Enhancing security in medical image informatics using geometrical attacks

A. Umamageswari* and M. A. Leo Vijilious

DMI College of Engineering, Chennai 600 123, India

The objective of this study is to provide security to medical images by embedding medical data (electronic patient record; EPR) along with the images to reduce the bandwidth during communication. Reversible watermarking and digital signature, will provide high security. This application is mainly used in tele-surgery. Only the authorized medical experts can explore a patient's image because of the use of the authentication Kerberos. The proposed study is mainly to restrict unauthorized access to patients' data. Hence medical image authentication may be achieved without biometric recognition such as finger prints, eye stamps, etc. Since the EPR itself contains a patient's entire history, after the extraction process medical experts can identify the patient and also the disease information. In future we can embed the EPR inside the medical image after encryption to enhance security. To improve the authentication, medical expert biometric information can be embedded inside the image in the future. Experiments were conducted using more than 500 (512 × 512) image archives in various modalities from the National Institutes of Health, USA, and Aycan sample digital images downloaded from the internet. Almost all images with greater than 15,000 bits showed 60.4–78.9 dB PSNR value with less alteration in the restored image because of compression, not of watermarking, and the average (number of pixels change rate) was 98.9%.

Keywords: Reversible watermarking, digital signature, medical image compression, security enhancement.

THE word 'Digital Watermarking' was introduced in 1990 (ref. 1), to provide security to medical images. These medical images are utilized in different applications like tele-surgery and tele-diagnosis[2]. One of the key concerns throughout the world is to provide high-quality healthcare to all. The recent advancement in healthcare is based on digital information management, to obtain, handle and transfer medical data.

Electronic patient record (EPR) linked with medical secrecy should be kept confidential during transmission. Medical information of injured patients can be sent to the experts in far of nations to get the opinions and treat the patients' within the vicinity[3]. Unfortunately medical images are transferred through the unreliable open networks which results in undesirable changes in the restorative images. Medical specialists who examine the restorative images from the web must make sure that the medical images have not been altered. Authentication of medical images like ultrasound (US), magnetic resonance (MRI), computed tomography (CT) can be done by hiding the secret message (watermark) identified with the host image embedded within the original image itself[4]. Digital image watermarking is an appropriate technique for medical and military-based applications. In lossless watermarking, the allotted watermark (EPR and security-related data) is inserted into the original image to get the image back from the watermarked one. The recovered watermark can be compared with the original one for authentication.

Digital signature (DS), includes a encrypted hash value where the original image is combined with EPR to create the watermark and embedded inside the original image[5].

Medical image compression

With rapid development in the medical field, medical associations and hospitals need to store huge volumes of digital medical images. Accordingly hospitals and medical associations have high volume of images with them and require tremendous transmission bandwidth for communication[6,7]. The solution to this issue could be the use of compression. Restorative image pressure is particularly essential at present for viable detailing and transmission of images[8]. Image compression can be named lossy and lossless. Medical images do not require lossy compression because of the accompanying reasons. The principal reason is the wrong judgment because of the loss of valuable data. The second reason is the operations like image upgrade may underline the debasements created by lossy compression. Lossy compression is by all accounts unavoidable. Anyway lossless compression is reversible and it changes only minimum amount of bits in original image and accordingly speed up the transmission and minimizing storage requirements.

Reversible watermarking

Reversible watermarking has an important feature that the principal computerized watermark can be completely

*For correspondence. (e-mail: r.umaramesh@gmail.com)

restored[9]. This component is appropriate for some basic media, for instance, restorative and military images, because these media do not allow any damage/misfortunes. The targets of lossless watermarking are to anchor the copyrights and obtain the first image. We are at the basic level with two designs in reversible or lossless watermarking, viz. spatial area and transform space strategies. Spatial space is useful for restorative image watermarking. It underpins two designs: (i) additive inclusion and (ii) substitutive insertion (LSB method)[10].

In additive plan the watermark w to be embedded will be embedded into the first image (host). $Iw = I + w$ (it is completely in view of signals). The methodology for embedding the watermark in the spatial region is to add pseudo arbitrary commotion guide to the intensity of image pixels. In substitutive insertion, the essential LSB plan uproots the pixels slightest noteworthy bit by bit of the message to be inserted. The system depends on the control of LSBs of images, in a way which is imperceptible and tangible to human eyes. The LSB substitution technique is exceptionally easy to realize and does not create any significant damage in the watermarking image.

Regions of interest and non-interest

The watermark to be embedded should not disturb the Region of Interest (ROI) as the ROI is important for diagnosis purpose. Normally in medical images, the entrenching region is a dim area with pixel values = 0. This feature will not be considered to create reversible or inversible watermarks. In medical images, the region of non-interest (RONI) generally contains a black background which surrounds ROI. However, depending upon the selection of ROI decided by the medical experts, RONI may contain some grey portion, thus increasing the capacity for embedding information[11,12]. Usually there is less interference with the image content belonging to the RONI area; therefore unnoticeable area is not taken into account, so a larger payload can be embedded[13].

