An Approach for Secured Medical Image Data and Information Transmission

Pallavi S. Lunge
Computer Science & Engineering Department, Amravati University [MH] India.

Abstract – This paper presents the work related to the secured medical image transmission based on watermarking and encryption. User specific watermark is embedded into the LSB of original image. Embedding watermark in LSB doesn't affect the quality of image. This watermarked image is then encrypted by using a pixel repositioning algorithm. Each pixel is repositioned based on the remainder obtained after division by number 10. This remainder matrix acts as encryption key and is required at the time of decryption too. Exhaustive experiments are carried out on proposed approach. The results show that the watermark embedded is imperceptible and can be easily extracted at the receiver. Also the encrypted image has no visual significance with the original image and histogram of encrypted image is altered. Encrypted image can be decrypted without any loss of information from the image. From this decrypted image watermark can be extracted which suffers no loss in the watermark. PSNR values for a set of medical images are satisfying.

Index Terms – LSB Watermarking, Pixel Repositioning Algorithm, Byte Rotation Encryption Algorithm (BREA), Encryption, Decryption.

1. INTRODUCTION

This chapter discusses some basic concepts needed to understand the rest of the report. This chapter consists of three sections: First section describes application domain i.e. Medical imaging. Second section describes the concept of security and why we need security of medical data. Third section introduces image encryption and watermarking.

Medical Imaging

Medical Imaging is the Technique and Process of creating visual representations of interiors of a Body, for clinical analysis and medical intervention, as well as visual representation of the functions of some organs or tissues. Medical imaging seeks to reveal internal structures hidden by the skin and bones as well as to diagnose and treat diseases.

Medical Disease Diagnosis is done by three ways:

- Consultation - Information which is obtained from Patients.
- Physical Examination - Inspection, Auscultation, Measurements.
- Medical Tests – Laboratory Analysis, Bio-signal Analysis (ECG), Image Analysis.

Image Analysis means to extract meaningful information from images; mainly from Digital Images. Basically, an Image is a rectangular array of pixels. It has a definite height and a definite width counted in pixels. The height of an image is the number of rows and the width of an image is the number of columns in an array. Thus the pixel array is a matrix of $n*m$ where n indicate number of rows and m indicate number of columns.

A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images. There are three types of digital image which are binary image, color image and gray-scale image.

I. Binary Images: Binary images are digital images that uses only 1-bit to represent each pixel which may either be 1 or 0.

II. Gray-scale images: Gray-scale images use 8-bits to represent each pixel of an image. Gray-scale images are referred to as monochrome images. They contain only gray level information and no color information.

III. Color images: Color image is a digital image that is made up of colored pixels each of which holds three colors corresponding to Red, Green and Blue. Color images are also called as RGB Images.

Image Security

In health care industry, Patients data are shifting from paper records to electronic records. Electronic patient record is a computer based memory that can be assessed over network. Electronic patient record contains all the health care related information of a patient and combines several enterprise-based electronic medical records specific to a patient. Electronic patient records changed the way of storing patients' information. Electronic health care systems enable health providers' to design and implement specific applications that can help doctors for diagnosis and treatment of patients.

Electronic patient records have created opportunities to health care frauds including medical identity theft. Inaccurate medical records may lead to medical mistreatment that will cause

harmful consequences to a patient. Many assume that medical identity theft is no different from financial identity theft but in fact medical identity theft has more devastating effects on patients for there is a lack of recourse for patient to correct the false entries in their medical records. In reality, false medical information can kill a patient.

With the advent of electronic patient records, patients' data can easily be shared among physicians, health care providers, nurses, supporting staff, medical research, and public health care services. Basically, most health care information including patients' data is not generated solely within a physician/patient relationship, but is generated from the diverse sources, such as non-physician specialist, nurse practitioners, public health officers, laboratories, and other ancillary health care professions. The sharing as well as distribution of patient information enables productive medical research, proper treatment of patients and improvement in health care quality.

On the other hand, patient records pose a challenge to maintain information confidentiality, integrity, and availability – the computerized record infers that the requester has the same hardware and software communication protocol and thus enables easy access to data. This may open doors to the unauthorized parties who may unscrupulously steal patients' data for personal benefits, alter patients' records, and expose patients' medical history. The high accessibility of patients' data has made it easier for perpetrators to invade patients' information confidentiality, integrity, and availability and commit health care fraud.

Need of data transmission through the network has led to the need of greater security to protect information against different attacks. Many techniques are used to provide security to information in transmission such as Image Encryption, Digital Watermarking, Fingerprinting, Cryptography, Digital Signature and Steganography etc.

Image Encryption

Image encryption is a process of transforming image into either an image which is unintelligible or into a data of other format having no reference to the original image. The input image to an encryption algorithm is generally referred as a plain-image and the output encrypted image is referred as a cipher-image. The encryption is a reversible process in which the encrypted image can be decrypted to recover the original image. This can be done only by the people having knowledge of the algorithm and the key used in algorithm to encrypt the image.

Encryption can be done using either a public key of the user or a secret key of user, and based on the key type it is classified as

- Public Key encryption: where the encryption is done using the public key of sender and the decryption is done using the secret key of the receiver.
- Private Key encryption: where the encryption is done using the private key of sender and the decryption is done using the combination of secret key of the sender and the public key of receiver.

