PROTECTION FOR IMAGES TRANSMISSION

1. Karimella Vikram
   Head of the Dept. of CSE
   Medak College of Engineering & Technology
   Siddipet, Kondapaka, Medak, (RR)
   Email Id: Vikramkarimella@yahoo.com

2. Dr. V. Murali Krishna
   Prof. & Principal
   Murthy Institute of Technology & Science
   AnkiReddy pally, Kesara, Hyderabad
   Email: Vmkrishna99@yahoo.com

3. Dr. Shaik Abdul Muzeer
   Professor & Director of PG studies
   Siddhartha Institute of Engineering & Technology
   Ibrahimpatnam, R.R., Dist.
   e-mail: bdl_muzeer @ yahoo.co.in

4. Mr. K. Narasimha
   Assoc.Professor & HOD of E.C.E.
   Murthty Institute of technology
   AnkiReddy pally, Kesara, Hyderabad
   Email: nrsimha_9@yahoo.com

ABSTRACT
Medical image security is the most important issue during its transmission. Watermarking, digital fingerprint/signature, encryption, time of coding and encoding are the existing techniques for protecting images. But, all this methods have some drawbacks. Lossless or reversible data embedding – is relatively new development, where both image and the message (embedded data) can be recovered in a lossless fashion and to verify the integrity and authenticity of DICOM images. Hash value of the whole image and
patient information is embedded in the least significant bits of the RONI. If the image has not been altered, the watermark will be extracted and the original image will be recovered. Hash value of the recovered image will be compared with the extracted watermark for authentication. The paper outlines that the present methods, previous work, need for security and requirements for new system and presents an approach to further research for lossless medical image security. 

**Keywords:** Medical image security, lossless compression, image authenticity and integrity, Information Hiding, DICOM.

**Keywords:** China insurance industry, Foreign fund, Challenge

**I. INTRODUCTION**

Medical image sharing is used in a wide variety of applications ranging from telediagnosis to telesurgery, and it also promotes applications such as remote diagnosis aid and e-learning. Today all business, government, organizations are connected through internet but it is both fascinating & complex because of the requirements for security services. Mechanisms to meet those services are quite complex. So the network security is the most important. Security is the protection from attack [1]. Data embedding is the most commonly used mechanism for medical images. It is usual that a medical image is diagnosed before storing the image in the long-term storage, so the significant part of the image is already determined [2]. The significant part is called ROI (Region of Interest). The Health Insurance Portability and Accountability Act (HIPAA) [3] require that medical providers and insurance companies implement procedures and policies to protect patient’s medical information. Data embedding applications could be divided into two groups depending on the relationship between the embedded message and the cover image [4],[5]. The first group is formed by steganographic applications in which the message has no relationship to the cover image and the cover image plays the role of a decoy to mask the very presence of communication. The content of the cover image has no value to the sender or the decoder. The second group of applications is frequently addressed as digital watermarking. In a typical watermarking application, the message has a close relationship to the cover image. The message supplies additional information about the image, such as image caption, ancillary data about the image origin, author signature, image authentication code, etc. Communication of medical images in a PACS environment is usually over the internal hospital network that is protected by a firewall from outside intruders. Three major organizations related to medical image/data security have issued guidelines, mandates, and standards for image/data security. Conventional Internet Security methods are not sufficient to guarantee that medical image had not been compromised during data transmission. A reversible watermarking scheme involves inserting a Watermark into the original image in an invertible manner in that when the watermark was later extracted, the original image can be recovered completely [6-9]. Medical image compression is very important in the Present era where the information storage having the highest concern. While storing the medical images it is also equally important that images should be effectively compressed by using lossless technique, so that we can reproduce the original medical images without any loss [10]. The amount of data required to present images at an acceptable level of quality is extremely large. High quality image data requires large amounts of storage space and transmission band width [11]. One of the possible solutions is to compress the information so that the storage space and transmission time can be reduced. Image compression address the problem of reducing the amount of data required to
represent a digital image with no significant loss of information. The goal of image compression is to represent an image with a few number of bits as possible while preserving the quality required for the given application [12].

II. EXISTING METHOD

There are four techniques to protect an image. 1) Watermarking 2) Digital Fingerprinting/Signatures 3) Encryption

1) Watermarking: Watermark is a “secret message” that is embedded into a “cover (original or host) message”. Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification message to digital audio, video or image signals and documents. a) Visible watermarks: Visible watermarks change the signal altogether such that the watermarked signal is totally different from actual signal. b) Invisible watermarks: Invisible watermarks change the signal to a perceptually great extent i.e. there are only minor variations in output signal.

2) Digital fingerprints/signatures: It is based on the concept of public key encryption. A public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it. It is mainly used in transmission of images.

3) Encryption: Plaintext is known as original message and cipher text is known as coded message. Encryption is the process of converting plaintext to cipher text to make it unreadable to anyone except those possessing key. Key specifies the particular transformation. Decryption is the process of restoring the plaintext from cipher text.