DS and EPR are inserted in RONI using modified lossless difference of expansion method. In a medical image area which has not used for diagnosis, RONI is watermarked, leaving ROI for diagnosis by the medical experts[14]. In the event that we insert the watermark in a vital region, the data will get distorted.

Role of digital signature

Utilization of cryptographic hash function provides the integrity control of images. Hash functions are generally used to create a DS to provide authentication for the information to be transmitted. These methods are restricted hash functions (i.e. non-reversible), and from a message of self-assertive length they give a fixed length process or resume[15]. The RSA (Rivest–Shamir–Adleman) computation is the most comprehensively used public key cryptographic structure[16].

Digital imaging and communications in medicine (DICOM) is the standard reference for restorative image stockpiling and sharing; there exists a DS rundown dependent on RSA. This outline is joined with the hashing capacities to produce a message digest (MD), which is scrambled utilizing a private RSA key. The DICOM image contains this DS in the header. Watermarking a cryptographic hash value inside a restorative image prompts the dependability control process[17]. With such a scheme, any modification will give an indication similar to lossy image compression and the reversible property of the scheme allows hash updates by distortion.

Importance of digital watermarking

Digital watermarking has some interesting favourable situations for medical image communication. Cryptographic/perceptual hashing has no impact on nature of the host flag, and is appropriate for inheritance content. It is either bit-sensitive (for cryptographic hash capacities) or needs access to a central database to filter for a match with a pre-registered hash (for perceptual hashing). However, an exactly created watermarking plan does not change the medical data[18] and the recommended three approaches to overcome the distortion are prompted in images by watermark embedding[19].

Memon *et al.*[20], proposed a digital watermarking plan, in which watermark is embodied patient data, clinic logo, and message authentication code, registered hash function, for some reason, Li-Qun *et al.*[21] presented digital signature algorithm (DSA) in view of RSA public cryptosystem, incorporating reversible watermarking with advanced signature as authentication framework.

Zain *et al.*[18], proposed that inserting watermark in clinical data creates distortion in ROI and makes diagnosis profligate. Differentiating ROI and RONI is difficult, in spite of the fact that is connected with few watermarking plan[22]. Moreover, creating reversible watermarking guarantees medical image application with no danger for relinquishing the analytic precision, although computational properties may cause extra complications. A compression system is utilized for accessing the embedding limit necessities of watermarking. A watermarking strategy which applies zero-tree wavelet (EZW) compression algorithm[23] on first image of CT and MRI uses Huffman encoding and Rivest Cipher4 (RC4) encryption algorithm for compression and encryption to scramble the metadata in the watermarking plan[24].

Enhancing security in open network

When medical images (DICOM) are streamed over an open system, at present secure socket layer (SSL) is

utilized to secure the images in picture archiving environment in communications (PACs) environment. More upgrades are expected to enhance the authentication, privacy and integrity. Kerberos is protected to give secure authentication over a conceivably unstable system.

For confirmed target administration, the medical expert must give its username and password to the framework[25]. At the point when the medical expert endeavours to utilize a specific target benefit, the client sends a ticket request to the Kerberos ticket granting server. Then Ticket Granting Authority (TGA) uses its secret key to decode the ticket granting ticket (TGT) in the appeal and the session key in TGT for decryption. The client decodes the ticket utilizing the given session key, to yield the server session key and an encoded service ticket. The medical expert can then access the embedded medical images at the sites through this ticket generated by TGT. Figure 1 shows the involvement of Kerberos in authentication for this clinical environment.

Quality measures

The proposed method has been evaluated using parameters like compression ratio (CR), peak signal-to-noise ratio (PSNR), normalized correlation coefficient (NCC) and number of pixel changing rate (NPCR).

$$\mathrm{CR} = \frac{\text{Size of the original image}}{\text{Size of the compressed image}}. \quad (1)$$

The ratio between the sizes of the images before and after compression is the compression ratio. PSNR is the important parameter to measure the quality of the watermarked image. If the PSNR value is extraordinary then the quality of output image will be good. The PSNR value for an image of size $M \times N$ is:

$$\mathrm{PSNR}(I, Iw) = 10 \log_{10}((2^p - 1)^2 \mid \mathrm{MSE}), \quad (2)$$

$$\mathrm{MSE} = \frac{1}{MN}\left[\sum_{i=0}^{M}\sum_{j=0}^{N}[\tilde{f}(m,n) - f(m,n)]^2\right], \quad (3)$$

where $f(m, n)$ is the representation of an original image in pixel grey level values and $\bar{f}(m, n)$ is used to represent the pixel grey level values of watermarked image. PSNR value is based on the capacity rate (watermark size). The NCC is used to measure the similarity between the original image W and the watermarked image W^1.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i, j) \times 100\%}{W \times H}, \quad (4)$$

$$\mathrm{NCC} = \frac{\sum_j \sum_k W(j,k) * W^1(j,k)}{\sum_j \sum_k W(j,k) * W^1(j,k)}. \quad (5)$$

Method

Transmission of medical images is utilized as a part of different applications like tele-surgeries, and tele-diagnosis bureau of tele-medicine[2]. Security can be achieved in PACs environment and hospital information system (HIS) utilizing DICOM security gauges as indicated by the Health Insurance Portability and Accountability Act (HIPAA), USA.

