Secure Sharing of Medical Information in Watermarked Image through Telemedicine using PKI Technique

Ishwarya.V
Software Programmer
Isysway Technologies
Thanjavur,TamilNadu

Thamarai Selvan.T
Software Consultant
Isysway Technologies
Thanjavur,TamilNadu

ABSTRACT

Security is the fundamental requirement for an information society in the distributed network environment. A watermark is a secret message that is embedded into a cover message. Digital watermarks are used to verify the authenticity of the carrier signal for the identity of the owners. In order to provide data integrity, confidentiality and authentication various techniques are available like cryptography, steganography and watermarking. To protect the patient information in telemedicine, watermarking is mainly used. Patient information is embedded within the cover medical image. Digital Imaging & Communications in Medicine is an universal standard of communication for secured medical images. In the proposed technique, to provide authentication the hash value will be generated using SHA and the Huffman compression algorithm(R-S vector) will be used to shrink the size of an image. With the patient information the medical image is protected through Public key cryptography in a secure manner. Compared to the previous system, the proposed technique is more efficient. The original image is completely restored without any loss at the receiver side. The patient information is hidden (protected) from the hackers during transmission.

General Terms

Medical Image Security.

Keywords

Watermarking, Medical images, Digital Imaging and Communications in Medicine Public key cryptography the proposed method**.**

1. INTRODUCTION

1.1 Related Works of watermarking for medical images

Data hiding embeds the data in a cover text. It is also known as information hiding. Data hiding techniques consists of cryptography, steganography and watermarking. To provide data integrity, confidentiality and authentication these techniques are used [2]. Cryptography is the study of information security [4].It changes the plain text or a word in to cipher text in a form of a code. Steganography is the art of hiding the information in other information. For hiding the secret information several steganographic techniques are available. Watermarking has more advantages than steganography. It makes the information imperceptible and more robust. Watermarking in medical image is used for storage, transmission and telediagonsis[3][12].

Watermark embeds the confidential data in the text, image, audio and video. Watermark is the visible image imprinted on the paper and added digitally to the image. It may be company logo, name of the person or copyright symbol. It ensures copyright protection [8][20]. Watermark is visible only for the owner and the people who know the key information [21][22]. Comparing to analog format digital images are more secure [16]17].One of the most important techniques in watermarking is digital image watermarking. Digital image embeds and transfers the data in to host image. In other words digital watermarking can be viewed as information hiding or steganography [3][23].

Woo et al [13] introduced wavelet transform for medical images. It consists of physician signature and the information of the patient. This information is inserted into wavelet transform. kobayashi et al[14] upgrade the security of medical images. With the integrity and authenticity stronger link is provided between image and information. DICOM images are used for development is an added advantage. Kannamal et al [18] proposed medical images with the fragile watermarking algorithms. Selective bit plane is used and the performance is analyzed. The algorithm is differentiated with DWT and ICA (Independent component Analysis) methods. With the limited scope Zain et al [9] proposed reversible watermarking techniques. Zhou et al [11] presents a method for encrypting digital signatures. This method has better authentication and integrity. Coatrieux et al [7] suggested watermarking algorithm for medical images. In most of the papers embedded information is in the non-ROI region. Eggers et al [6] proposed the symmetric methods with the combination of public detectors. In this technique the watermark is removed simultaneously or it made as unreadable. The private keys ensure the security.

Hartung and Girod[15] proposed the asymmetric watermark with the spread spectrum of watermarking. Private Key is used for watermark embedded process. Watermark is verified using public key and the redundancy made with the private key. With the Legendre sequences the method is proposed by schyndel et al [5]. Legendre sequences combines with the Fourier transform. Legendre sequences are used as a private key to embed the watermark image. The sequence length is made as a public key. This method has N-2 Legendre sequences. Some malicious attacks are preferred in this technique.

1.2 Related Works of Existing with the Proposed Scheme

The integer wavelet transform is used with medical images for data hiding [24].The disadvantage of this fact is it is suitable only for gray scale images not for color images. Our proposed system overcomes this problem. Mohamed et al [1] suggested that Patient id, hash value and the compression process are concatenated to form a watermark and it is encrypted using AES encryption technique. The Same key is used for both encryption and decryption. So it is less secure. In the proposed system the watermarked image is encrypted using public key cryptography and RSA algorithms to enhance the security during transmission.RSA algorithm are one of the widely used public key algorithms. In RSA algorithm the image is encrypted using receiver public key and decrypted using the private key. The public key is known to everyone and the private key is kept secret. To protect medical images LSB watermarking methods are used for encryption [25].Due to LSB (Least Significant Bit) the hidden information is identified easily.