Image encryption can be used to protect images at rest, such as images stored on computers or storage devices which are being exposed through loss or theft of laptops. Image encryption as rest helps protect them from being uncovered and shared.

In order to facilitate secret communication, image encryption has found significant place highly sensitive areas such as military surveillance, satellite information systems, health-care, confidential video conferencing etc. Some of the algorithms use traditional text based encryption schemes to encrypt images directly, but it is not a feasible idea due to difference in size of text and image, and hence consumes more amount of time.

Encryption of image can be either a visual encryption wherein the encrypted image will be a result of a shuffling mechanism applied on the original image which changes all or a major number of pixel positions in the original image or it might be a transformation based scheme where the image pixels values will be altered in a way to form a new image with totally different set of pixel values. In the first scheme, changing the positions of pixels encrypts the image only visually but the properties of image remain same for example size, resolution, histogram etc., on the other hand, in second approach changing the intensity values implies the change in histogram by which the identity of the image is masked. The encryption algorithms can take inputs either in block mode or in stream of data bits. Depending on the type of input they can also be classified as block cipher and stream cipher.

Image Watermarking

Digital image watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended, by its developers, as the solution to the need to provide ownership protection to the image.

Image watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into an image such that watermark can be detected or extracted at receiver side to make an assertion about the image. A simple example of digital watermark would be a visible "seal" placed over an image to identify the copyright of the image. However the watermark might contain additional information including the identity of the owner or purchaser of a particular copy of the image.

Image watermarks can be divided in 2 types based on the visibility of the watermark in the watermarked image.

- Visible watermark: A process where the watermark is embedded in the original image in a way that the watermark is visible to naked eyes. The resulted image, here, is the original image with visibly "stamped" watermark on it.
- Invisible watermark: A process where the watermark is embedded in a way that it is perceptually invisible to human visual system and can be detected only using the scheme used for embedding it. The resulted image has no visual differences with the original image.

Visible watermarks are generally used in applications where only the ownership proof needs to be added to prove the source of image such as photography magazines where image visual quality degradation is tolerable, on the other hand, the invisible watermarks are used in highly sensitive applications such as military applications, medical applications, secret services, etc., where the contents of the image are highly important and no degradation of the image quality is expected.

Depending on the level of security the watermark can be embedded in two different domains of the image viz.

- Spatial domain: Gives the position map of pixels in the image.
- Frequency domain: Gives the intensity values of pixels in the image.

Generally spatial domain watermarking is used when only the ownership details of the image need to be sent at low security level, on the other hand frequency domain watermarking is used in applications where tamper detection is important at receiver and also the images are subjected to high risks of attacks in transmission.

The key characteristics are as given below:

- Difficult to notice: The invisible watermark should not be noticeable to the viewers nor should the watermark degrade the quality of the content of image.
- Robustness: Watermarked image should be robust to attacks mainly transformations and lossy compressions and others like scaling, cropping, rotating etc.
- Tamper resistance: Watermark should be resistant to tampering intended to remove the watermark and recover original image, any such attempts should be reflected from the recovered watermark.
- Minimum alteration of pixels: It must not alter a large number of pixels in order to preserve an acceptable visual quality.

Encryption and Watermarking

Image encryption provides high degree of security but the certificate of originality cannot be achieved from the encryption only. Encrypted image is secured until it is in the encrypted form but after decryption it can be attacked either to form new image or to manipulate the content of image. Using watermarking jointly with encryption can resolve this issue. The concept of encryption and watermarking means to combine encryption and watermarking with each other either in a single stage or at two different stages. We could first watermark the image and then encrypt it, or first encrypt the image and then watermark the encrypted image. Depending on the methods used the original image can be decrypted at receiver and watermark is extracted. Both the decryption and extraction can be applied independently at receiver or need to be performed in sequence defined by the applied scheme.

Steganography

Steganography is the art of hiding messages inside unsuspicious medium. The purpose of steganography is to hide the existence of a message from a third party. Cryptography is widely used with steganography. Steganography works in two stages, embedding then extracting. During the embedding stage, a key is used to embed a message in a cover medium resulting in a stego-object. The stego-object is then transmitted along public channels to its destination. When the stego-object is received, the embedded message is extracted from stego-object using the known stego-key. Steganalysis is the art of discovering and rendering such covert message. Its goal is to avoid drawing suspicion to the transmission of a hidden message. Steganalysis contains two main issues: Detection and Distortion. Drawback of Steganography is if the key is known then the data can be retrieved easily. Therefore no security is provided for the encrypted image. The encrypted image can be secured by combining these steganography with visual cryptography and digital watermarking.

2. RELATED WORK

Number of researchers has proposed a numerous encryption techniques having different features of each for secure image encryption purpose. This chapter describes the analysis of some of the available literature related to image encryption and watermarking.

