A Privacy Preserving for Medical Images Using Watermarking

Miss. Dongare Tejaswini G[1]., Miss. Tarate Varsha N[2]., Miss.Pansare Mangal B[3]., Miss. Tamb Gayatri A[4].
BE Computer Engineering, S.V.C.E.T. Rajuri, Pune-412410[1,2,3,4].
dongaretejaswini@gmail.com[1],varshana11@gmail.com[2], Mangal1994@gmail.com[3],
gayatritambe1991@gmail.com[4]

***Abstract*— Now a day's security is an important issue in transmission of images over network. Provide security to an images and data is very important. For that purpose we can use various techniques. In this technique watermarking is important for provide security and authentication. Watermarking is secret code applied on images or text. Watermarking is used for provide security as well as protect the copyrights of user. Watermarking technique is used in Hospital Data Management for protect the patient diagnostic, X-ray images and information. In these paper we introduce new concept which is useful for provide security patient medical images and his information. In Hospital Data management System there is need of effective data management; authentication, data Storage, and secure access control watermarking provide these various facilities to system. The main objective of this paper is embedding, and extracting watermark without loss of data. In that we used invisible watermarking also used concept reversible watermarking to retrieve original image.**

***Index Terms*— Authentication, Cryptography, Encryption, DCT, DWT, ROB, RONI, ROI, Watermarking.**

I. INTRODUCTION

In recent years, Internet and multimedia data introduce reproduction. This helps digital information make more easy and useful. The new technologies provide much more facilities to transmit the information one form to another form without any effort. So the protection and authentication like issues are arises. In recent years, digital watermarking provides copyright protection, authentication, and authorization and protects the digital content of data [8]. Telemedicine combine the information with information technology and transmitted over long distance. Telemedicine are used in telesurgery, teleconsulting, telediagnosis and remote medical information [1]. Exchange medical information between different hospitals is common issue. Hence, in health care secure, robust, and more secure data protecting techniques are needed. In modern hospital managing the hospital data computer network are used. In hospital data medical images are main entity which is stored in digital form and it is transmitted using computer network. Computer network are not secure for transmitting data so protect the medical image over the transmission is important. The image is most important entity in diagnostic procedure that can help physician evaluate the patient diagnosis. Watermarking provide these all services. Watermarking technique is mainly based on data modification. Therefore these watermarking is called as reversible watermarking. For integrity and privacy purpose reversible watermarking is used. It provides user authentication, authorization, integrity, and information confidentiality. For obtain this all facility encryption and decryption techniques are used. This includes MD5, R-S-Vector, Hash value, AES encryption techniques.

).

In this system owner decide to how her file is encrypting, users have his own encryption or decryption key. These are allowing to user who have authorized. Here protect the confidentiality of user. We provide confidentiality, scalability for secure sharing medical images. We can also compare our technique to pervious various techniques.

II. LITERATURE SURVEY

Digital watermarking is a secret code applied on paper or image. Digital watermarking technique are used for protect the image or copyright protection, prove the ownership. Digital watermarking is secure for researcher to hide the information inside image which is not easily detected. Basically digital watermarking divided into different types. These various types are introduced according to different working domain [2].

The reproduction of information is become easy using network. For data reproduction, manipulation, distribution digital data can create a problem for authorized user which is want prevent data from illegal use. Watermarking is used for copyright protection. Digital watermarking is robust, imperceptible and embedded secure message on image or document for example copyright information. Modification, re-distribution, and coping of document cannot itself by digital watermarking. Whenever copy protection fails in encryption, watermarking allows backtracking to its authorized user and successfully identified unauthorized user. Watermarking hide the information always digital object which is his user need to prevent. Steganography can be used for only hide any information. Watermarking does not need any key but cryptography needs encryption key for encryption process and decryption key for decryption [3].