III. DRAWBACKS OF EXISTING METHODS

a) Major problem with watermarking schemas is that they are not very robust against different types of image manipulations or attacks. These techniques are quite complicated to implement in real-time.

b) Digital fingerprints: Technological Compatibility, Security Concerns, Legal Issues are the prime concerns with respect to finger print.

c) Encryption: Criminals can use encryption to secure communications, or to store Incriminating material on electronic devices.

IV. REQUIREMENTS FOR A NEW SYSTEM

a) Lossless: It is the way of compressing the data which is fully reversible. The obtained image is exact replica of the original image. Therefore it is fully reversible. The word lossless is used to denote a form of compression that does not degrade the quality of the image being compressed. The decompressed image is exactly the same as the original image. In other words, the lossless method is a method of decompression in which no data is discarded. The image is stored in a noncompressed format.

b) Progressive image: Here first low-resolution version of the image is transmitted, and then, upon the reviewer’s request, the low resolution can be progressively improved by further transmission. People don't optimize their images properly, which results in extremely slow loading time. When you intend to publish your images online, you have to compromise the quality, just face the fact you cannot use a 10MB image on a website layout. It's not fair to Visitors. A progressive image transmission allows visualization of a full-sized image even when only a small piece of information has reached the receiver; this full-sized image is an approximate version of the original image. The greater the amount of data received, the more
similar the compressed image is to the original one. In a progressive image transmission, every element of the transmitted data contains information for refining the image globally, instead of locally as a nonprogressive transmitter does. c) Embedding: The distortion due to embedding can be completely removed from the watermarked image without accessing any side channel. The lossless data embedding enables hash insertion while retaining the information content of the image in its entirety. Lossless embedding is a term for a class of data hiding techniques that are capable of restoring the embedded image to its original state without accessing any side information. d) Compression: Code in communications is set of symbols and rules for their manipulation by which the symbols can be made to carry information. Entropy coding is a special form of lossless data compression. It involves arranging the image components in a “zigzag” order employing run length encoding (RLE) algorithm that groups similar frequencies together, inserting length coding zeros, and then using Huffman coding on what is left.

V. NERALMETHODOLOGY

The following diagram describes a general methodology and principles as listed below: At sender side:

1) Define Area: This will define the ROI where the smallest rectangle is obtained. The size of the rectangle is the same for all medical images. The case will be different for other image modalities.

2) HASH value and Patient information: Compute the hash value for the whole image. It is easy to generate a hash given an image, but virtually impossible to generate the image given a hash value and patient information.

3) Embed: This will embed the hash value to the RONI in their LSB. LSB is chosen because of its vulnerability to attack that makes it a perfect candidate for verifying authenticity and integrity of an image. The exact location where the hash value is watermarked is not important in this paper because the image quality does not depend on where the watermark is embedded, but how many pixels have been changed. In our experiment, we determine the area within RONI.

4) Compression: High quality image data requires large amounts of storage space and transmission bandwidth. One of the possible solutions is to compress the information so that the storage space and transmission time can be reduced. Image compression address the problem of reducing the amount of data required to represent a digital image with no significant loss of information. The goal of image compression is to represent an image with a few numbers of bits as possible while preserving the quality required for the given application. In this paper, as per the conventions of Huffman, the sequence of symbols associated with a given message will be called the message code. The entire number of messages to be transmitted will be called the message ensemble. The amiability between the sender and receiver about the meaning of the code for each message of the ensemble will be called the ensemble code. In the way to formulate the requirements of an ensemble code, the coding symbols will be represented by numbers. At receiver side: 1) Extraction: At the receiver end, the watermark is extracted by visiting the back to the watermarking area and read the LSB value. 2) Flipping: The beauty medical images is that the LSB for all pixels in the RONI are zeroes. The flipping function is not literally means that. This function resets the corresponding LSBs back to zero. 3) Hash value: In theory, the extracted image is the same pixel by pixel as the original image. Applying hash value to the extracted image will give the same hash value to the one produced by the original image. 4) Authentication: This can be achieved by comparing the extracted hash values with the hash of the extracted image. If they are the
same, then the image is authentic and that it has not been tampered with (integrity).

**SENDER**

![Sender Side Diagram](Figure 1: Sender Side)

**RECEIVER**

![Receiver Side Diagram](Figure 2: Receiver Side)

**VI. CONCLUSION**

While protection of a patient’s personal data is very crucial it is also important that the patient be reassured that the data being viewed is that of themselves. We proposed a lossless reversible scheme being capable of verifying authenticity and integrity of DICOM images. Besides that the
original image can be exactly recovered at the receiver site, the whole images integrity can be strictly verified. We presented our watermarking scheme, including data embedding, extracting and verifying procedure. Experimental results showed that such scheme could embed large payload while keeping distortion level very low.

VII. REFERENCES