Basically, injured patients can be dealt within the vicinity itself, by transferring medical images to hospitals found in distinctive nations to provide good treatment to the patients by getting opinions from medical experts[3,20]. It is necessary to provide security to the medical images with patient information while transferring in an open network; so digital watermarking can be used to improve the medical image security[6].

DS calculations are basic in securing confidential data[26]. To generate DS, hash value of the input medicinal image is calculated and it is encrypted to provide the authentication and integrity to the medical image which is shared through the open network[26].

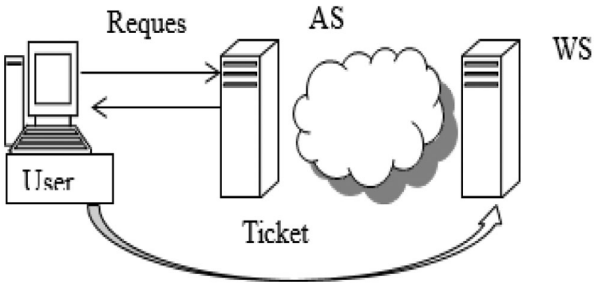

Figure 1. Involvement of Kerberos. AS, Authentication server; WS, web server.

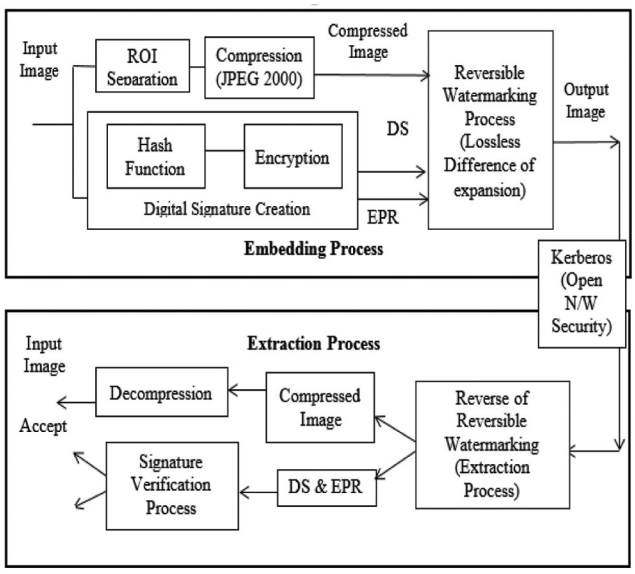

Figure 2. Architecture diagram.

System architecture

Figure 2 shows the architecture diagram for embedding and extraction process of the entire study.

Generation of digital signature

Encrypted hash value will be the DS. The hash value is generated using additive hash function (AHF) algorithm and it is scrambled using existing RSA to generate the DS.

Additive hash function: This study proposes a novel algorithm for the hash value of an image known as additive hash function (AHF). It accepts the first pixel row as the input image and applies some confusions and diffusions mathematically to generate a fixed length hash value of only 128 bits.

Step 1: The first row of the image will be taken as separate table from the converted 512×512 pixel mapped table (512 elements = 8192 bits).
Step 2: Separate it into four divisions namely $a1$, $a2$, $a3$ and $a4$, each of 128 elements (128 elements = 2048 bits).
Step 3: Add alternative sets. $b1 = a1 + a3$; $b2 = a2 + a4$.
Step 4: Subtract $b1$ from $b2$, hash2048 = $b2 - b1$.
Step 5: Split hash2048 into eight parts, namely $c1$, $c2$, $c3$, $c4$, $c5$, $c6$, $c7$ and $c8$.
Step 6: Add alternatives, each value of hash contains 16 elements = 256 bits.

Hash1 = $c1 + c5$, Hash2 = $c2 + c6$,
Hash3 = $c3 + c7$, Hash4 = $c4 + c8$.

Step 7: To provide confusion and diffusion, subtract and add the alternative values of Hash.

HFinal1 = $H3 - H1$, HFinal2 = $H4 + H2$.

Step 8: Add HFinal1 and HFinal2 to obtain the Final Hash256 value.

The additive hash value,

AHValue = HFinal1 + HFinal2;

AHF contains 16 elements = 256 bits.

AHValue will be encrypted using RSA algorithm to generate DS.

Lossless modified difference of expansion

Watermark is the combination of DS and EMR. It is embedded in a medical image using the lossless modified difference of expansion method. This algorithm creates little changes in an original image by embedding watermark inside an image[27]. At that point we grow the created qualities to embed the bits of watermark.