Applying embedded signal on to image for security purpose is called as watermarking. In previous binary watermark is introduced which is contain minimum value of image from every 2*2 block. Arnold Transform [7] is used for disordering purpose but it is cannot show the robustness against in compression or rotation operation. Improving this problem innovative watermarking is introduced. Better utilization of rescaled version of original image and obtaining low frequency sub band of wavelet domain innovative watermarking is ^{used}. Using Discrete Transformation Domain embedding and extraction process is done on high level frequency. In that extraction process is done absence of original image, here quality of image is measure by blind computing [4]. In diagnostic and management decision medical imaging is important. Embedding process data is inserted into medical image. This data is robust and secure from various attacks. Data can be including patient and his diagnostic information. These method can used improve the telemedicine application. The main purpose of these watermarking is increase integrity and confidentiality level over network sharing. This is based on LSB (Least Significant Bit) [5].

III. Related work

This section includes different techniques which are used for image authentication through watermarking [2]. Reversible watermarking technique is used for image authentication and self-correction. In this technique image is divide into two part ROI and RONI. It is useful for if there is some changes in image it can easily detect and restored it from original image by extracting ROI from the RONI [7].

On the base lossless watermarking authentication is proposed [3]; it is used for patient information and message with using lossless compression technique. Using MD5 algorithm calculate the authentication code. Patient information and authentication code are concatenated and then encrypted. Least Significant Bit is used for select all pixel for compression. These proposed system having the disadvantage of LSB embedding process which will change statically [9] [10]. Computer system easily detects hiding process.

In [4] a blind watermarking is based on wavelet transformation. It is used for hide patient record in image for save patient information and save storage space over transmission. It embedded patient record using wavelet transformation. It increases the robustness but having the disadvantage of it purely implemented on gray scale image and also it has low embedding capacity.

To provide copyright protection and authentication robust fragile watermarking technique is used [5]. It provides the authentication CT scan images against distortion. In this technique separate ROI and RONI from image. These techniques increase the embedding capacity of image. It does not affect diagnostic value of image for embedding the watermarking. It is replace LSB method by spatial domain [9].

A reversible watermarking is based on histogram and classification of image. In this method most important part is select efficient watermarking method. On the based on reference image embedding and extraction process is implemented [6]. Using this method predicts the errors between image and reference image. It is embed with high capacity of embedding and low distortion.

Reversible watermarking is also based on Quantization Index Modulation in health care management system. It is useful for reconstruct the original image; embedding capacity is increase using this technique. It is work on only gray scale image. There is need to test watermarking on color image. Basically most security techniques are based on encryption methods and watermarking is proposed to protect image.

1. AES ALGORITHM

AES is new cryptographic algorithm which is used for protect digital information. It is called as advanced encryption standard algorithm for encryption. AES is a symmetric key block cipher that can use keys of 128, 192, and 256 bits, and encrypts or decrypts data in blocks of 128 bits (16 bytes). AES use a pair of key, symmetric key ciphers use the same key to encryption and decryption of data. The data which encrypted returned by block ciphers have the same number of bits that the input data. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data. The AES algorithm is depends on permutations and substitutions. A permutation means that rearrangements of data and substitutions are the replacement of the data i.e. replaces one unit of data with another. Using several different techniques, AES performs permutations, and substitutions. The key size used for an AES cipher represents the number of repetitions of transformation rounds which convert the input, called the plaintext, into the final output, called the cipher text.

The number of cycles of repetition is as follows:

1. For 128-bit keys 10 cycles of repetition
2. For 192-bit keys 12 cycles of repetition.
3. For 256-bit keys 14 cycles of repetition

Several processing steps are consisting by each round, each containing four similar but which are different stages. In those, one that depends on the encryption key itself. To transform cipher text back into the original plaintext, a Set of reverse rounds are applied using the same encryption key.

2. DCT ALGORITHM

DCT based watermarking techniques are more robust as compared to spatial domain watermarking techniques. This algorithm is robust against simple image Processing operations like low pass filtering, contrast and brightness adjustment. How- ever, they are difficult to implement and are computationally more costly. And also they are weak against geometric attacks like scaling, rotation and cropping etc. DCT watermarking can be classified into Block Based DCT watermarking and Global DCT watermarking.

