Global Journal of Computer Science and Technology: H
Information & Technology
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Fusion of Steganography Digital Watermarking Data Hidden in Patient Medical Image using PPC Approach

By Dr. S Santhosh Baboo & V R Sasikumar
Manonmaniam Sundaranar University, India

Abstract- Privacy is a critical issue when the patient message storage or processing to the medical services. Digital Image processing is the quick emerging area of medical science. The improvement of image processing was given by the technology improvement like digital visualizing, computer processor and large storage devices. Image processing allowed to compute the image in multidimensional within the system. First, the real problem becomes many severe due to the decrease of visual proofs in telehealth applications. A watermark is a protect message that message hidden into a mask message. Digital image watermarks are used for check the approval of the carrier signal for confirmation of the owners. In order to give information honesty, confidentiality and authentication various approaches are accessible like networking side cryptography, image processing side steganography and digital watermarking. To protect the patient message in telehealth, hidden into a mask message is recently used. Patient details are watermark within the cover medical image. The public and personal key cryptography (PPC) is insufficient for providing the trust a patient may attain during a face-to-face service.

Keywords: medical image, public and personal key cryptography method, cryptography, steganography and watermarking.

GJCST-H Classification: J.3

Fusion of Steganography Digital Watermarking Data Hidden in Patient Medical Image using PPC Approach

Dr. S Santhosh Baboo [α] & V R Sasikumar [σ]

Abstract- Privacy is a critical issue when the patient message storage or processing to the medical services. Digital Image processing is the quick emerging area of medical science. The improvement of image processing was given by the technology improvement like digital visualizing, computer processor and large storage devices. Image processing allowed to compute the image in multidimensional within the system. First, the real problem becomes many severe due to the decrease of visual proofs in telehealth applications. A watermark is a protect message that message hidden into a mask message. Digital image watermarks are used for check the approval of the carrier signal for confirmation of the owners. In order to give information honesty, confidentiality and authentication various approaches are accessible like networking side cryptography, image processing side steganography and digital watermarking. To protect the patient message in telehealth, hidden into a mask message is recently used. Patient details are watermark within the cover medical image. The public and personal key cryptography (PPC) is insufficient for providing the trust a patient may attain during a face-to-face service. Second, telemedical services, such as tele-watching or tele-consultant, normally demand a systematic company of users, roles, assets, and flows of message. Image processing operation can be applied to the digital image processing to taken craved output image. In this paper to provide authentication the hash value that generated applying SHA and the lossless compression rule (Regular-Singular vector) will be allowed to shrink the dimension of an digital image. With the patient message the medical image is secure through Public and personal key cryptography (PPC) in a protectable manner. Compared to the previous technology, the suggested approach is more effective and valuable technology. The original image is fully restored without any loss at the acceptor end.

Keywords: medical image, public and personal key cryptography method, cryptography, steganography and watermarking.

I. Introduction

Steganography word coming from the Greek for masking and essentially means “to hide in plain sight”. Easy steganographic methods was used for hundreds of years, but with the increasing use of files in an electronic format new approach es for message embed have become possible. Steganography and inscription two technology used to ensure information confidentiality. The major difference between the two is that with inscription anybody can see that both parties are sharing in undercover. Steganography hides the older of undercover message and in the best case nobody can see that two technology parties are sharing in undercover. This concept makes steganography proper match for some concept for which inscription isn’t, like us copyright marking.

Extra incrusted message of a file could easily to delete but hiding it within the file itself can prevent it being easily identified and removed. This paper checks some resent examples of steganography and the general rules behind its usage. This suggested system will discussion of some specific approaches for hiding information in a different of files and the attacks that detecting to steganography. Same time, such process also poses specific challenges to their new idea and design process. A key is often necessary in the embedding system. This key in the format of a public or secret key so you can encode the undercover message with your public key and the recipient can decode it applying your personal key.

In hiding the message this way, you can reduce the chance of a new other party attacker tacking hold of the stego image and extracting it to find out the undercover message. In general the hiding process defuse a mark, M, in an object, I. A key is mansion in the letter K, usually prepare by a random number process is used in the hiding process and the resulting marked object, $\tilde{I}$, is created by the mapping: I x K x M → $\tilde{I}$. They are passed through the encoder; a stego message will be produced. A message is the real masked object with the undercover message embedded inside of the image. This process should look nearly mentioned to the mask object as otherwise a new user attacker can see hiding message. Having produced the message, then it will be send through some networking channel, such as message, to the intended recipient for decoding. The received message must decode the message in order to find the undercover message. The decoding system is the reverse system of the encoding process. It is the taken of undercover message from a image.