Techniques used for Image Encryption

AES encryption algorithm is public, which brings many problems for its security. So to solve the safety problems of AES encryption algorithm, Yang et al. 2015 [1] proposed an approach which improves AES encryption algorithm by means of using chaos theory. Results show that the feasibility and correctness of the approach are good enough. Patel and Ragha 2015 [2] have presented a steganography methodology that uses concepts of image processing and wavelet transform

techniques. This process provides a method for hiding secret binary data within a cover image without increasing the size or dynamic range of the image by means of combining cryptography and steganography. Steganography when combined with encryption provides a secured means of secret communication between two parties. Image is encrypted by using a scrambling algorithm. Higher PSNR is achieved. Jyoti and Neginal 2015 [3] introduced new secure image transmission technique which creates a meaningful mosaic image and also transforms the secret image into a secret-fragment-visible mosaic image of the same size and has the same visual appearance as the target image. Selection of target image is flexible and doesn't require any database creation. Original secret image can be extracted nearly complete from the received image. Tasneem and Bhavni 2014 [4] used cryptography and steganography methods together to increase the security of the data while transmitting through networks. Proposed approach uses text data as watermark. Before embedding text into the image it is encrypted by using AES algorithm with key of size of length 8. The encrypted text is embedded into image using Discrete Wavelet Transform (DWT) method and the resultant image is transmitted to the receiver. Watermark embedded is reversible and data can be decrypted at receiver. Saraf et al. 2014 [5] proposed an approach to combine of C code, Code Composer Studio and DSP processor for text encryption. Text encryption uses 128 bit size of key as well as plaintext.16 strings of size 8 are formed for encryption. AES encryption algorithm in CFB mode with PKCS5 Padding method is used here for image encryption. Maitri et al. 2014 [6] have introduced Byte Rotation Algorithm for file encryption and decryption with minim delay. This algorithm improves the security and reduces time for file encryption and decryption. Results of Byte Rotation Algorithm are comparable with those achieved from AES encryption algorithm. To improve file security random key generation of 128bit is used. Khandelwal and Sahu 2014 [7] proposed a narrative image steganography technique to hide both image and key in color cover image using Discrete Wavelet Transform (DWT) and hereditarily direct clustering based on Fuzzy C-Means Clustering. Results show that there is no visual similarity between stego-image and original image and the information can be retrieved completely. Singh and Singh 2013 [8] presented concept which uses 64-bits Blowfish Algorithm, which is designed to increase security and to improve performance. Algorithm is used with variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. Higher number of rounds makes the approach more secure. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm. Banu and Velayutham 2013 [9] have analyzed AES Encryption algorithm to provide sufficient levels of security for protecting the confidentiality of the data. A sleep scheduling method is explored to reduce the delay of alarm broadcasting from any sensor node in WSNs. Specifically, here two determined traffic paths are used for the transmission of alarm message along with level-by-level offset based wake-up pattern. On a critical event an alarm is quickly transmitted along one of the traffic paths to a center node, and then it is immediately broadcast by the center node along another path without collision. Nurhayati and Ahmad 2013 [10] carried out research to design an application of steganography using Least Significant Bit in which the message is encrypted using the Advanced Encryption Standard algorithm (AES). The result of research shows the steganography is expected to hide the secret message, so the message is not easy to know other people who are not eligible. Tang et al. 2009 [11] came with a new image encryption and steganography scheme. First, the secret message is encrypted through the combination of a new gray value substitution operation and position permutation which makes the encryption system strong. And then the processed secret message is hidden in the cover image to fulfill steganography. Experimental results show that the scheme proposed in this paper has a high security level and better image stego-image quality.

Rad and Hosseini 2008 [12] proposed Grid-Based Hyper Encryption application that uses the computational resources of multiple desktop PCs in order to encrypt/decrypt large data files with one of the most efficient and secure encryption algorithms, the advanced encryption standard. Simplicity of use and high performance of GBHE makes it an ideal choice for deploying in any organization that needs this functionality.

Techniques used for Medical Image Watermarking

Balamurugan and Senthil 2016 [13] combined three different research domains namely fingerprint biometric, cryptosystem and reversible watermarking. Proposed system uses the finger print biometric for authentication, symmetric as well as public key for cryptography process for confidential data and reversible watermarking for integrity. To provide CIA methodology for the MDBMS, conformation SMS is sent to the patient for the convenient, that their information had reached safely to the corresponding destination. Nemade and Kelkar 2016 [14] proposed a reversible watermarking technique for colored medical images using Histogram shifting method the colored images is converted to YUV image and watermark is embedded in the Luminance (Y) component. Histogram shift method is also evaluated by applying the Technique on RGB components. Kaur and Madanlal 2015 [15] proposed a blind image-watermarking algorithm which based on both the Modified Fast Haar Wavelet Transform and the Redundant Second Generation Wavelet Packet Transform. The idea behind the proposed algorithm is to decompose the cover image using Modified Fast Haar Wavelet Transform and Redundant Second Generation Wavelet Packet Transform according to the size of the watermark. The watermark is