Embedded value = $h^1 = 2 \times h + b$,

where h^1 is the pixel after embedding process, h the pixel of the original image and b is the watermark.

Using the modified values, the watermarked image is reconstructed. Figures 3 and 4 show examples of the embedding and extraction process. In a grey-scale image for a pair of pixels (x, y), $0 \le x, y \le 255$, define average A and their difference D as

$$A = [(x + y)/2], \tag{6}$$

$$D = x - y, \tag{7}$$

x and y are considered as two adjacent pixels.

Results and discussion

This methodology is implemented with Matlab 2009b and C# .NET for image processing and Java for networking implementation. Medical images of $512 \times 512 \times 16$ have been taken for evaluation with different modalities. These images are taken from Aycan database.

Proposed method (work I)

Table 1 shows the PSNR of proposed and existing techniques. Beyond reliability control, the goal is to embed

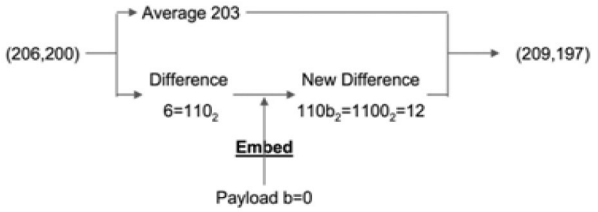

Figure 3. Example of embedding process.

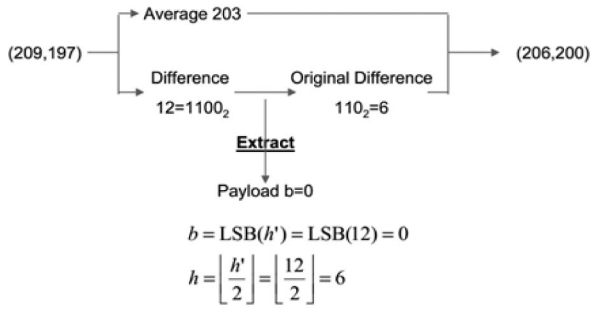

Figure 4. Example of extraction process.

Table 1. PSNR of proposed and existing work 1

Grey images	PSNR (dB)		
	Proposed method (AHF + RSA + lossless watermark)	Existing methodology (2009; MD5 + RSA + LSB)	Existing methodology (2014; MAC + MD5 + LSB)
1	74.21	58.77	73.12
2	72.02	55.46	70.37
3	69.13	53.23	69.22
4	78.32	68.84	66.98
5	76.17	67.72	66.45

Table 2. PSNR and NPCR of proposed and existing work

MRI image	Pay load (bpp)	PSNR (dB)			NPCR (%)
		Proposed method	Existing method	Existing method	
1	0.5	72.32	68.84	51.91	98.5
2	0.5	71.27	67.72	50.31	99.8
3	0.5	68.02	64.02	49.67	99.7
4	0.5	71.12	58.77	48.62	99.8
5	0.5	70.02	55.46	49.61	99.7
6	0.5	69.13	53.23	52.74	99.7
7	0.5	68.75	49.32	51.76	98.6

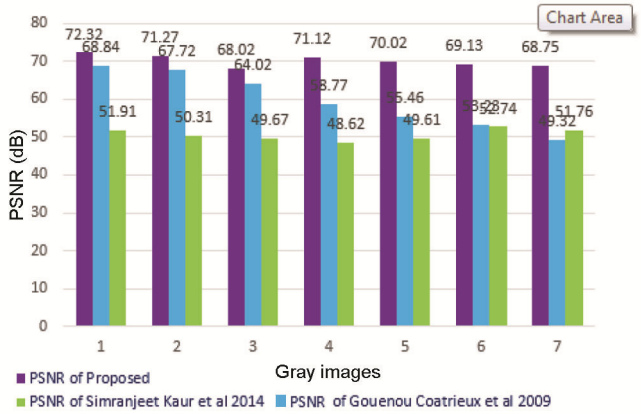

Figure 5. PSNR of proposed and existing in CT, US and MRI images with respect to payload.

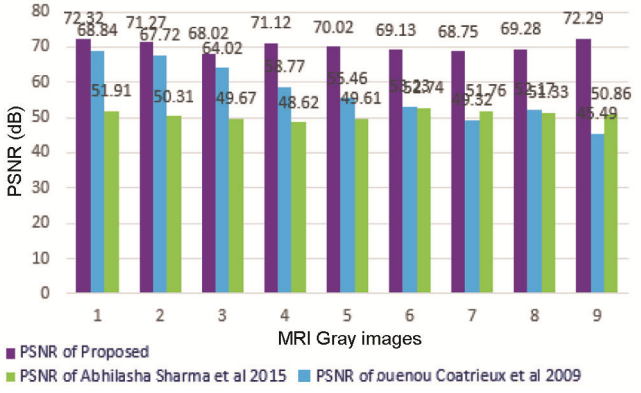

Figure 6. Comparative results of PSNR for proposed and existing (work II) methods for MRI grey images.

a large volume of information into a medical image with less distortion. The table shows that the proposed method has given better results for PSNR value compared to the existing method[28,29]. The proposed method achieved 78.32 dB as PSNR value, which is high compared to existing methods[28,29], which achieved only 68.84 dB as maximum PSNR value.