In the decoding process, the image is fed in to the decoding system. The public or secret key that can

Author α : Research Supervisor, Manonmaniam Sundaranar University, Tirunelveli. e-mail: santhos1968@gmail.com

Author σ : Research Scholar, Manonmaniam Sundaranar University, Tirunelveli. e-mail: vrsasikumar@gmail.com

be used for decode the original message that is used inside the encoding process is also necessary so that the undercover message can be decoded. Depending on the encoding process, sometimes the original masked object is also needed in the decoding process. Otherwise, there may be no way of decoding the undercover message from the image. finaly the extracting process is finished, the undercover message hiding in the image can then be decoding and viewed. The generic extracting process again requires a public or personal key, K, this time along with a potentially marked object, Ĩ'. Also required is either the mark, M, which is being checked for or the real object, I, and the result will be either the extracting mark from the object or indication of the likelihood of M being present in Ĩ'. Different types of making systems use different inputs image and outputs image.

In particular, squired is crucial to telehealth message due to the fact that medical services may be critical to patients' health or even life. In this paper, we process two safety measure problems in telehealth process in the context of a medical-health portal system. First, a single trust problem came due to the low of visual proofs in telehealth process. For example, a patient may have doubts in the identity of a doctor at the other end of a telehealth service provided via the Internet. The public and personal key (PPC) can enable a patient in establishing real in the organization's website or telehealth process, which is the very famous of PPC by design. However, PPC is sufficient for giving the same kind of real a patient may attain during a face-to-face identification process. Second, telehealth services, such as tele-measurement, usually in a difficult process that normally demands a systematic process of many users playing different roles in finding exchange assets and flows of message.

Digital Image processing is the fast improved area of medical science. The development of image processing was given by the process development like digital visualizing, computer processor and large storage devices. The image itself has an addition image that is mentioned as region of interest which is used to identify the message in the image. Many fields like medicine, sensing, cinema, safety measure monitoring, photography and automatic sensing which are applying the any type of imaging are changing over to digital image because of its conciliatory and significant cost. There is no need of human being to audit the process of deciding which done by the computer. There are other than two levels of image processing rules. At the low level it message of pixel value, for edge detection and de-noising. With these low level results it proceeds from the middle level for resent process like segmentation. And at the next level, it utilizes some methods to extract the useful message for face detection.

II. Literature Survey

a) Relative Honesty of digital medical image without lossless watermarking

DVENTS of multimedia combined with message and communication technology increasing the potential of medical message handling and exchange with applications ranging from telediagnosis to telesurgery and cooperative operating session. At the similar time, these benefits introduce concomitant difficult for exchange electronic patient records and call for more secure message management. Really devoted to medical document Digital Rights operation [1], watermarking has also advance properties that fixed in to the healthcare domain, although the interests at stake are different[1][2][3]. Watermarking is the insertion of a message, also called content or watermark message, in a host document in some multimedia format. It is required that the watermark message remains hidden to any unwanted user (as for information encoding, a personal key is necessary to access the watermark content).

Two main purposed of watermarking are foreseen in the medical domain [1]: information hiding for the purpose of applying meta-information to render the image many usable and message safety with application like honesty control. Despites its attentive, medical watermarking methods may encounter limitations in medical image. The added watermark message quickly alters the original image in an irreversible manner and may mask subtle details. Consequently, suggested problem finding try to preserve the image diagnosis quality value deleting critical message loss. In this paper, we focused to update watermarking image and its role through a difficult process of recent watermarking process in healthcare.