embedded in the fine-scale bands of the Redundant Second Generation Wavelet Packet Transform of the fine-scale bands of the last Modified Fast Haar Wavelet Transform decomposition level of the host image. Paul and Sunitha 2015 [16] proposed a new method for increasing the capacity and privacy of watermarking based on circular histogram modulation by taking the host system as color image. By increasing the capacity it can be beneficial for secure transmission of huge databases like hospital records through the network. Anandkumar and Mukeshgupta 2015 [17] developed two algorithms for embedding and extraction process. The original image is first DWT-decomposed, and then the colour watermark is implanted. Watermark embedding is applied in different frequency bands of the image and PSNR and NC plots are drawn for all the frequency bands. Bolandt and Kuannitlh 1995 [18] proposed watermarking scheme based on block DCT WT and FFT based algorithm. The approach watermarks are designed to be invisible even to a careful observer but contain sufficient information to uniquely identify both the origin and intended recipient of an image with a very low probability of error. The further development of robust error correction codes and digital signature techniques is to be done. Another approach of watermarking is proposed by Chang and Lu (2008) [19] which is based on embedding watermark into gray-level images according to pixel correlation between them. The author claims the approach to be lossless in terms of quality of de-watermarked image. Approach is capable of hiding large amount of information and can restore the original image without any loss, and this is shown by results. Also it has been claimed that the scheme outperforms RS-embedding scheme and Tian's scheme and hence can practically be applied. Shukla 2005 [20] proposed real time copyright protection algorithm using both visible as well as invisible watermarking schemes and also implementation of real time image processing techniques on Android and Embedded Platform. The concept is based on DCT and OpenCV. Images captured from the Smart-phone camera are efficiently watermarked using this system. The authors claim that DCT provides an efficient methodology for implementing invisible watermarking process. Visible watermarking involves embedding text watermark which is resilient to common image processing operations. Mathon et al. 2014 [21] used distortion optimization for secure spread spectrum watermarking for grayscale images. This approach of distortion minimization is based on elements of transportation theory and hence claims to achieve strong security properties and is called as Transportation Natural Watermarking. Here, the multi-resolution image is decomposed and combined with a multiplicative embedding at distribution level. Embedding distortion and its visual impact on image can be reduced using the proposed approach and this can be seen in results. Peng 2011 [22] proposed a block-based singular value decomposition of the image and the discrete network method to embed and extract watermark to and from the digital image. It has solved singular value decomposition problem of poor robustness. The concept is based on the neural network and singular value decomposition. The author claims well extraction throughout the common image processing and compressing operations. Kamran and Farooq 2012 [23] proposed an approach of watermarking providing good quality of image after watermark extraction. Author used feature extraction and ranking to watermark images. The use of feature ranking contributes to preservation of information contained within the image. To create and embed watermark to original image, Particle Swarm Optimization Algorithm is used. The proposed scheme is claimed to be resilient to a variety of attacks and is confirmed by results shown Kishor and Vankat 2014 [24] proposed a RSA-DWT based medical image watermarking. Public key encryption of watermark is done before embedding watermark into the image. This encrypted watermark is then embedded into the image using DWT. Results show satisfactory values of PSNR and no visibility of watermark. Dragoi, and Coltuc 2014 [25] proposed a watermarking scheme which is based on local prediction to achieve difference expansion reversible watermarking. Here, a least square predictor is computed for each pixel on a square block, centered on the pixel and the prediction error corresponding to that pixel is expanded. This prediction error is then recovered at receiver without any additional information. Prediction context depends on the size of blocks used in expansion. Appropriate block sizes for each context are determined and are given in results. Results obtained by Rhombus context are best among all the other contexts. Su et al. 2013 [26] introduces an approach of using Scale Invariant Feature Transform and extended pilot signals for watermarking. This approach addresses the problem of synchronization in watermark detection at receiver. The watermarking signal is embedded in the invariant regions which are formed by applying interest point extraction as scale-invariant feature transform. Square grids are used to embed signal. This approach achieves right balance between efficiency of signal detection and robustness of watermark. Embedded signal are guided by pilot signal contributing towards synchronization in detection. At detection when the same interest point is extracted, the related affine parameters of grids are adjusted to detect hidden pilot signal achieving synchronization and successful retrieval of watermark and original image. Panyavaraporn 2013 [27] came up with an approach of using wavelet transform to watermark QR code images. The binary watermark is embedded into a selected sub-band which can be either of LH, HL or HH sub-bands. The results show that the scheme can withstand basic attacks acceptably but is not robust against attacks such as strong noise, high compression geometric transformation and occlusion and hence limits the performance of the scheme. Abdallah et al. 2011 [28] introduced wavelet based watermarking which doesn't require original image or any pilot image to reconstruct watermark at decoder. The watermark is embedded into the

coarsest scale wavelet coefficient. Decomposition upto level 3 and watermark of size equal to sub-band is used. Scheme uses quantization of wavelet coefficients in binary manner. Unlike traditional wavelet based methods, this method has less degradation. Lin and Wu 2011 [29] proposed an approach to watermark 3D images. Here multiple watermarking is used to solve content protection problem of Depth Image Based Rendering (DIBR) 3D images. A 3D image comprises of 3 images in itself viz. left-eye image, right-eye image and a center image.

The center image and depth image generated by content provider is called as (DIBR) 3D image. Both the, mutual orthogonality and order of embedding plays important role watermarking 3D images. The advantage of the approach is that it does not need original data and depth image during watermark detection. Results show that the approach is secure to compression and noise attacks and also doesn't get affected by range variations and baseline distance adjustment up to certain degree. Zhang et al. 2011 [30] carried out research for watermarking on Perceptual Quality Metric based on second-order statistics.

