermarked Image. In method I, Watermarking is performed first and cryptography is performed second in the combined system. In method II as shown in Figure 5 (b), the cover image is encrypted and watermarked with the watermark. Thereby the system generates Watermarked Encrypted Image. In method III, the watermark is encrypted before being watermarked with the cover image. The system also generates a Watermarked Encrypted Image which is depicted in Figure 5 (c). In method IV, both the cover image and the watermark are encrypted before being watermarked as shown in Figure 5(d).In method II, III and IV, Cryptography is performed first and watermarking is taken second in the combined system.

6. Performance Metrics

6.1 Histogram

Histograms are used for frequency distributions, and the images of histograms describe the frequency of intensity values that occur in an image. Willhelm Burger et.al (2008) describes an image histogram, where the X axis shows the gray level intensities and Y axis shows the frequency of these intensities. For an image of 8-bit gray scale, 256 different possible intensities are there. Therefore, the histogram will display 256 numbers to represent the

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

distribution of pixels amongst the grayscale values. The image is scanned in a single pass and a running count of the number of pixels found at each intensity value is kept which is used to construct a histogram. Paul.A.J et.al (2012) proved that Histograms also can be taken for colour images either individual histogram of red, green and blue channels are often taken, or a 3-D histogram are often produced, with three axes representing the red, green and blue channels, and brightness at each point representing the pixel counts. With a histogram, it is easy to determine certain type of problems in an image, for example, it is simple to conclude if an image is properly exposed by visual inspection of its histogram. In addition to image capturing, histograms are also used to improve the appearance of an image and as a tool to determine what type of processing has previously been applied to an image

6.2 Mean Square Error

Mean Square Error (MSE) between two images is a picture fidelity measure.The goal of the image fidelity measure is to match two images by providing a quantitative score that describes the degree of similarity/fidelity or conversely, the extent of error/distortion between them.Usually, it's assumed that one among the signal may be a pristine original,while the opposite is distorted or contaminated by errors presented by Zhou Wang.et.al (2009).

In other words, Mean Square Error is that the average squared difference between a reference image and a distorted image.It is computed pixel -by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count citedby Tom Distler et.al (2011). The lower the worth of MSE the image is claimed to be in fitness . Suppose there are two images and of size M N ,the MSE between the pictures is,

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{m=1}^{M} \sum_{n=1}^{N} [g'(m,n) - g(m,n)]^2 \qquad (6.1)$$

6.3 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) analysis uses a standard mathematical model to measure an objective difference between two images.It estimates the quality of a reconstructed image with respect to original image. Reconstructed images with higher PSNR are judged better.PSNR is the ratio between maximum possible power of a signal and the power of noise.It is usually expressed in terms of the logarithmic decibel cited from V.Santhi et.al (2016). In literature of image processing, MSE is often converted in to a Peak Signal to Noise Ratio and measured as ,

$$\mathrm{PSNR} = 10 \log_{10} \frac{\mathrm{L}^2}{\mathrm{MSE}} \qquad (6.2)$$

Where, 'L' is the maximum pixel intensity. If the two images are identical then MSE is 0 and PSNR is infinity. The improvement in PSNR increases the visual exterior of the image. In medical images, the PSNR is a factor for authentication. If the image is having any kind of noise then PSNR falls into a not acceptable lower value. Even if the image is recovered, there is no use as the medical images need high quality and precision. Thus greater the PSNR the image is said to be in good quality even after the processing cited from Mohan Kumar .S et.al (2012).