In today's medical world, many process has got digital around us. Even in medical application the older diagnosis is exchange by e-diagnosis [2][1]. Nowadays, transpose of digitized medical message has become very simple due to the availability and generality of network communication. However the digital form of these images can easily be measure and degraded. The problem of copyright safety and medical safety measure poses a big problem to privacy safety applying watermarking approaches. This paper presents a hole work on digital watermarking as an effective technology to protect property correct and decreasing the distribution of medical information [2][1]. In this exiting paper a CT scan of head is taken as original image in which the patient's message and doctor's message together taken as a watermark and incrusted by coding approach called EBCDIC coding approach to enhance the robustness of suggested method. The scheme is blind so that the Electronic patient record can be taken from the medical image without the need of original image. In exiting method is useful for telemedicine applications. The performance of different approaches is calculating by considering the correlation factor for exact recovery of watermark and PSNR for perfect reconstruction of watermarked image. High value of PSNR indicates quality reconstruction of output medical image.

b) Related process of Existing system

Message hiding embeds the information in a masked text. It is also known as message hiding. Information hiding approaches consists of cryptography, steganography and watermarking. To provide information honesty, confidentiality and authentication these process are used [2]. Cryptography is the study of message safety measure [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 message in other message. For hiding the undercover message several steganographic approaches are accessible. Watermarking has more leverage than steganography. It makes the message imperceptible and more robust. Watermarking in medical image is used for storage, transposal and telediagonsis[3][12].

Watermark embeds the confidential information 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 message [21][22]. Comparing to analog format digital image are more secure [16]17].One of the most important approaches in watermarking is digital image watermarking. Digital image embeds and transfers the information in to host image. In other words digital watermarking can be viewed as message hiding or steganography [3][23].

Woo et al [13] introduced wavelet convert for medical image. It consists of physician signature and the message of the patient. This message is diffused into wavelet convert. kobayashi et al[14] upgrade the safety measure of medical image. With the honesty and authenticity stronger link is provided between image and message. Digital Image And Communication In Medicine image are used for development is an added advantage. Kannamal et al [18] exiting medical image with the fragile watermarking rules. Selective bit plane is used and the performance is analyzed. The rule is differentiated with DWT and ICA (Independent component Analysis) methods.

With the limited scope Zain et al [9] suggested reversible watermarking approaches. Zhou et al [11] presents a method for encrypting digital signatures. This method has better authentication and honesty. Coatrieux et al [7] suggested watermarking rule for medical image. In most of the papers embedded message is in the non-ROI region. Eggers et al [6] suggested the symmetric methods with the combination of public detectors. In this approach the watermark is removed simultaneously or it made as unreadable. The secret keys ensure the safety measure.

Hartung and Girod[15] suggested the asymmetric watermark with the spread spectrum of watermarking. Secret Key is used for watermark embedded process. Watermark is verified applying public key and the redundancy made with the secret key.With the Legendre sequences the method is suggested by schyndel et al [5]. Legendre sequences combines with the Fourier convert. Legendre sequences are used as a secret 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 approach.

The integer wavelet convert is used with medical image for information hiding [24].The disadvantage of this fact is it is match only for gray scale image not for color image. Our suggested 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 incrusted applying AES inscription approach. The Same key is used for both inscription and decoding. So it is less secure. In the suggested system the watermarked image is incrusted applying public key cryptography and Riyest,Shamir And Adleman rules to enhance the safety measure during transposal.Riyest,Shamir And Adleman rule are one of the widely used public key rules. In Riyest,Shamir And Adleman rule the image is incrusted applying acceptor public key and decoded applying the secret key. The public key is known to everyone and the secret key is kept undercover. To protect medical image LSB watermarking methods are used for inscription[25].Due to LSB the hidden message is identified easily.

III. Proposed System

a) Digital Watermarking Image Processes

This suggested groundwork for finding the image pattern choosing a given image applying an interpolator that is trained in advance with training information, based on Regular and single vector approach for determining the optimal and compact support for valuable image expansion. Experiments on test information show that learned interpolators are compact yet superior to classical ones. To derived an valuable learning procedure for its parameters on the basis of variation approximation. When plenty of computational assets is accessible, or when the observation process is too severe to recover by mere linear filtering, the complicated image expansion methods will be preferred. In this method, at first we find out the interpolator of the given image. Then replace the low resolution pixel by the interpolator (high resolution pixel).After expanding the image does not scattered. We aim to resolve the tradeoff between high quality and low cost. The process involved in PPC approach consists of the coming steps.

i. In the PPC approach, all users have the key pair of public key and personal key.
ii. The two users, one is transmitter and another one is the acceptor. Transmitter provides the copy of the public key to acceptor.
iii. Acceptor's trust the handler's public key and use it to encrypt the information in the medical image hiding message.
iv. Acceptor sends incrusted information hidden medical image to handler.
v. Handler decrypts the message in the hidden copy of medical image. Secret Key is used.

b) *Digital imaging and communication in medicine image and Regular and single vector Compression*

Watermark is embedded with the use of public key. For the safety measure purpose, in this module the Riyest,Shamir And Adleman rule is used. Riyest,Shamir And Adleman is one of the widely used Public key rules. In RIYEST,Shamir And Adleman rule the image is incrusted applying public key. Digital Imaging and Communications in Medicine is the univeriyest,shamir and adlemanl standard communication for secured medical image.