Exploiting the perceptual distortion with human perception is key for robust watermarking scheme. The proposed scheme of SOS performs better than some state-of-the-art metrics and correlates with several databases of images by means of texture masking effect and contrast sensitivity in Karhunen-Loeve transform domain. Use of simple metric ensures fat implementation and results show that the robustness is improved. Author also proposes involvement of third party metrics to rate the quality of watermarked image. Tang and Hang 2003 [31] proposed use of Mexican Hat wavelet scale interaction method based on feature points embedding and extraction as watermarks.

This is achieved using image normalization which is applied to non-overlapped images separately. A sequence of 16-bit signals is embedded in original image improving robustness of watermarking. Reference image is not required at detector to extract watermark. The synchronization problem is overcome by using visual point on image and invariance points reduce the watermark search space. Guerrini et al. 2011 [32] proposed a technique to watermark High Dynamic Range (HDR) images having high luminance values. The HDR images are tone mapped using TM algorithm and then watermarked using Quantization Index Modulation (QIM). Watermarking system developed for LDR images is used here in LogLuv domain. The detection of watermark depends on the TM algorithm. Disadvantage is that the scheme is not fully blind and selection of blocks to embed data is not possible.

Techniques used for Image Security

Sundari et al. 2015 [33] came up with three technique watermarking, steganography and cryptography to provide high level of security. First the cover image is be compressed using JPEG compression algorithm, Then the message to be sent is encrypted using RSA encryption algorithm and later the encrypted message bits and the bits of watermark are embedded into cover image. Patel and Patel 2015 [34] proposed combined strategy of cryptography, steganography and digital watermarking to hide secure image with watermark logo inside cover image. For this purpose they used DCT, DWT, SVD and RSA approach. Using DCT, encrypted watermark logo (encryption performed using RSA) is hid inside secure image resulting in Stego image. Gayathri and Nagarajan 2015 [35] introduced approach with information hiding in image using Zig-Zag scanning pattern which is more complex algorithm in Steganography again encrypted as shares

The share is embedded into the host image using Least Significant Bit Insertion Technique (LSB). The scheme provides more secure and meaningful secret shares that are robust against a number of attacks. Kishor et al. 2014 [36] proposed RSA-DWT based medical image watermarking like MRI. Watermark image is encrypted with key generated RSA algorithm. Encrypted patient image is used as payload which is embedded into Medical image in Wavelet domain. Experimental Result shows that RSA-DWT demonstrates superior protection on unsecured network.Suganya et al. 2013 [37] proposed a new joint watermarking and encryption system which guarantees a priori and a posteriori protection of medical images. It merges the stream cipher algorithm or block cipher algorithm with the QIM based watermarking technique. The proposed method uses two encryption algorithm namely RC4, AES are Stream cipher, Block cipher algorithm respectively. The system gives access to insert two messages in the spatial domain and encrypted domain respectively during encryption process. These two messages are used to verify the reliability of images in decryption part. Li and Bai 2012 [38] developed an algorithm with digital watermarking scheme which uses a part of sign sequence of DCT coefficients as a feature of vector images, at same time watermark is encrypted by logistic map to enhance confidentiality.

3. PORPOSED MODELLING

This chapter gives the description about the approach we have proposed. It consists of the steps involved in proposed approach and the flow of the approach along with data flow in the system. Flow diagrams for the approach are also recorded here.

Evolution in the internet, today, has simplified information sharing over the wider area. Both the visual and textual information of a patient can easily be transmitted all across the world. But the ease of information exchange has introduced security issues for the information being transmitted over the internet, as the information can easily be stolen and illegally modified at any stage without having any identity of the person.

Images being shared over the internet can be protected by using some security measures like encryption and watermarking.

Work proposed here focuses on the aim to provide security to images being shared over the internet. The approach uses watermarking and encryption both to provide authentication data and visual security to medical images. Watermark embedding is done using LSB substitution and encryption of watermarked image and patients' data is encrypted using scrambling method. The approach is as discussed below.

The proposed work can be divided into four phases as follow:

I. Embedding watermark in the original image.

II. Encryption of Watermarked image.

III. Encryption of patients' information.

IV. Decryption of patients' image and extraction of watermark.

V. Decryption of patients' information.

In first phase the watermark is embedded into original image to form a watermarked image. Both the original image and watermark are used in the image format. Data from other format except image cannot be embedded in the original image.

In second phase, watermarked image in encrypted using a shuffling algorithm discussed later. An encryption is also generated in this same phase which is used for decryption also.

Then in third phase the information of patient is encrypted using Byte Replacement Encryption Algorithm (BREA). All characters from the patients information chart are converted encrypted using a key formed using random distribution of numbers.

Finally at the receiver, received encrypted watermarked image is decrypted using the same keys used for encryption first and the original watermark is extracted from the decrypted image. Extracted watermark can be used to detect the authenticity and originality of image.

Embedding Watermark

Watermarking is the process of hiding a secret image or message into the original image in order to provide authenticity to the image. Message image can be embedded in the original image using pixel substitution method wherein one of the bit planes of the original image is replaced using the message image.