The proposed method gives 0.4329 bpp/69.02 dB for US images, 0.3432 bpp/78.32 dB for MRI images, and 60.75 dBs/0.55 bpp for CT images. This method produced maximum 78.9 dB to minimum 60.4 dB as the PSNR value, with less alteration in the reconstructed image for almost all medical images with an embedding size of 15,000 bits; that too not of watermarking because of JPEG2000 compression. Figure 5 is a graphical representation of PSNR of existing and proposed methods in CT, MRI and US with respect to payload.

Proposed method (work II)

The PSNR values of proposed and existing methods were compared with nine MRI grey images when capacity was 0.5 bpp. Table 2 shows the comparative results. The parameter PSNR and NPCR improved in the proposed work because PSNR was up to 68.84 dB in the existing method but in the proposed work, it was up to 72.32 dB. Almost all medical images with watermark size of 64×64 bi-cubic images achieved the PSNR value of 68.02–78.32 dB.

Table 2 shows that the suggested method gives a improved PSNR value than present (Figure 6).

Table 3. PSNR and existing (work methods III) proposed algorithm

Sample images	PSNR (dB)			
	Pan *et al.*[21]	Md. Moniruzzaman *et al.*[17] LSB + ACM	Rupali Bhardwaj[23]	Proposed method
1	51.2	51.14	51.76	54.78
2	53.1	51.113	57.50	59.28
3	48.2	51.20	58.09	58.52
4	50.4	48.44	51.54	54.45

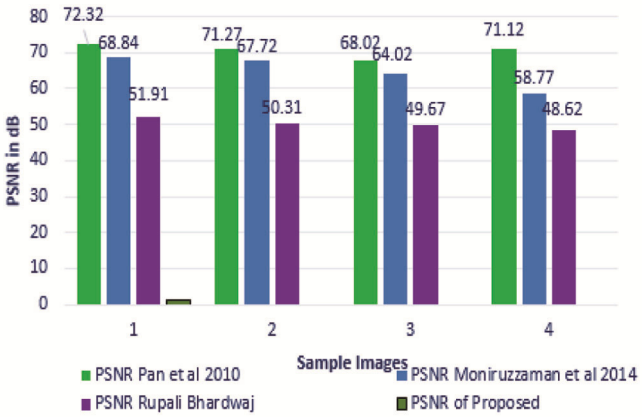

Figure 7. Comparative results of PSNR for the proposed and existing methods.

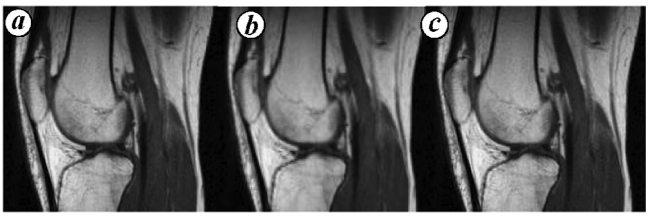

Figure 8. ***a***, Input image. ***b***, output/watermarked with PSNR 75.6 dB. ***c***, wavelet compressed image with PSNR 69.2 dB.

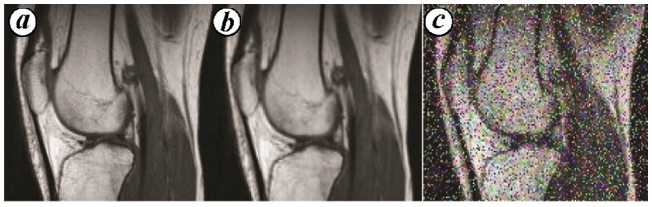

Figure 9. ***a***, Input image. ***b***, output/watermarked image with PSNR 75.6 dB. ***c***, Salt-and-pepper noise 40% attacked image with PSNR of 62.9 dB.

Proposed method (work III)

Table 3 shows the PSNR, NPCR and CR of four images considered in the proposed method III. PSNR value was better in the proposed method (59.28 dB). This is applicable for all the images used.

Figure 7 is a graphical representation of the result of the proposed method. PSNR esteem in existing system is just 58.09 dB; however, in the proposed method it is 59.28 dB. It is appropriate for images used for the proposed work and also Table 3 shows the comparison of PSNR of existing and proposed method[4,30,31]. PSNR values of the proposed method is better than the existing method. NPCR is over 99%. It implies that the proposed encryption plan is delicate for little changes in the key. Cryptanalysis like chosen cipher text attack, known plain text attack, differential attack and brute force attack is not possible with the suggested algorithm.

Evaluating robustness with geometrical attacks

The power of proposed calculation has been assessed with different geometrical assaults. The medicinal image is subjected to different geometrical attacks.