Digital image are obtained from x-ray, digital radiography, ultrasound and the hospital message system. The original image are completely restored with the digital image. Digital Image and Communication in Medicine file consists of header and the image information. The header associated with the patient name, dimensions of the image and type of the scan. The information elements consist of patient message and hospital message. When the Digital Image and Communication in Medicine file has to authenticated the pixel values must be extracted. Convertation is used to recover the real pixel values. The hidden details of the image are appeared. Digital Imaging and Communications in the Medicine is the univeriyest, shamir and adlemanl standard communication for secured health check image. Digital image are obtained from x-ray, digital radiography, ultrasound and the hospital message system. The original image are completely restored with the digital image. Digital Image and Communication in Medicine file consists of header and the image information. The header associated with the patient name, dimensions of the image and type of the scan. The information elements consist of patient message and hospital message. When the Digital Image and Communication in Medicine file has to be authenticated the pixel values must be extracted. Converiyest,shamir and adlemantion is used to pick up the real pixel values.

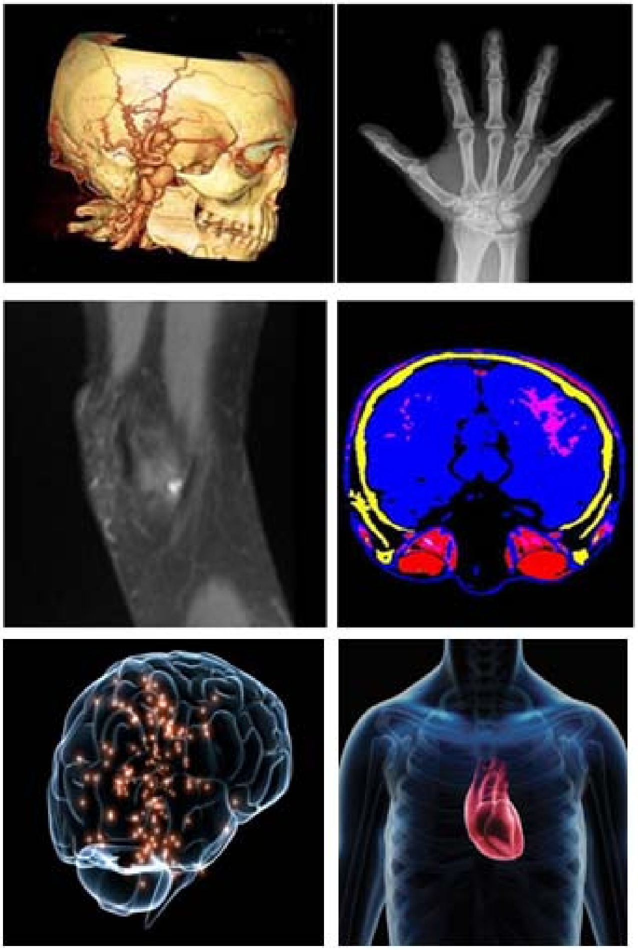


Figure 1: Digital Image and Communication In Medicine image

Fig 1 shows the Digital Image and Communication in Medicine image. This image is compressed applying Regular and single vector. Hash value, Regular and single vector are embedded in the image matrix and it is written again according to the Digital Image and Communication in Medicine standard. For authentication of Digital Image and Communication in Medicine, the image file is extracted then the Regular and single 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 association of pixels has a single value: 1 for R (Regular association), 0 for S (Singular association) and -1 for U (Unused association).