6.4 Number of Pixel Change Rate and Unified Average Change in Intensity

To implement differential attack, an opponent usually makes a slight change on one pixel in the plain image and ciphers the two images using the similar secret key. Chong Fu et al (2014) stated that if some meaningful relationship between the plain image and cipher image can be found by comparing the two cipher images, the secret key may be determined with the help of some other analysis methods. In case of image processing Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) test are used to reduce the probability of differential attack. High NPCR and UACI are expected to reach the goal. NPCR defines the number of pixels change rate of chipper image while one pixel is changed. Mathematical expression of NPCR as explained follows: Suppose P1 is a plain image, C1 is corresponding cipher image, P2 is another plain image which is exactly same as P1 except one pixel. Now C2 is considered as a cipher image of plain image P2.

$$\mathrm{NPCR} = \frac{\sum_{i,j} \mathrm{D(i,j)}}{\mathrm{W} \times \mathrm{H}} \times 100\ \%$$

Where 'D(i, j)' is defined as

$$\mathrm{D(i,j)} \begin{cases} 1, \text{if } \mathrm{C1(i,j)} = \mathrm{C2(i,j)} \\ 0, \text{if} \mathrm{C1(i,j)} \neq \mathrm{C2(i,j)} \end{cases} \qquad (6.4)$$

Where, 'W'means width of image and 'H' height of image. UACI is used to identify average intensity changes among two cipher images whose one pixel is changed. Mathematical expression is as follows:

$$\mathrm{UACI} = \sum_{i,j} \frac{|\mathrm{C1(i,j)} - \mathrm{C2(i,j)}|}{\mathrm{F\ T}} \qquad (6.5)$$

Where, C1 and C2 are cipher images of plain image P1 and P2. Both P1 and P2 are same except one pixel. 'F' is largest pixel value supported by cipher image and where 'T' is total number of pixels.

6.5 Entropy

Entropy can be explained as a measure of chaos in a system. Another way of entropy is to consider the spread of

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

states that a system can adopt. A low entropy system engages a small amount of such states and a high entropy system carries a large amount of states. In an image, these states correspond to the gray levels that an individual pixel can adopt. For example, an 8-bit pixel has 256 states. If all such states are equally engaged, as they are in an image which has been entirely histogram equalized, the spread of states is utmost, as the entropy. On the other hand, if the image has been threshold, so that only two states are occupied, the entropy is low. If all pixels are having the same value, then the entropy of the image is zero. In information theory, entropy is thus the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy $H(s)$ of a source s, we have:

$$H(S) = -\sum_{I=0}^{2^N-1} P(S_i)\log_2 P(S_i) \qquad (6.6)$$

Where, 'N' is the number of bits to represent a symbol $S_i \in S$ and $P(S_i)$ represents the probability of symbol S_i so that the entropy is expressed in bits. The entropy for a truly random source emitting 2^N symbol is $H(s)=N$. So the entropy should ideally be $H(s)=8$ for a 256 gray level ciphered image. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security cited form Chong Fu et.al (2014).

6.6 Structural Similarity Index Measure

Natural image signals are highly structured. There are strong dependencies between the pixels of natural images, particularly when they are spatially adjacent. These dependencies carry important information about the structure of objects in a visual scene. Structural similarity based quality assessment approaches try to find a more direct way to compare the structure of the reference and the distorted signals. If human vision reacts quickly to structural information based on the HVS characteristics in the viewing field, this approach approximate the perceived image distortion using a measure of structural information change. Structural Similarity Index (SSIM) is an example of this category, Shahriar Akramullahsed et.al(2014).The ideal value of SSIM lies between -1 and 1.

SSIM computes the quality of a distorted image by comparing the correlations in luminance, contrast and structure, locally between the reference and distorted images and averaging these quantities of the complete image. Luminance is the local mean of pixel blocks, contrast is the variance of a pixel blocks, and structure is the pixel –wise correlation between reference block and distorted block.