2. PROPOSED SYSTEM

2.1 Asymmetric Watermarking

This type of cryptography consists of private key and public key. What is encrypted by one key can be decrypted by the other one. Public key made publicly available. Public key is used for encrypting the watermark while the private key is used for decrypting the watermark [10]. If the authenticity of the public key is trusted then we can know the author of the model and who embedded the watermark. Public key cannot be used as the private key [19]. If the key is chosen it is difficult to compute the private key starting from the knowledge of public key. The process involved in PKI technique consists of the following steps.

i. In the PKI technique, everyone has the key pair of public key and private key.
ii. The two users, one is sender and another one is the receiver. Sender provides the copy of the public key to receiver.
iii. Receiver’s trust the sender’s public key and use it to encrypt the data in the medical images hiding information.
iv. Receiver sends encrypted data hidden medical images to sender.
v. Sender decrypts the information in the hidden copy of medical images. Private Key is used.

2.2 DICOM image and R-S Vector Compression

Digital Imaging and Communications in the Medicine is the universal standard communication for secured health check images. Digital images are obtained from x-ray, digital radiography, ultrasound and the hospital information system. The original images are completely restored with the digital images. DICOM file consists of header and the image data. The header associated with the patient name, dimensions of the image and type of the scan. The data elements consist of patient information and hospital information. When the DICOM file has to be authenticated the pixel values must be extracted. Transformation is used to pick up the real pixel values.

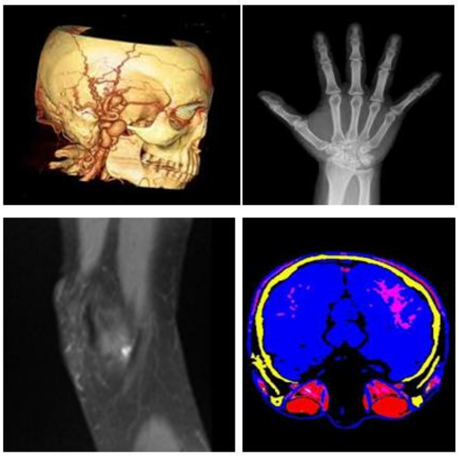


Figure 1.DICOM images

Figure 1 shows the DICOM image. This image is compressed using R-S vector. Hash value, R-S vector are embedded in the image matrix and it is written again according to the DICOM standard. For authentication of DICOM, the image file is extracted then the R-S vector, hash value are extracted. The R–S-Vector consists of a stream of bits (zeros and ones). Symbols 4 and 8 are used in the compression process. Each group of pixels has a single value: 1 for R (Regular group), 0 for S (Singular group) and -1 for U (Unused group).

2.3 Creating Hash value

Hash value mainly used for message integrity and password validity. Hash value of the image is determined using SHA hash function.SHA produces image integrity and patient authentication more advanced than MD5.The SHA hash value, patient id and the compressed R-S vector are concatenated to form watermark and it is encrypted using RSA algorithm be justified, not ragged.

2.4 Embedding Process

In the embedding process the watermark is inserted into medical image. Figure 2 shows the watermark embedding process. Then the watermark image is encrypted. The watermark embedding consists of following steps.

i. The image is partitioned into groups. Each group has four pixels with a single value. The state of the group is identified for R-S vector.
ii. Determine and compress the R-S vector.
iii. Calculate the SHA value of the image. Add the SHA value to the compressed R-S vector and patient id to form a watermark.
iv. Encrypt the watermark using public key.
v. In embedding process the algorithm achieves image integrity and authentication.