c) *Building Hash value of an digital Image*

Hash value mainly used for message honesty and password validity. Hash value of the image is regulated applying SHA hash function.SHA produces image honesty and patient authentication more advanced than MD5.The SHA hash value, patient id and the compressed Regular and single vector are concatenated to form watermark and it is incrusted applying Riyest,Shamir And Adleman rule be justified, not ragged. The R–S-Vector consists of a stream of bits (zeros and ones). Symbols 4 and 8 are used in the compression process. Each association of pixels has a single value: 1 for R (Regular association), 0 for S (Singular association) and -1 for U (Unused association).It provides sufficient space for hiding the watermark. The compression process depends on the symbols. For compressing the Regular and single vector it must have lossless compression. Then it must contain binate information and random information. The range of hiding the watermark can be findingd by applying R.[18].

$$R=S_R+S_S-|R| \qquad (1)$$

Where S_R is the sum of regular association in the image and S_S is the sum of singular association in the image. |R| is the length of the Regular and single vector. The main aim is to maximize the hiding capacity with the |R| of compressed Regular and single vector.

$$-S_R(S_{R/}S_{R+}S_s)-S_S\log(S_s/S_{R+}S_S)\text{bi ts} \qquad (2)$$

From equation (1) and (2) the real range values(R') can be findingd according to[19].

$$R'=S_{R+}S_{S+}S_R\log(S_{R/}S_{R+}S_S)+S_Sx\log(S_{S/}S_R+S_S) \qquad (3)$$

Two middle pixels of the association(N_R+N_S) increase the value. These are the unique association belong to LSB of both association.

d) Hiding Process

In the hiding process the watermark is deffused into medical image. The watermark message is incrusted applying Riyest, Shamir And Adleman rules to enhance the safety measure during transposal. In Riyest, Shamir and Adleman rule the image is incrusted applying acceptor public key and decrypt the incrusted message applying the acceptor secret key. The public key is made accessible to everyone and the secret key is the undercover key remains confidential. Riyest, Shamir And Adleman rule protects the watermarked image from tampering and eventually applies compression to reduce the size of incrusted watermarked image. Fig 2 shows the watermark hiding process. Then the watermark image is incrusted. The watermark hiding consists of coming steps.

i. The image is partitioned into association. Each association has four pixels with a single value. The state of the association is identified for Regular and single vector.
ii. Regulate and compress the Regular and single vector.
iii. Finding the SHA value of the image. Add the SHA value to the compressed Regular and single vector and patient id to form a watermark.
iv. Encrypt the watermark applying public key.
v. In hiding process the rule achieves image honesty and authentication.

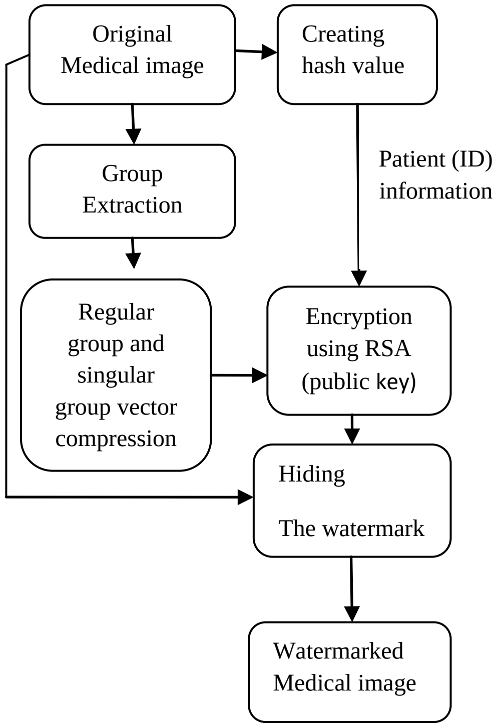

Original Medical image
Creating hash value
Group Extraction
Patient (ID) information
Regular group and singular group vector compression
Encryption using RSA (public key)
Hiding
The watermark
Watermarked Medical image

Figure 2 : Hiding Process

i. *Inscription Applying Riyest, Shamir and Adleman*

The watermark message is incrusted applying Riyest, Shamir And Adleman rules to enhance the safety measure during transposal. In Riyest, Shamir And Adleman rule the image is incrusted applying acceptor public key and decrypt the incrusted message applying the acceptor secret key. The public key is made accessible to everyone and the secret key is the undercover key remains confidential.Riyest, Shamir And Adleman rule protects the watermarked image from tampering and eventually applies compression to reduce the size of incrusted watermarked image. The process consists of the coming steps. In Riyest, Shamir And Adleman rule the key is generated as follows.
Random prime numbers are selected such as a and b.