Effect of compression attack

The original MRI knee image of size $512 \times 512 \times 16$ was watermarked with a capacity of 0.5 bpp and tested with wavelet compression attack and extracted watermark without any attack and distortion in the receiver side with PSNR value of 69.2 dB. Even though the compression rate was found to increase; there was no rapid change in the extracted watermark. Figure 8 shows the original image, watermarked image with PSNR value of 75.6 dB, and watermarked compressed images with PSNR value of 69.2 dB. The proposed method gives 99.23 as the NCC value, which is greater than that of the existing method (98.99).

Effect of salt-and-pepper noise

Figures 9 and 10, and Table 4 show an analysis of PSNR and NCC values of the tested images after salt-and-pepper noise attack.

The output image starts to get distorted if geometrical attack is tested with 40% of salt-and-pepper noise. Figure 10 shows that the proposed method gives better PSNR and NCC values compared to the existing method.

Table 4. Comparison of salt-and-pepper noise results

Percentage of noise attack	PSNR (dB) of proposed method	PSNR (dB) of existing method	% NCC of proposed method	% NCC of existing method
10	62.9	21.59	99.56	91.25
25	62.5	17.65	99.47	83.18
50	61.9	14.64	99.48	72.03
75	62.3	17.82	99.40	65.02

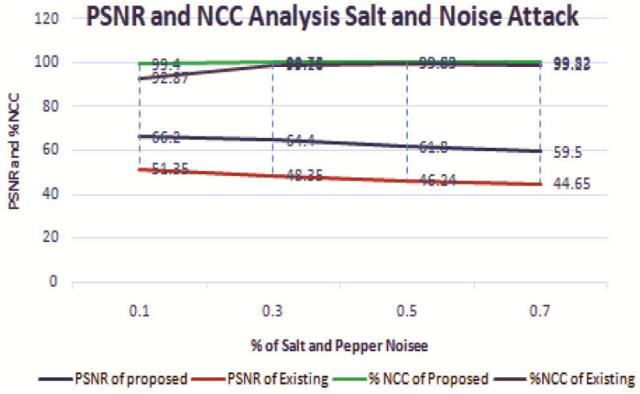

Figure 10. Comparison of salt-and-pepper noise attack results.

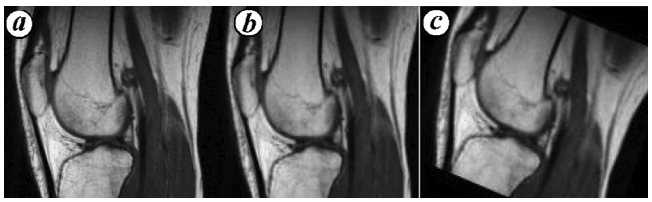

Figure 11. ***a***, Original image. ***b***, Watermarked image with PSNR 75.6 dB. ***c***, Rotated image 20° with PSNR 66.7 dB.

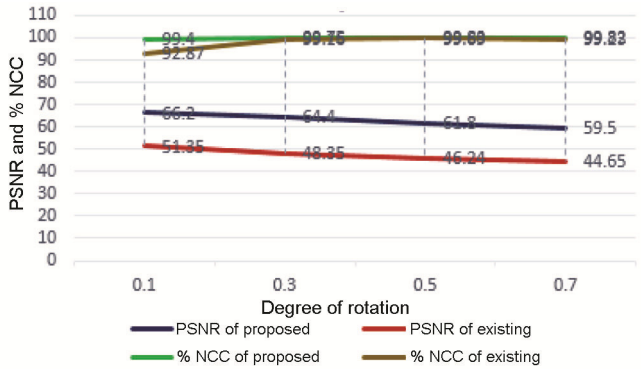

Figure 12. Comparison of rotation attack results.

Effect of rotation attack

The outcomes show that the proposed method is robust to rotation attack. Figure 11 shows a comparison of various degrees of rotation of existing and proposed methods. Table 5 summarizes the results. The graphical representation (Figure 12) shows that the proposed method performs better than the existing method.

Effect of cropping attack

The new outcomes show that the proposed algorithm is more robust against cropping attack (Figure 13).

A comparison of various cropping attacks of the existing and proposed methods has been made. Table 6 summarizes the results and Figure 14 is a graphical representation of the same. The figure depicts that the proposed method performs better when compared to the existing method.

Effect of scaling attack

The new outputs show that the algorithm is robust to scaling attack (Figure 15) with 50% scaling of input image with PSNR value of 61.8 dB.

A comparison of various scaling factors of the existing and proposed methods was done. Table 7 summarizes the results and Figure 16 is a graphical representation of the same. The figure depicts that the proposed method performs better when compared to the existing method. The proposed method is robust to compression, cropping, scaling, salt-and-pepper noise and rotation attacks from the experimental results.