Pixels in the image have 8-bit value representing their color intensity. If the Least Significant Bit (LSB) of these 8-bits is altered the total value of the pixel will change only by 1. For example, changing LSB of pixel with value 128 from 1 to 0 will change the value to 129 and visually an human eye cannot distinguish such a small difference.

Watermark, in the proposed approach is of binary form and is embedded by means of replacing the LSBs of the original image. First the original LSB plane of the image is made 0, then the binary watermark is added to this LSB plane.

LSB watermarking is one of the easiest methods used to watermark images. It is because of the low complexity and high recovery efficiency of the watermark. Watermark can always be recovered without any loss from a safe image.

Encryption of Watermarked image

Watermarked image from phase one is encrypted in this second phase. Aim of encrypting image is to secure image against stealth and manipulation attacks. This is because even a slight manipulation in the patients' medical image can cause him his life. Encryption is the process of translating image into unintelligible information represented in either image form or a text form.

Approach proposed in this work uses decomposition of pixel values in order to shuffle their positions. Encryption process, proposed here, shuffles all the pixels in the original image and also changes their original pixel intensity values in order to alter the histogram of the final encrypted image.

Encryption algorithm can be divided into several stages. To reposition a pixel remainder of the division of original value by 10 is used. Not the actual value but the quotient of division is placed at the position specified by the remainder.

Step 1: In first step original pixel value is divided by 10 and both remainder and quotient are recorded in matrices Q and R respectively.

Step 2: A new matrix with same number of rows as that of original image and with columns 10 times as that of the original image is formed, such that all the elements take random numeric values from 0 to 255.

Step 3: First element in the Q is placed at position represented by first element of R, in new matrix. Second element from Q is placed at the position represented by second element+10 of R.

Step 4: Perform step 3 for all elements in first row of Q.

Step 5: Repeat step 4 for all columns of Q.

Step 6: Finally convert all the elements from encrypted matrix into their ASCII forms to achieve a text file with encrypted image data.

Elements of this text file are then mapped in the range of 0 to 255 by means of using their respective ASCII codes to get the final encrypted image

Here, the matrix with remainder values i.e. R acts as a key for encryption and is required to decrypt the encrypted image. Figure shows the image encryption process in detail

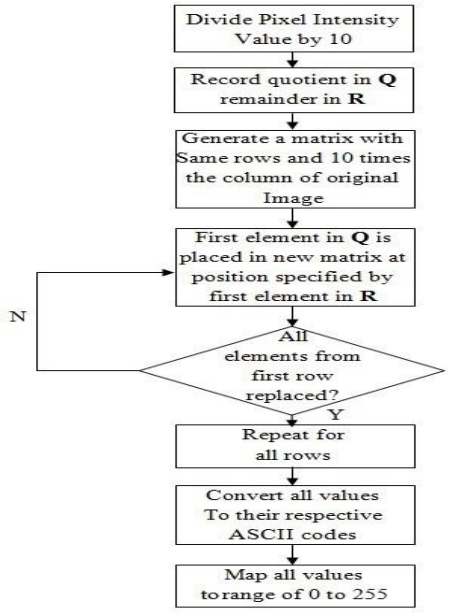


Figure 1: Encryption of watermarked image flow diagram

Encryption of Patients' Information

Patient data is input in the form of text. This text data is encrypted using Byte Replacement Algorithm. BREA algorithm encrypts text data sampled in blocks and each block is then encrypted in parallel manner. A key is generated for encryption which is further used for decryption also.

BREA samples input data into strings of size 16 characters. Each such string is then reshaped into a matrix of size 4*4. All the elements are then replaced by their equivalent ASCII codes. Another matrix, a key matrix, is generated by means of randomly selecting all elements uniquely from 1 to 26.

Elements of key matrix are then scaled by means of taking mod by 2. This key matrix is then added with each block element by element. Then, first element of first row is rotated at the end of row by shifting all elements to left. First two elements of second row are rotated by shifting other elements towards left and finally first three elements of third row are rotated at the end. Fourth row is kept unchanged.

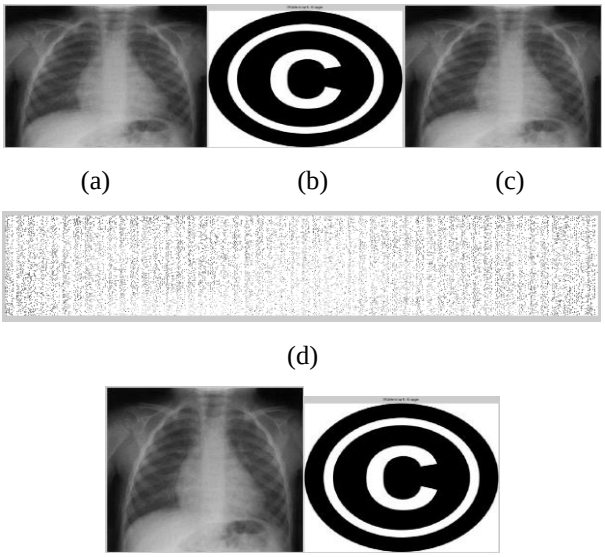
Similarly, first element of first column is rotated at the end by shifting other elements towards up. First two elements of second column are rotated at the end and finally first three elements from third column are rotated towards down side. Fourth column is kept unchanged.