i. Check a!=b
ii. Evaluate Modulus n=axb
iii. Evaluate z=(a-1)x(b-1)
iv. Select public exponent e,1<e<z
v. Evaluate secret exponent (dxe)modz=1
vi. {n,e}is the public key, d is the secret key.
vii. C=m^emod n(m-message,c-incrusted message)

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

e) Extraction Process

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

i. Extract the incrusted watermark.

ii. Decrypt the watermark image applying acceptor secret key .It remains confidential
iii. Extract the hash value, patient id and Regular and single vector of the watermark image, and then finding 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 fig 3.

f) Decoding Applying Riyest,Shamir And Adleman

Decoding involves the reverse process of inscription. In case of RIYEST,SHAMIR AND ADLEMAN rule, the image is decoded applying acceptor's secret key. Secret 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 safety measure and authentication. The reversible watermark cannot be retrieved by an unauthorized person. This provides the major safety measure in the Human Management System.

IV. Experiential Results

The experiential results of the suggested approach for authentication of medical image based on watermarking approach are discussed in this section. An application is programmed applying C#.NET language to implement this approach. For authentication and honesty, Riyest, Shamir And Adleman is a potential method for medical image. The performance parameters that are represented to measure the performance of the suggested approach are:

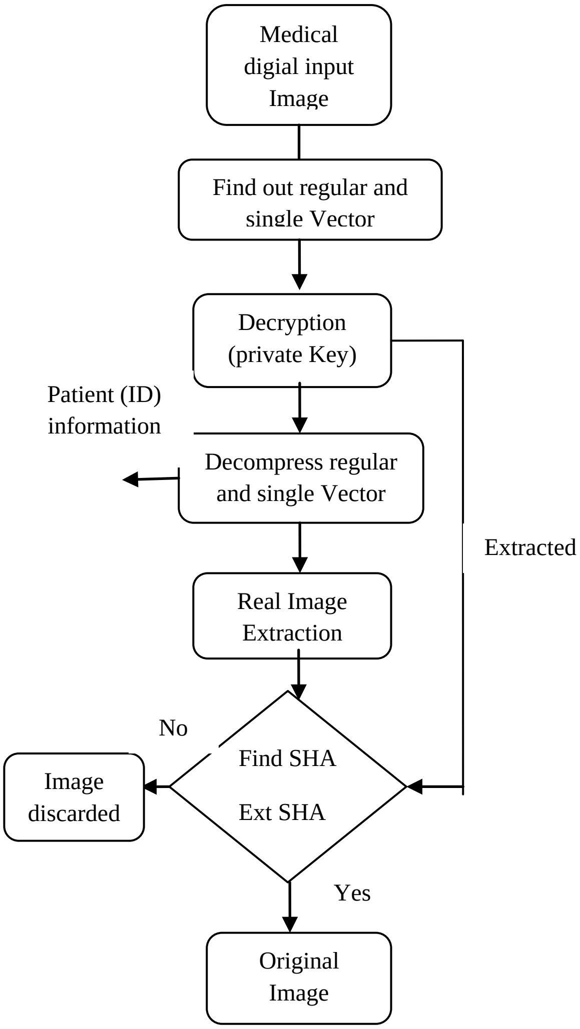


Figure 3 : Extraction Process

Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Bit Error Rate (BER).The original image before hiding the watermark and the authenticated image after hiding the watermark is displayed in Fig 4.

Experiential results shows that PSNR has high range values and it is consistent and the MSE has a least values therefore the quality of the image is not affected.BER is equal to zero for all the four Digital Image And Communication In Medicine image.SNR also has large values. The values predicted in Table 1.

Table 1: Output results of Digital Image And Communication In Medicine grayscale and color medical image