The common form of metric to compute the structural similarity between two signal vectors x and y is,

$$SSIM(x,y) = [l(x,y)]^{\alpha}[c(x,y)]^{\beta}[s(x,y)]^{\gamma} \qquad (6.7)$$

The term $l(x,y) = \frac{(2\mu_x\mu_y + C_1)}{(\mu_x^2 + \mu_y^2 + C_1)}$ compares the luminance of the signals, $c(x,y) = \frac{(2\sigma_{xy} + C_2)}{(\sigma_x^2 + \sigma_y^2 + C_2)}$ compares the contrast of the signals and $s(x,y) = \frac{(\sigma_{xy} + C_3)}{(\sigma_x\sigma_y + C_3)}$ measures structural correlation of signals. The quantities μ_x, μ_y are the sample means of x and y respectively, σ_x^2, σ_y^2 are the sample variances of x and y respectively, and σ_{xy} is the sample cross – variance between x and y. The constants C_1, C_2, C_3 are the stabilization metrics if the mean and variances becomes small. The parameters $\alpha > 0 \beta > 0, \gamma > 0$ are used to adjust the relative importance of the three components, Sumohana S. Channappayya et.al (2007).
The other form for evaluating SSIM is given as ,

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad (6.8)$$

6.7 Cross Correlation

The most basic requirement of a good block cipher is that the input plain image and cipher image generated should be statistically independent, if not attacks against the cipher are most probable. A cross correlation analysis using images can indicate the degree of statistical independence between plain image and cipher image generated by a cipher. Usually for a good algorithm in the cross correlation plots between original images and ciphered mages, the points spread over the entire x-y plane indicating weak correlation. Whereas, in the cross correlation plots between original images and decrypted images the points are along the diagonal in the x-y plane indicating 100% correlation, Paul.A.J et.al (2012).
Table 2 gives a detailed comparison of the Watermarking and Cryptography techniques under various criterions and methods.

Table 2. Comparison of Watermarking and Cryptography [Abbas et al (2010)]

Criterion/Method	Watermarking	Cryptography
Objective	Copyright preserving	Data protection
Secret data	Watermark	Plain text
Result	Watermarked file	Cipher text
Concern	Robustness	Robustness
Types of attacks	Image processing	Cryptanalysis
Visibility	Visible/invisible	Visible
Fails when	It is removed/replaced	De-ciphered
Relation to the cover image	Related	Not applicable
Flexibility	Cover choice is restricted	Not applicable
Domain	Spatial frequency	Spatial

DOI: 10.30726/esij/v7.i3.2020.73014

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

7. Conclusion

This paper presents a theoretical approach for developing algorithms for secured transmission of medical images over public networks. The focus is on combining Watermarking and Cryptography techniques for developing algorithms to efficiently transact medical images over open channel. The algorithms which combine both the techniques can generate imperceptible watermarked medical image with high level of security. The paper also discusses the standard parameters used for the evaluation of the algorithms constructed by combining both the cryptography and watermarking techniques.

References

[1] Abdelaziz, I.H., A.Basem and A.H., Heba (2013). An Intelligent Watermarking Approach Based Particle Swarm Optimization in Discrete Wavelet Domain, International Journal of Computer Science (IJCSI), Vol.10, No 1, pp330-338.

[2] Abdullah, A.H., R. Enayatifar and M. Lee (2012). A hybrid encryption algorithm and chaotic function model for image encryption,AEU Int. J. Electron Commun., Vol.66, pp. 806-816.

[3] Acharya, U.R., P.S.Bhat, S.Jumar and L.Min (2003). Transmission and storage of medical images with patient information, J.Comp.Biol.Med.Vol.33, pp. 303-310.

[4] Acharya,R., U.C.Niranjan, S.S.Iyengar, N.Kannathal and L.C Min (2004).Simultaneous storage of patient information with medical images in the frequency domain, J. Computer Methods and Programs in Biomedicine.,Vol.76,pp.13-19.

[5] Bouslimi, D., G.Coatrieux and C.Roux (2012). A joint encryption / watermarking algorithm for verifying thereliability of medical images: application to echographic images, J. Comput. Methods Prog. Biomed, Vol.106,pp.47-54.

[6] Cao, H.K., Huang and X.Q. Zhou (2003). Medical image security in a HIPAA mandated PACS environment, J.Comput.Med.Imaging Graphics, Vol. 27, pp. 185-196.