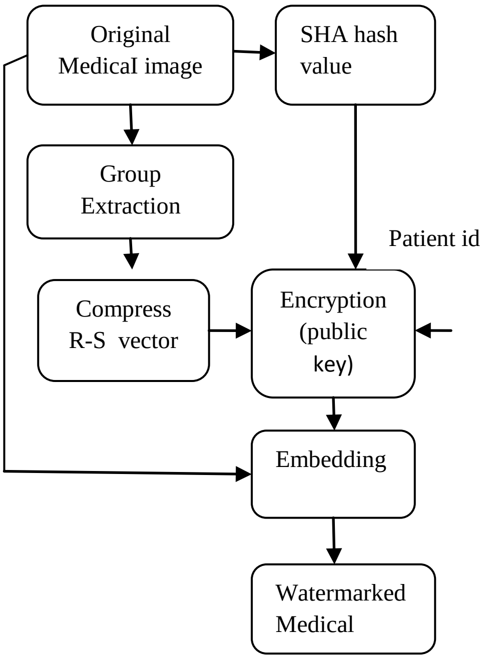


Figure 2.Embedding Process

2.4.1 Encryption using RSA

The watermark information is encrypted using RSA algorithms to enhance the security during transmission. In RSA algorithm the image is encrypted using receiver public key and decrypt the encrypted message using the receiver private key. The public key is made available to everyone and the private key is the secret key remains confidential.RSA algorithm protects the watermarked images from tampering and eventually applies compression to reduce the size of encrypted watermarked image. The process consists of the following steps. In RSA algorithm the key is generated as follows.

i. Random prime numbers are selected such as a
ii. and b.
iii. Check a!=b
iv. Evaluate Modulus n=axb
v. Evaluate z=(a-1)x(b-1)
vi. Select public exponent e,1<e<z
vii. Evaluate private exponent (dxe)modz=1
viii. {n,e}is the public key, d is the private key.
ix. C=m^emod n(m-message,c-encrypted message)

Therefore encrypted form is described as number m,0<m<n-1.e and n are the public keys which is to be transmitted.

2.5 Extraction Process

In Extraction process the image is retrieved and the process consists of the following steps:

i. Extract the encrypted watermark.
ii. Decrypt the watermark image using receiver private key .It remains confidential.
iii. Extract the hash value, patient id and R-S vector of the watermark image, and then calculate the hash value with extracted original image.
iv. If the hash values are equal the image is authenticated else image is discarded. The process for extracting the watermark is shown in figure 3.
v. Watermark extraction that applies one or more pre-process and the extracted watermark is same as the original watermark.
vi. The SHA hash value of the extracted non-watermarked image is calculated and it is compared with the decrypted SHA hash value.
vii. If the hash values are different the image is no longer authenticated. If the image is authenticated encrypted process is coordinated by legal user in the medicinal system because the user has private key.

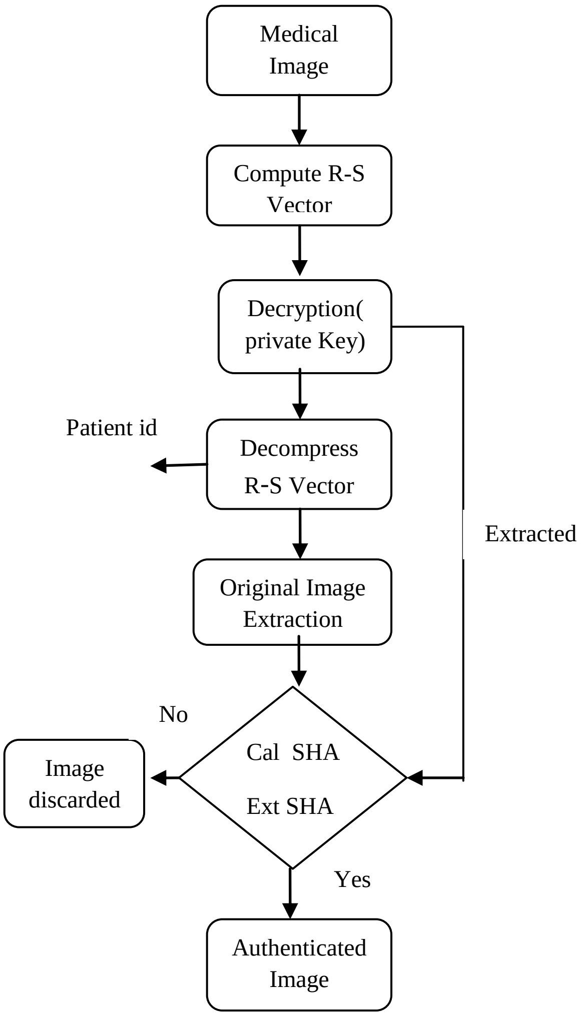


Figure3. Extraction Process

2.5.2 Decryption Using RSA

Decryption involves the reverse process of encryption. In case of RSA algorithm, the image is decrypted using receiver's private key. Private Key d is used to decrypt messages. m is the original message.

$$c^d \text{mod } n=m$$

Finally the watermark image is formed. This watermarked image provides security and authentication. The reversible watermark cannot be retrieved by an unauthorized person. This provides the major security in the Human Management System.