4. RESULTS AND DISCUSSIONS

Following are the snapshots of the results for the proposed approach. Figure1 represents the actual textual data entered by the patient or a representative, encrypted data achieved from the Byte Replacement Encryption Algorithm and the decrypted information obtained using reverse BREA.

Figure 2: Original, encrypted and decrypted textual information

From the figure 2, the information entered was "Abc Def Xyz 123 789", a mixed string of uppercase letters, lower case letters, blank spaces and numbers. Encrypted string achieved is g "2bX2c z4!Dz!Be 8 9 8". It can be clearly seen that encrypted doesn't resemble with the original text directly and is very hard to understand. It also doesn't have any standard meaning.



(a) (b) (c)

(d)

(e) (f)

Figure3: (a) through (f): Original X-Ray image, watermark image, watermarked image, encrypted image, decrypted image and extracted watermark

Figure3 shows the result of complete process of encryption and watermarking on image along with decryption and extraction results. It can be seen from figure (c), (d) and (e) that watermen image can be encrypted without leaving any perceptual relation with original image. Also the increased size introduces larger number of possibilities for false pixel repositioning reducing the attack possibility and the same encrypted image can be decrypted without any loss.

Again because of the entirely changed pixel values histogram of original image doesn't co relate with encrypted image.

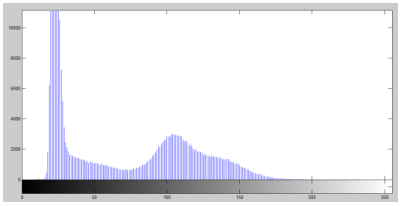
PSNR Analysis

Higher PSNR values are desired for better results. Table shows values of PSNR for Rib Cage Image when undergone Salt 'n' Pepper attack.

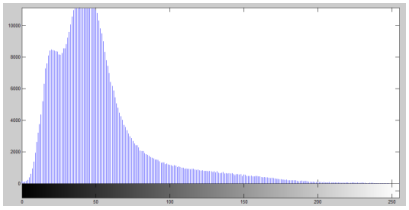
Table: PSNR Analysis of Images

Image	PSNR
USG Image	33.5732
X-Ray Image	33.5716
Brain Image	34.5979
MRI Image	33.6976
Kidney Image	34.6006

It can be noted from the Table that for all the images higher PSNR values are achieved.



(a)



(b)

Figure4: (a) and (b) Histogram of original Sonography image and histogram of encrypted Sonography image

It can be clearly noted from figure4 that encryption not only makes the image imperceptible but also changes the histogram which reduces the chances of histogram attacks, or attempts of regenerating image from histogram.

5. CONCLUSION

In proposed scheme watermarking of image is done prior to encryption. Because of prior watermarking the encryption is given more focus in the approach. We have used LSB watermarking technique, an easy to implement and effective, for embedding the watermark into the cover image. And for encrypting the image we have a repositioning algorithm which shuffles the pixels based on the result of a division.

It is then understood from the results that the proposed approach has succeeded to watermark and encrypt image and the retrieval of image and watermark is also possible without any loss. A noteworthy point is that the decrypted image maintains high visual quality. Also the extracted watermark is comparable to the original one embedded and thus can be used for authentication and copyright protection.

REFERENCES

[1] Zi-Heng Yang, Ao-Han Li, Ling-Ling Yu, Shi-Jun Kang, Meng-Jiang Han, Qun Ding, "An Improved AES Encryption Algorithm Based on Chaos Theory inWireless Communication Networks" 2015 Third International Conference on Robot, Vision and Signal Processing

[2] Krupi Patel, Dr. LeenaRagha, "Binary Image Steganography in Wavelet Domain" 2015 International Conference on Industrial Instrumentation and Control (ICIC)

[3] Jyoti R H, Prof JyotiNeginal, " A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Image" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015

[4] Syeda Farhana Tasneem, S DurgaBhvni,"Secure Data Transmission Using Cryptography And Steganography" International Journal of Emerging Trends in Electrical and Electronics, Vol. 10, Issue. 9, Oct. 2014

[5] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014

[6] Punam V. Maitri, Rekha V. Sarawade, Sarika T. Deokate, Mayuri P. Patil. "Secure File Transmission using Byte Rotation Algorithm in Netwok Security" International Conference for Convergence of Technology – 2014

[7] Poorva Khandelwal, Barkha Sahu. "Novel Technique Data- Hiding Scheme for Digital Image" 2014 IEEE

[8] Pia Singh, Prof. Karamjeet Singh "Image Encryption And Decryption Using Blowfish Algorithm In MATLAB" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013

[9] A. Jesima Banu, R. Velayutham "Secure Communication In Wireless Sensor Networks Using AES Algorithm With Delay Efficient Sleep Scheduling" 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[10] Nurhayati, Syukri Sayyid Ahmad. "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm"

[11] Hongmei Tang, Gaochan Jin, Cuixia Wu, Peijiao, "A New Image Encryption and Steganography Scheme" 2009 International Conference on Computer and Communications Security

[12] NimaBehnood Rad, Hamed Shah-Hosseini. "GBHE: Grid-Based Cryptography with AES Algorithm" 2008 International Conference on Computer and Electrical Engineering.