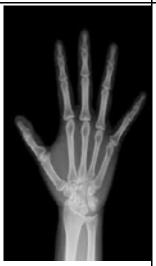
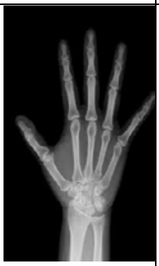
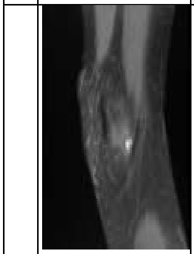
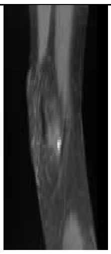
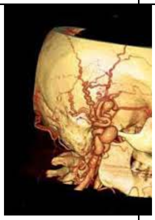
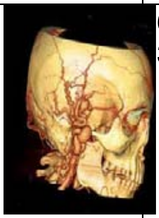
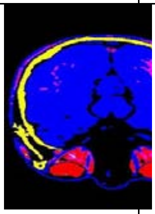
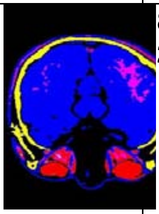
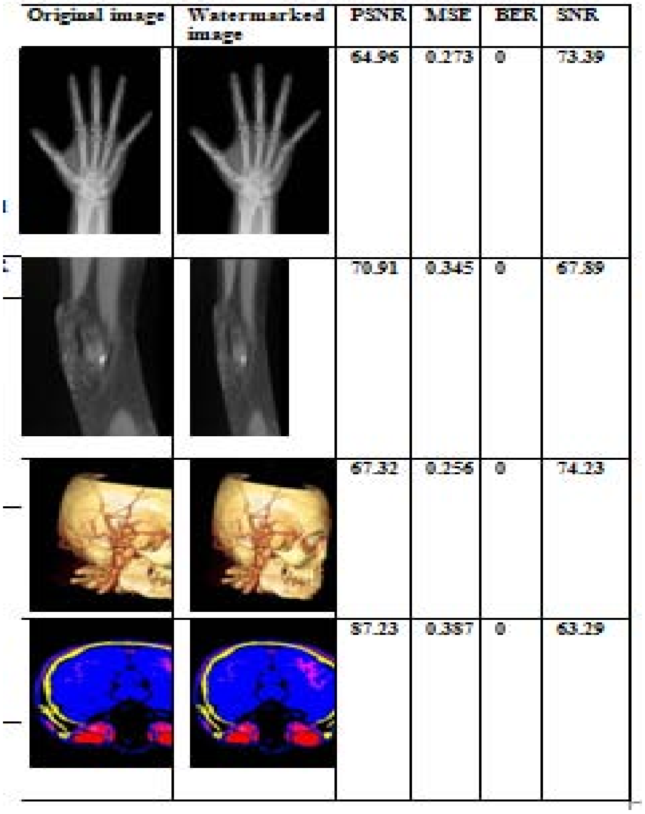
SNo	Original image	Watermarked image	PSNR	MSE	BER	SNR
			64.96	0.273	0	73.39
			70.91	0.345	0	67.89
			67.32	0.256	0	74.23
			87.23	0.387	0	63.29

Table 2 : Output results of grayscale and color test image



Original image	Watermarked image	PSNR	MSE	BER	SNR
		64.96	0.273	0	73.39
		70.91	0.345	0	67.89
		67.32	0.256	0	74.23
		87.23	0.387	0	63.29

The results prove that the suggested approach is totally revertible, and the original image can be retrieved at the acceptor side without any distortion because of the R–S-Vector is extracted without errors. In table 1 and table 2 gray scale image and color medical image are compared with test image of color and grayscale. PSNR and SNR have higher values. In[1] the grayscale and color medical image is similar to the test image of grayscale and color watermark image. In the suggested approach the grayscale and color medical image is different from the test image. Therefore by applying symmetric inscription the performance measurements are consistent. Even though the Public key Inscription has its own undercover key and it is secure they are not consistent in the performance measurements.

V. Conclusion

Based on the Digital Image and Communication in Medicine image the watermarking approach is suggested. This approach is tested with color and grayscale of medical image as well as test image. The hash value based on SHA is regulated from the image. With the patient id, hash value and the compressed Regular and single vector watermark is formed and incrusted applying public key cryptography. Riyest, Shamir And Adleman is a secure public key inscription rule provides message safety measure. The quality measures such as PSNR, SNR, MSE and BER estimates the safety measure of rules. 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 image. As in future work public key cryptography with SHA hash value can be in performed in convert domain for enhancing the safety measure.