Real-time applications

EPR management is a web application used to gather information on patients' health right from the medicines prescribed. This provides separate portals for patients, doctors, pharmacy and laboratory. Using the information, medical experts can analyse the health details of a particular patient and share them during tele-surgeries in a secured manner. The patient can view his/her health information using Aadhar ID. EPR management simply streamlines the information gathering processes in the organization. Right from creating patient data for performing case management and recording the patient's medical history, this module captures every bit of medical and surgical information about any patient at the entry level. For better accessibility and efficient information

Table 5. Comparison of rotation attack results

Degree of rotation	PSNR (dB) of proposed method	PSNR (dB) of existing method (2014)	% NCC of proposed method	% NCC of existing method (2014)
10	65.9	20.98	99.40	98.75
20	66.7	19.43	99.75	98.83
50	66.1	18.92	99.52	98.72
70	66.3	19.22	99.51	98.84

Table 6. Comparison of cropping attack results

Percentage of cropping	PSNR of proposed method (dB)	PSNR of existing method (dB)	% NCC of proposed method	% NCC of existing method
10	64.2	24.42	92.1	91.25
25	64.6	20.04	91.5	83.18
50	64.9	16.73	91.1	82.03
75	64.5	14.89	89.9	83.23

Table 7. Comparison of scaling attack results

Scaling factor	PSNR of proposed method (dB)	PSNR of existing method (dB)	% NCC of proposed method	% NCC of existing method
0.1	66.2	51.35	99.40	92.87
0.3	64.4	48.35	99.75	99.16
0.5	61.8	46.24	99.83	99.69
0.7	59.5	44.65	99.82	99.23

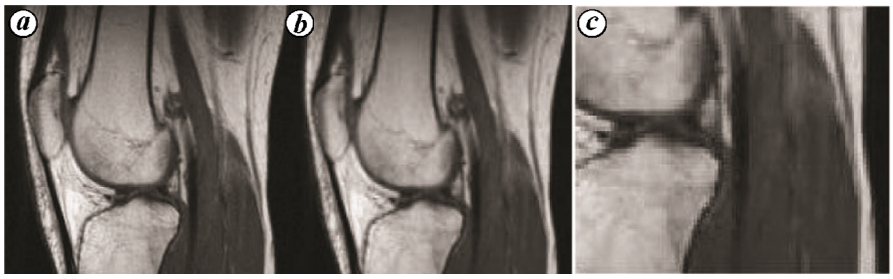

Figure 13. ***a***, Input image. ***b***, output/watermarked image with PSNR 75.6 dB. ***c***, 25% cropped image with PSNR 64.6 dB.

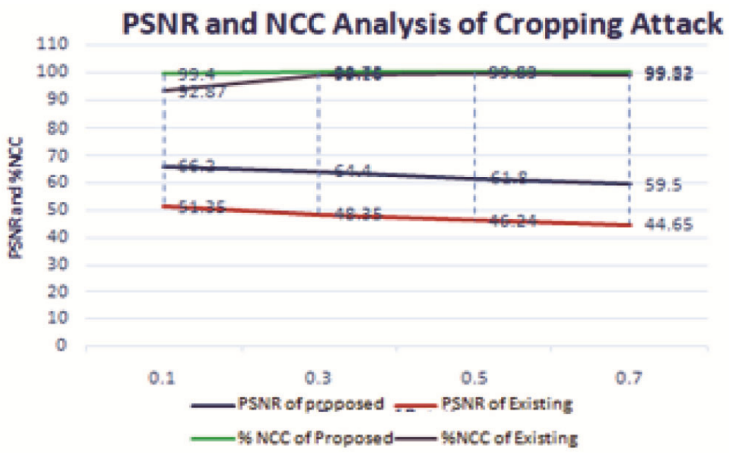

Figure 14. Comparison of cropping attack results.

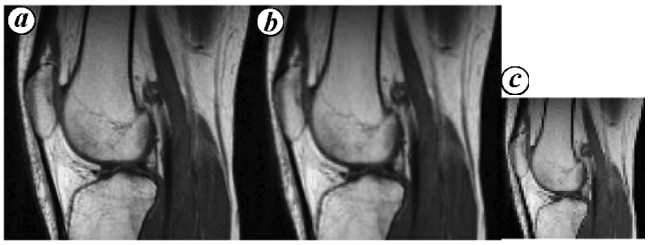

Figure 15. ***a***, Input image. ***b***, output/watermarked image with PSNR 75.6 dB. ***c***, 50% scaled Image with PSNR 61.8 dB.

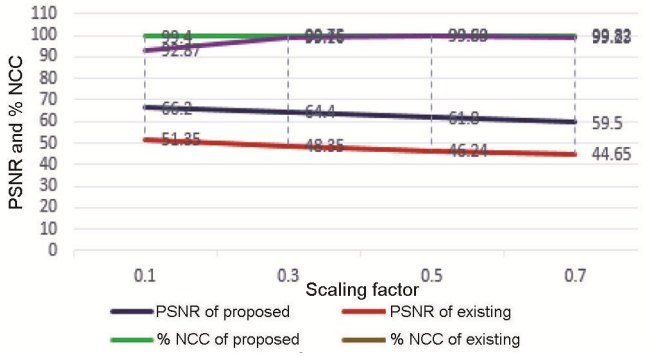

Figure 16. Comparison of scaling attack results.

processing, this project integrates with every imperative unit. It also captures information such as patient's prescription, tests to be performed, information about test reactions, past test records and current test reports. For user convenience, this system has been designed using the latest technology and ground-breaking ideas. This application provides an improved electronic version of public health repository management system to administrate the clinical data by the service providers.