3. R-S VECTOR

In this algorithm first scan a cover image block by block, in resulting it is called as R-S-vector formed by representing. In which R-block by binary 1 and an S-block by binary 0 with the U groups simply skipped. Then the algorithm lossless compresses this R-S-vector as an overhead for book keeping usage in reconstruction of the original image late. By assigning binary 1 and 0 to R and S blocks, respectively, one bit can be embedded into each R or S block. If the bit to be embedded does match the type of a block under consideration, the flipping operation F is applied to the block to obtain a match. The actual embedded data consist of the overhead and the watermark signal. In data extraction, the algorithm scans the marked image in the same manner as in the data embedding. From the resultant RS-vector, the embedded data can be extracted. The overhead portion will be used to reconstruct the original image, while the remaining portion is the payload.

IV. REQUIREMENTS

To achieve preserve privacy of patient and provide security to image there is need to take care about related security issues. This various aspects are listed below;

- *Data Confidentiality:* watermarking is added in image to protect the copyright of user and image also. Any unauthorized user cannot access the data or not made changes in information.
- *Scalability:* It is one of the important requirements of watermark system. Always take care about system should be scalable.
- *Efficiency:* There is need of our system should be work efficiently.
- *Usability:* The system should be support users. So there is need of system should be usable.

V. SYSTEM OVERVIEW

Main goal of our system is provide security to image or preserve the privacy of patient. In this section describe the proposed system working. In that watermarking embedding process, watermark encryption, watermark extraction process, R-S-vector compression process is explaining detail.

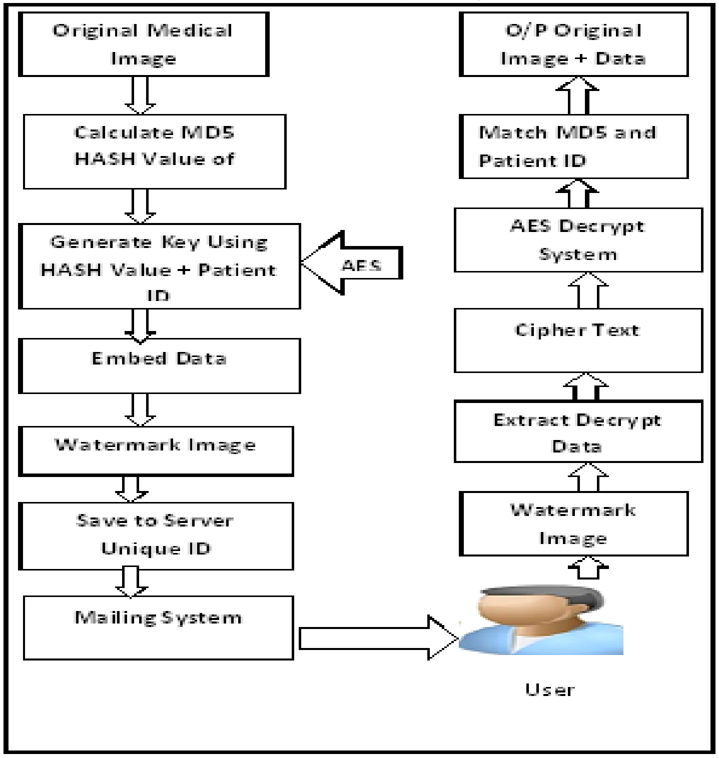


Fig.1. Architecture of proposed system

1) *Watermark Embedding process*

Image integrity is achieved in watermark embedding process using algorithm. Authentication is add in image using following step :(Fig. 1)

1) Extract group of pixel
2) Determine R-S-Vector by extract group of pixel.
3) Compress R-S-Vector of pixels
4) Calculate MD5 hash value of image.
5) Encrypt the data into watermarking using key 1.
6) Embedding watermark using key 2.