[13] Balamurugan. G, Senthil. M "A Fingerprint Based Reversible Watermarking System For The Security of Medical Information" 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16)

[14] Hitesh Nemade, Vishakha Kelkar "Reversible Watermarking for colored Medical Image using Histrogram Shifting Method" 2016 International conference on computing for sustaintable global development.

[15] Sukhpal Kaur, Madanlal "An Invisible Watermarking Scheme Based on Modified Fast Haar Wavelet Transform and RSGWPT" IEEE 2015.

[16] Anju Paul, Sunitha E V "Distortion less Watermarking of RelationalDatabases Based on Circular Histogram Modulation" 2015 International Conference on Circuit, Power and Computing Technologies.

[17] Anandkumar, Mukeshgupta "Semi visible Watermarking Scheme Based onDWT and PCA" IEEE 2015.

[18] F.bl. Bolandt, J.J. Kuannitlh "Watermarking Digital Images for Copyright Protection" Image Processing and Its Applications, 4-6 July 2007
[19] Chin-Chen Chang and Tzu- Chuen Lu" Noise Features for image tampering detection and steganalysis" 2007 IEEE.
[20] Ronak Jayesh Shukla" Platform Independent Real Time Copyright Protection Embedding and Extraction Algorithms on Android and Embedded Framework" 2014 IEEE
[21] Benjamin Mathon et al."A Parametric Solution for Optimal Overlapped Block Motion Compensation" 2011 IEEE
[22] JianxiPeng "The research on digital watermarking algorithm Based on neural networks and singular value decomposition" 2011 IEEE
[23] M. Kamran and Muddassar Farooq" A New Spatial Decomposition Scheme For Image Content- Based Watermarking" 2009 IEEE
[24] P. P. Kishor N. Yankat "Medical image watermarking using RSAencryption in Wavelet Domain" 2014 IEEE.
[25] Ioan-Catalin Dragoi, and Dinu Coltuc" Local-Prediction-Based Difference Expansion Reversible Watermarking," Image Processing, IEEE Transactions,2014
[26] Po-Chyi Su et al."Ching-Yu Wu, "Geometrically Resilient Digital Image Watermarking By Using Interest Point Extraction and Extended Pilot Signals," Information Forensics and Security, IEEE Transactions on, Dec. 2013.
[27] Jantana Panyavaraporn "QR code watermarking algorithm based on wavelet Symposium transform," Communications and Information Technologies (ISCIT), 2013 13thSept. 2013.
[28] Hanna A. Abdallah, Mohiy M. Hadhoud, Abdallahameed," Blind Wavelet Based Image Watermarking", International Journal of Signal Processing, Image Processing and Patter Recognition VolNo. 1, March 2011.
[29] Yu-Hsun Lin and Ja-Ling Wu" A Digital Blind Watermarking for Depth-Image-Based Rendering 3D Images," Broadcasting, IEEE Transactions on ,June2011
[30] Fan Zhang et al" "Spread Spectrum Image Watermarking Based on Perceptual Quality Metric," Image Processing, IEEE Transactions on, Nov. 2011.
[31] Chih-Wei Tang and Hsueh-Ming Hang "A feature-based robust digital image watermarking scheme", Signal Processing, IEEE Transactions on, Apr 2003
[32] Fabrizio Guerrini.; Okuda, M.; Adami, N.; Leonardi, R., "High Dynamic Range Image Watermarking Robust Against Tone-Mapping Operators," Information Forensics and Security, IEEE Transactions on , June 2011
[33] M Sundari, P B Revathi, and S Sumesh. "Secure Communication using Digital Watermarking with Encrypted Text hidden into an Image" 2015 IEEE
[34] Palak Patel, Yask Patel "Secure and authentic DCT image steganography through DWT – SVD based Digital watermarking with RSA encryption" 2015 Fifth International Conference on Communication Systems and Network Technologies.
[35] R. Gayathri, Dr. V. Nagarajan "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme" IEEE ICCSP 2015 conference.
[36] P.V Kishor, N Venkatraman, Sarvya, S Reddy "Medical Image Watermarking Using RSA Encryption In Wavelet Domain" 2014 IEEE.
[37] Suganya G, Amudha K "Medical Image Integrity Control Using Joint Encryption And Watermarking Techniques" 2013 IEEE.
[38] Dong, Li, Huang, Bai "Medical Image Watermarking Algorithm With Encryption By DCT and Logistic" 2012 IEEE.
[39] Tarek FARAH, Houcemeddine Hermassi, Rhoouma Rhoouma and Safya Belghith "Watermarking and Encryption Scheme to Secure Multimedia Information" 2012 IEEE.
[40] Muhammad Imran Khan*, Varun Jeoti, Aamir Saeed Malik, Muhammad Farhan Khan "A Joint Watermarking and Encryption scheme for DCT Based Codecs" 2011 17th Asia-Pacific Conference on Communications (APCC)
[41] D. Bouslimi, G. Coatrieux, Ch. Roux "A Joint Watermarking/Encryption Algorithm for Verifying Medical Image Integrity and authenticity in Both Encrypted and Spatial Domains" 2011 IEEE