3. EXPERIMENTAL RESULTS

The experimental results of the proposed technique for authentication of medical images based on watermarking technique are discussed in this section. An application is programmed using C#.NET language to implement this technique. For authentication and integrity, RSA is a potential method for medical images. The performance parameters that are represented to measure the performance of the proposed technique are: Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Bit Error Rate (BER).The original images before embedding the watermark and the authenticated image after embedding the watermark is displayed in Fig 4.

Experimental results shows that PSNR has high range values and it is consistent and the MSE has a least values therefore the quality of the images is not affected.BER is equal to zero for all the four DICOM images.SNR also has large values. The values predicted in Table 1.

Table 1.Output results of DICOM grayscale and color medical images

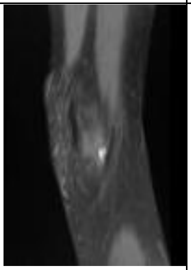
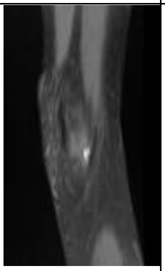
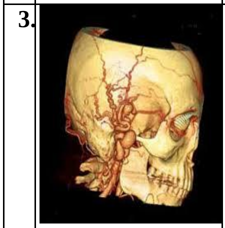
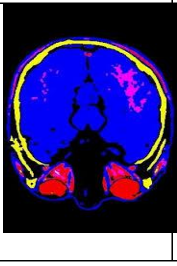
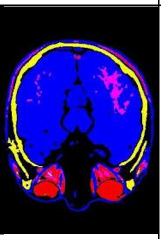
S No	Original image	Watermarked image	PSNR	MSE	BER	SNR
1.			53.21	0.585	0	38.20
2.			50.82	0.745	0	42.38
3.			50.94	0.751	0	42.50
4.			51.56	0.778	0	43.12

Table 2.Output results of grayscale and color test images

S No	Original image	Watermarked image	PSNR	MSE	BER	SNR
1.			64.96	0.273	0	73.39
2.			83.73	0.806	0	92.17
3.			71.12	0.390	0	79.56
4.			65.79	0.286	0	74.23

The results prove that the proposed technique is totally revertible, and the original images can be retrieved at the receiver side without any distortion because of the R–S-Vector is extracted without errors. In table 1 and table 2 gray scale images and color medical images are compared with test images of color and grayscale. PSNR and SNR has higher values.In[1] the grayscale and color medical images is similar to the test images of grayscale and color watermark image.In the proposed technique the grayscale and color medical image is different from the test images.Therefore by using symmetric encryption the performance measurements are consistent. Eventhough the Public key Encryption has its own secret key and it is secure they are not consistent in the performance measurements.

4. CONCLUSION

Based on the DICOM images the watermarking technique is proposed. This technique is tested with color and grayscale medical images as well as test images . The hash value based on SHA is determined from the image. With the patient id, hash value and the compressed R-S vector watermark is formed and encrypted using public key cryptography.RSA is a secure public key encryption algorithm provides information security. The quality measures such as PSNR, SNR, MSE and BER estimates the security of algorithms. Concluded results shows that BER equals 0, SNR and PSNR has a high consistent values.MSE have a low bit rate for all grayscale and color images. As in future work symmetric key cryptography with SHA hash value can be in performed in transform domain for enhancing the security.

5. REFERENCES

[1] Mohamed M. Abd-Eldayem.A Proposed Security Technique Based On watermarking and Encryption for Digital Imaging and communications in medicine, Egyptian Information Journal,2012.

[2] Planitz, B.M., Maeder, A.J.:" A Study of Block-Based Medical Image Watermarking Using Perceptual Similarity Metric", In: Proceedings in DICTA 2005, p. 70 ,2005.