These all steps are explained following subsection;

1. Extract Group

In these step, image is divided into group of pixels, each group contain group of four pixels. This pixel represented as singular value. This singular value can be identified by Flipping function or Discrimination.

- Discriminating Function (F)
  Describe the state of group discrimination function
  Is used.
- Flipping Function(F)

To modify the pixel value flipping function is used.

2. *Creating R-S-Vector*

In creating R-S-Vector each pixel value 0 for singular(S-value) and 1 for regular (R-value) group. In that unused groups can be remove because they cannot affected on flipping function. That's why R-S-Vector use stream of bits. These bits represent state of pixel in group.

3. Compression process of R-S-Vector

Compression algorithm needs following conditions for compress the data in image:

1) There is need to restore original R-S-Vector that is lossless compression.
2) Maintain better compression ratio like these types of data.
3) There is need in compression algorithm to ability of compress binary data.
4) In compression algorithm ability to compress random data.

These all are the main criteria to compression R-S-Vector.

For providing the efficient space to watermarking there is need of compress the R-S-Vector. Efficiency of compression process is depends on nature of data. Embedding capacity is calculate using following formula:

$$Cap=NR+Ns-|C| \qquad (1)$$

Where (NR) represent regular group in image, (Ns) represent singular group, (C) is a length of R-S-Vector.

There is target to maximize embedding capacity by using minimum compressed length (|C|).

$$-N_R \text{ Log } (N_R)/(N_{R+}N_S)-N_S \text{ Log}(N_S)/(N_R+N_S)\text{bits} \qquad (2)$$

From Eqs. (1) and (2) real capacity is calculate as following formula:

$$Cap'=N_R+N_S+N_R \text{ Log } (N_R)/(N_R+N_S)+N_S \qquad (3)$$

Flipping function basically is used for modify the LSB of the four pixel. There is unused groups are increased so we can modify only middle two bits.

4. Calculate MD5 hash value of image

Integrity is main aspect to provide integrity of medical image MD5 algorithm is used. S MD5 can be produced message authentication code which is unique. Its size is equal in only 128 bits. It can save the size of compression algorithm.

5. Creating watermark on image

In this process concatenate MD5 hash value, Patient-id, information, and the compressed R-S-Vector in the original image. This concatenated information encrypted using AES algorithm. It is useful for create watermark; this can be embedded into image.

MD5 is used to maintain image integrity, for authentication purpose patient-id is used, and the AES is used in watermarking for provide confidentiality. AES is allow to user encrypt the watermark using private key to shared between sender and receiver user.

2. Extraction process of watermark

This process is used to retrieve original image and information from watermark image; this process consists following steps to retrieved original image:

1. Extract the group as per 4 pixels.
2. After R-S-Vector is calculate then extract the Encrypted watermark.
3. Using AES decrypt the watermark.
4. Extract the embedding information i.e. patient-id, R-S-Vector, MD5 hash value.
5. Decompress the R-S-Vector.
6. Original image is extracted.
7. Calculate hash value of extracted image.
8. Compare hash value and extracted hash value, if it is same then the image is authenticated, it has integrity.

VI. EXPERIMENTAL RESULT

The proposed technique applied on X-ray image. The result is shown below:

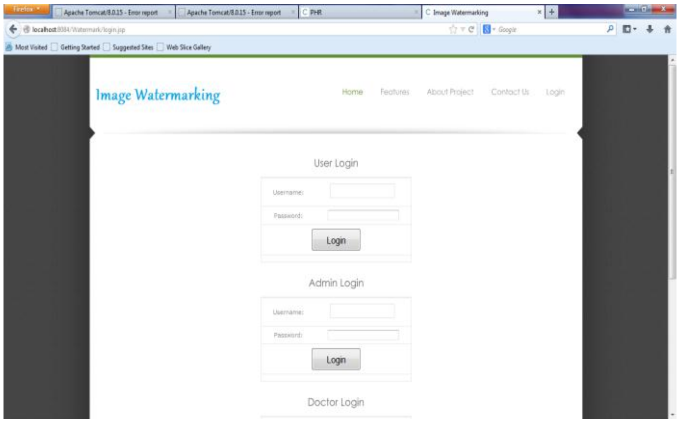
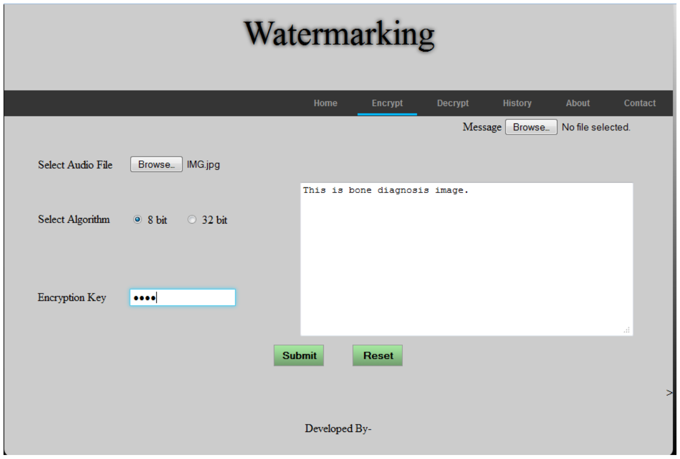


Fig.2.1 User Log-in process

Proposed system is useful for provide security so there is need users are validate. Security purpose user need to create his account in system. Using user-id and password they can create own secure account in system for secure image transmission.



Message No file selected.

Select Audio File IMG.jpg

Select Algorithm ● 8 bit ○ 32 bit

Encryption Key ••••

```
This is bone diagnosis image.
```

Fig.2.2 Encryption and watermarking process

This is encryption and watermarking process, in that using user-id and password user log into system. After that he can select image from database which send to another user. Also write patient report message on text box. These all embedded in patient image. In this process user provide encryption key.

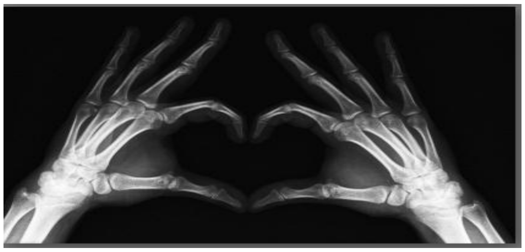
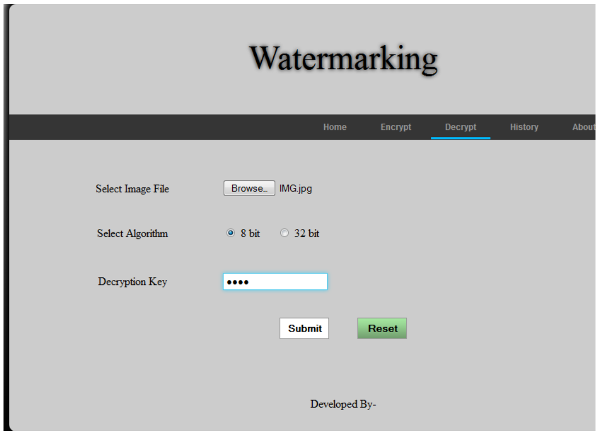


Fig.2.3. Watermark image

Fig.2.3. shows watermark image with embed patient information without any distortion.