References Références Referencias

1. G. Coatrieux, H. Maˆıtre, B. Sankur, Y. Rolland, R. Collorec: Relevance of Watermarking in Medical Imaging. in Proc. of IEEE EMBS Int. Conf ITAB, Arlington, USA, 2000, pp.250-255.
2. X. Q. Zhou, H. K. Huang, and S. L. Lou: Authenticity and honesty of digital mammography image. IEEE Trans. on Medical Imaging,vol. 20, no. 8, pp. 784791, 2001.
3. Mohamed M. Abd-Eldayem.A Suggested Safety measure Approach Based On watermarking and Inscription for Digital Imaging and communications in medicine, Egyptian Message Journal,2012.
4. Secure Watermarking Pattern Applying R-S Sha Vector Rule For Privacy In Medical Cloud. Ishwarya.V, Thamarai Selvan
5. Planitz, B.M., Maeder, A.J.:" A Study of Block-Based Medical Image Watermarking Applying Perceptual Similarity Metric", In: Proceedings in DICTA 2005, p. 70 ,2005.
6. M. Naor, B. Pinkas," Visual authentication and identification", Lecture Notes in Computer Science, vol 1294, pp.322,1997.
7. Xiaoqing Tan, Qiong Zhang," A Kind of Verifiable Visual Cryptography Scheme", International Conference on Emerging Intelligent Information and Web Technologies, 2013.
8. 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.
9. J. J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear converts," in Proc. Eur. Signal Processing Conf:, Tampere, Finland, Sept. 2000.
10. 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.
11. Memon N. Watermarking of medical image for content authentication and copyright protection. PhD thesis, Pakistan: Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology; May 2010.
12. Zain J M, Baldwin L P, Clarke M ,"Reversible watermarking for authentication of Digital Image And Communication In Medicine image", Proc. 26 th Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC 2004) 2: 3237–3240, 2009
13. P. Wong, "A Public Key Watermark for Image Verification and Authentication, "Proceedings of ICIP' 98, pp. 425-429, 1998.
14. Zhou X Q, Huang H K, "Authenticity and honesty of digital mammography image", IEEE Trans. Med. Imag. 20 (no. 8): 784–791,2001.
15. B. Mathon, ''Development of safe watermarking methods for tracing of multimedia contents", International thesis cotutelle, University of Grenoble and of Louvain, 2011.
16. C.S. Woo, J. Du, and B. Pham, Multiple watermark method for privacy control and tamper detection in medical image, WDIC2005 pages, Australia, February, pp. 59–64,2005.
17. L.O.M. Kobayashi, S.S. Furuie, and P.S.L.M. Barreto, Providing Honesty and Authenticity in DIGITAL IMAGE AND COMMUNICATION IN MEDICINE Image: A Novel Approach, IEEE Trans Inform Technol Biomed, 2009.
18. 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.
19. H. M. Chao, C.M. Hsu, S.G. Miaou, "A Information Hiding Approach With authentication,Integration, and Con_dentiality for Electronic Patient Records", IEEE Transactions on Message Technology in Biomedicine, Vol. 6, No. 1, pp. 46-53, March 2002.
20. S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A Secure Information Hiding Approach with Heterogenous Information 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.
21. A. Kannammal, S. Subha Rani, K. Pavithra, "Authentication of DIGITAL IMAGE AND COMMUNICATION IN MEDICINE medical image applying independent component analysis (ICA)", Int J Med Eng Inform 4 ,2012.
22. Dariusz Bogumi," An asymmetric image watermarking scheme resistant against geometrical distortions" Elsevier B.V.2005.
23. B.Nassir, R.Latif, A.Toumanari," Secure transposal of medical image by watermarking approach"IEEE 2012.
24. M. Kutter, "Digital ImageWatermarking: Hiding Message in Image", PhD thesis,University of Rhode Island, Kingston, USA, 1999.
25. C.-T. Hsu, J.-L. Wu, "Hidden Digital Wateramrks in Image", IEEE Transactions on Image Processing, Vol. 8, pp. 58-68, 1999.
26. G.-J. Yu, "Digital Image Watermarking for Copyright Protection and Authentication", PhD Thesis, National Central University, Taiwan, R.O.C, 2001.

27. Memon N, Gilani S. Adaptive information hiding scheme for medical image applying integer wavelet convert. In: IEEE international conference on emerging technologies, Islamabad, Pakistan; 2009.p. 221–4.

28. Bouslimi D, Coatrieux G, Roux C. A joint inscription/watermarking rule for verifying the reliability of medical image: application to echographic image. Comput Methods Programs Biomed 2012; 106 (1):47–54.

This page is intentionally left blank