[7] Chao, H.M., C.M. Hsu and S.G. Miaou (2002). A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, IEEE Transactions Information Technology in Biomedicine, Vol. 6,pp. 46-53.

[8] Cheng,S., Q.Wu and K.R.Castleman (2005).Non-ubiquitous digital watermarking for record indexing and integrity protection of medical images, Proc. of ICIP, Vol. 2, pp. 1062-1065.

[9] Coatrieux.G., H.Maitre,B.Sankur,Y.Rolland and R.Collorec (2000).Relevance of watermarking in medical imaging,Proc. of IEEE-EMBS Conference on Information Technology Application in Biomedicine, Arlington,VA, pp. 250-255.

[10] Farina, M., K. Deb and P. Amota (2004).Dynamic mutli-objective optimization problems test cases, approximation and applications, IEEE Transaction Evolutionary Computations, Vol. 8, pp.425-442.

[11] FrankY.Shih and Yi-Ta Wu (2005). Enhancement of image watermark retrieval based on genetic algorithms,Elsevier journal of visual communication and visual representation, Vol.16, pp.115-133.

[12] Fridrich,J., ,M.Goljan and R.Du (2001). Invertible authentication, Proc.SPIE Proc. on Security and Watermarking of Multimedia Contents, San Jose, California, pp.23-26.

[13] Giakoumaki,A., S.Pavlopoulos and D.Koutsouris (2003).A medical image watermarking scheme based on wavelet transform,Proc. 25th Annual Int.Conf. of the IEEE EMBS ,Vol.1, pp 856-859.

[14] Hernandez.J.R., and F. Pérez-González (1999).Statistical analysis of watermarking schemes for copyright protection of images,Proc. IEEE Special Issue Identification and Protection of Multimedia Information, Vol. 87, pp. 1142-1166.

[15] Luo,X., Q.Chenag and J.Tan (2003).A lossless data embedding scheme for medical images in application of e-diagnosis,Proc. 25th Annual Int. Conf. of the IEEE EMBS, Vol.1, pp. 852-855.

[16] Leier,A., C.Richter, W.Banzhaf and H.Rauhe (1997). Cryptography with DNA binary stands, J.of BioSystems, Vol.57,pp.9-22.

[17] Nayak,J., P.S.Bhat, M.S.Kumar and R.Acharya (2004).Reliable transmission and storage of medical images with patient information using error control codes,Proc.of IEEE Indicon, pp. 147-150.

[18] Pareek,N.K.,Vinod Patidar and K.K.Sud (2006).Image encryption using chaotic logistic map, Elsevier Image and Vision Computing, Vol.24, pp.926-934.

[19] Rabil,B.S., R.Sabourin, E.Granger (2010). Intelligent watermarking with multi objective population based incremental learning,IEEE International conference on intelligent information hiding and multimedia signal processing (IIH-MSP), Darmsdt, Germany, pp. 131-134.

[20] Sharp .T (2001).An implementation of key based digital signal steganography,Proc.4th International workshop on Information Hiding ,Vol. 2137, pp.13-26.

[21] Shih,F.Y., and Y.Ta Wu (2005) .Robust watermarking and compression for medical images based on genetic algorithms, Journal of Information sciences ,Vol.175, No. 3, pp. 200-216.

[22] Srinivasan,Y., B.Nutter, S. Mitra, B.Phillips and D.Ferris (2004). Secure transmission of medical record using high capacity steganography,Proc. 17th IEEE symposium on computer based medical systems, pp. 122-212.

[23] Turner, L.F., (1989), Digital Data Security System, Patent IPN, WO 89/08915.

[24] Wei,X., L.Guo , Q.Zhang , J.Zhang and S.Lian (2012).A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, J.System and Software,Vol.85, pp.290-299.

[25] Zhou, X.Q., H.K. Huang and S.L. Lou (2001).Authenticity and integrity of digital mammography images, IEEE Transactions on Medical Imaging, Vol. 20, pp. 784-791.

DOI: **10.30726/esij/v7.i3.2020.73014**