Select Image File IMG.jpg

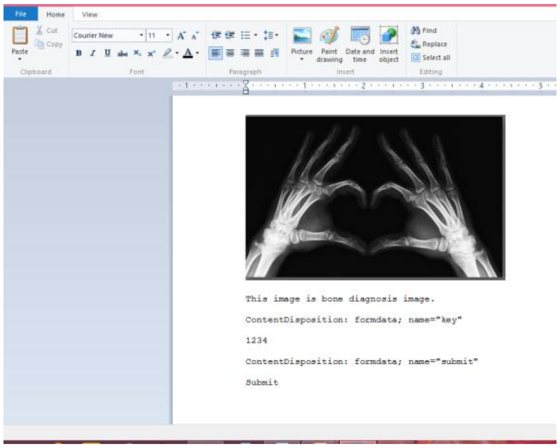
Select Algorithm ● 8 bit ○ 32 bit

Decryption Key ••••

Developed By-

Fig.2.4 Decryption process

Decryption process is useful to retrieve original image and patient embed information. In this process user need correct decryption to decrypt the image. If user having correct decryption key he can successfully decrypt the image.



```
This image is bone diagnosis image.

ContentDisposition: formdata; name="key"

1234

ContentDisposition: formdata; name="submit"

Submit
```

Fig.2.5 Original image with embedding information

In this figure successfully retrieve original patient image with his information without loss any data or destroy quality of image. In this way proposed system provides security, integrity, confidentiality to patient using invisible watermarking.

VII. ACKNOWLEDGMENT

We are thankful to our project guide Prof. Hase A.K. for his proper guidance and valuable suggestions. We are really grateful to them for their kind support. We are grateful to Prof. Patil H. K., Head of Computer Engineering Department, S.V.C.E.T. Rajuri for his indispensable support, suggestions. We are also greatly thankful to other faculty member and our friends to help us.

VIII. CONCLUSION

In this paper medical image security technique is based on reversible watermarking. This technique provides security, integrity, confidentiality to medical image. This technique is reversible because at the receiver side successfully achieve original image without loss of data.

As per speed increases of computer security problems becomes complex. Providing secure algorithm to protect medical images and information is complicated because of special concern of medical community. The proposed security technique increase security level, maintain integrity, reduce encryption processing time.

References

[1] K. Youngberry, "*Telemedicine Research*", Journal of Telemedicine and Telerate, Vol. 10, No. 2, pp. 121-123, 2004.

[2] Memo N, Gilani S, "*Adaptive data hiding scheme for medical image using integer wavelet transform"* In: IEEE International conference on emerging technologies, Islamabad, Pakistan; 2009, P-221-4.

[3] Boucherkha S, Benmohamed M., "*A lossless watermarking based authentication system for medical images*", Int J signal Process 2004;1(4):278-81.

[4] Mostafa S, EI-sheimy N, Tolba A, Abdelkader F, Elhindy H. "*Wavelet packets-based blind watermarking for medical image management*", OpenBiomedicalEngg.J2010;4;938<http://www.benthamscience.com/open/tobej/opennaccess2.htm.>.

[5] An L,**Gao**X,Xuelong L, Tao D,Deng C, Li J, "*Reversible watermarking via clustering and enhanced pixel-wise masking*", IEEE Trans image Process 2012;21(8):,pp. 890-896.

[6] Pan W, Coatrieux G, Cuppens N, Cuppens F, Roux C, "*Reversible watermarking based on invariant image classification on and dynamical histogram shifting*", In Engineering in medical and biology society, annual international conference of the IEEE, August, 2011. P. 4477-80.

[7] Sonika C. Rathi, and Vandana S. Inamdar, "*Medical images authentication through watermarking preserve ROI",* Health Informatics - An International Journal (HIIJ) Vol.1, No.1, August 2012.

[8] R.LAKSHMI PRIYA, V.SADASIVAM, "*A survey on watermarking techniques, requirements, applications for medical images"* Journal of Theoretical and Applied Information Technology, Vol. 65 No.1 10 th July 2014.

[9] Abdullah Bamatraf, Rosziati Ibrahim and Mohd, Najib Mohd. Salleh, "*A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit",* JOURNAL OF COMPUTING, VOLUME 3, ISSUE 4, APRIL 2011, ISSN 2151-9617.

[10] Gurpreet Kaur, Kamaljeet Kaur, "*Image Watermarking Using LSB (Least Significant Bit",* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.