[3] M. Naor, B. Pinkas," Visual authentication and identification", Lecture Notes in Computer Science, vol 1294, pp.322,1997.

[4] Xiaoqing Tan, Qiong Zhang," A Kind of Verifiable Visual Cryptography Scheme", International Conference on Emerging Intelligent Data and Web Technologies,2013.

[5] R. G. van Schyndel, A. Z. Tirkel, and I. D. Svalbe, "Key independent watermark detection,"in Proc. IEEE Int. Conf: Multimedia Computing and Systems, Florence, Italy, pp. 580-585,1999.

[6] J. J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in Proc. Eur. Signal Processing Conf:, Tampere, Finland, Sept. 2000.

[7] Coatrieux G, Lecornu L " A review of image watermarking applications in healthcare".Proceedings of the 28th Annual International Conference of the IEEE: Engineering in Medicine and Biology Society,EMBS ,2006.

[8] Memon N. Watermarking of medical images for content authentication and copyright protection. PhD thesis, Pakistan: Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology; May 2010.

[9] Zain J M, Baldwin L P, Clarke M ,"Reversible watermarking for authentication of DICOM images",Proc. 26th Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC 2004) 2: 3237–3240,2009

[10] P. Wong, "A Public Key Watermark for Image Verification and Authentication,"Proceedings of ICIP'98, pp. 425-429, 1998.

[11] Zhou X Q, Huang H K, "Authenticity and integrity of digital mammography images", IEEE Trans. Med.Imag. 20(no. 8): 784–791,2001.

[12] B. Mathon, ''Development of safe watermarking methods for tracing of multimedia contents", International thesis cotutelle, University of Grenoble and of Louvain, 2011.

[13]C.S. Woo, J. Du, and B. Pham, Multiple watermark method for privacy control and tamper detection in medical images, WDIC2005 pages, Australia,February, pp. 59–64,2005.

[14] L.O.M. Kobayashi, S.S. Furuie, and P.S.L.M. Barreto, Providing Integrity and Authenticity in DICOM Images: A Novel Approach, IEEE Trans Inform Technol Biomed, 2009.

[15] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," In Proc. Of the IEEE Intl. Conf on Image Processing 1997, vol. 1, pp. 528-531, October 1997.

[16] H. M. Chao, C.M. Hsu, S.G. Miaou, "A Data Hiding Technique With authentication,Integration, and Con_dentiality for Electronic Patient Records", IEEE Transactions on Information Technology in Bio-medicine, Vol. 6, No. 1, pp. 46-53, March 2002.

[17] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A Secure Data Hiding Technique with Heterogenous Data Combining Capability for Electronic Patient Records",Proceedings of IEEE International Conference in Medicine and Biology Society (EMBC'00), Chicago, USA, Vol. 1, pp. 280-283, 2000.

[18] A. Kannammal, S. Subha Rani, K. Pavithra, "Authentication of DICOM medical images using independent component analysis (ICA)", Int J Med Eng Inform 4 ,2012.

[19] Dariusz Bogumi," An asymmetric image watermarking scheme resistant against geometrical distortions" Elsevier B.V.2005.

[20] B.Nassir, R.Latif, A.Toumanari," Secure transmission of medical images by watermarking technique"IEEE 2012.

[21] M. Kutter, "Digital ImageWatermarking: Hiding Information in Images", PhD thesis,University of Rhode Island, Kingston, USA, 1999.

[22] C.-T. Hsu, J.-L. Wu, "Hidden Digital Wateramrks in Images", IEEE Transactions on Image Processing, Vol. 8, pp. 58-68, 1999.

[23] G.-J. Yu, "Digital Image Watermarking for Copyright Protection and Authentication", PhD Thesis, National Central University, Taiwan, R.O.C, 2001.

[24] Memon N, Gilani S. Adaptive data hiding scheme for medical images using integer wavelet transform. In: IEEE international conference on emerging technologies, Islamabad, Pakistan; 2009.p. 221–4.

[25] Bouslimi D, Coatrieux G, Roux C. A joint encryption/watermarking algorithm for verifying the reliability of medical images:application to echographic images. Comput Methods Programs Biomed 2012;106(1):47–54.