Conclusion

The security system for medical images based on digital lossless watermarking scheme to achieve higher authentication, integrity and reliability was executed and checked with different types of algorithms. The proposed method achieved authentication, integrity and reliability of medical image by using AHF and RSA methods. Since it requires secret key for both embedding and extraction process, it gives better authentication to medical images. Kerberos algorithm was used in web server to authenticate the medical images. The proposed method provide precise recovery of original image in the receiver side, are proves to be robust according to thorough experiments with various properties. The proposed system is effective for medical images in the sense that it is able to completely recover the original image at the receiver end after authenticity of an image is verified. In future same methods can be applied for colour medical images.

1. Komatsu, N. and Tominaga, H., A proposal on digital watermark in document image communication and its application to realizing a signature. *Trans. Inst. Electron. Inf. Commun. Eng.*, 1990, **73**(5), 22–33.
2. Lehmann, T. *et al.*, Content based image retrieval in medical applications. *Methods Inf. Med.*, 2004, **43**(4), 354–361.
3. Osbarne, D., Rogers, D., Muzumdar, J., Coutts, R. and Abbott, D., An overview of wavelets for image processing for wireless applications. In Proceedings of SPIE Smart Structures Devices and Systems, University of Melbourne, Australia, 2009, vol. 4935, pp. 427–435.
4. Pan, W., Coatrieux, G., Cuppens Boulahia, N., Cuppens, F. and Roux, Ch., Medical image integrity control combining digital signature and lossless watermarking. *Lecture Notes Comput. Sci.*, 2009, **5939**, 153–162.
5. Umamageswari, A. and Suresh, G. R., Security in medical image communication with Arnold's cat map method and reversible watermarking. In Proceedings of IEEE International Conference on Circuits Power and Computing Technologies, Noorul Islam University, Nagercoil, 21–22 March 2013, pp. 1116–1121.
6. Micheal, W. Marcellin, Micheal, J., Garmish, Ali Bilginand Martin Bolick, P., An overview of JPEG2000. In Proceedings of IEEE Data Compression Conference, Snowbird, UT, USA, 2009, pp. 523–541.
7. Miaou, S.-G., Ke, F.-S. and Chen, S.-C., A lossless compression method for medical image sequences using JPEG-LS and interframe coding. *IEEE Trans. Inf. Technol. Biomed.*, 2005, **13**(2), 236–251.
8. Padmaja, G. M. and Nirupama, P., Analysis of various image compression techniques. *ARPN J. Sci. Technol.*, 2009, **2**(4), 371–376.
9. Feng, J.-B., Lin, I.-C., Tsai, C.-S. and Chu, Y.-P., Reversible watermarking: current status and key issues. *Int. J. Network Security*, 2006, **2**(3), 161–170.
10. Lin, C. Y. and Chang, C. F., A robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Trans. Circuits Syst. Video Technol.*, 2004, **11**(2), 153–168.
11. Moniruzzaman, M., Hawlader, M. A. K. and Hossain, M. F., An image fragile watermarking scheme based on chaotic system for image tamper detection. In IEEE International Conference on Informatics, Electronics and Vision, Kitakyushu, Fukuoka, Japan, 2014, pp. 1–6.
12. Shih, F. Y. and Wu, Y. T., Robust watermarking and compression for medical images based on genetic algorithms. *J. Inf. Sci.*, 2005, **175**(3), 200–216.
13. Coatrieux, G., Sankur, B. and Maitre, H., Strict integrity control of biomedical images. In Proceedings of Electronic Imaging, Security and Watermarking of Multimedia Contents, SPIE, USA, 2001, pp. 229–240.
14. Wakatani, A., Digital watermarking for ROI medical images by using compressed signature image. In 35th Annual Hawaii International Conference on System Sciences, Computer Society Washington, DC, USA, 2002, pp. 2043–2048.
15. Gilbert, H. and Schuh, H. H., Security analysis of SHA-256 and Sisters, Selected Areas in Cryptography, 2003, pp. 175–193.
16. Rivest, R., Shamir, A. and Adleman, A., A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM Trans.*, 1978, **21**(2), 120–126.
17. Zain, J. M., Baldwin, M. P. and Clarke, M., Reversible watermarking for the authentication of DICOM images. In Proceedings of 26th IEEE Engineering in Medicine and Biology Society, EMBS Annual International Conference, San Fransico, USA, 2004, pp. 3237–3240.
18. Zain, J. M., Fauzi, A. R. M. and Aziz. A. A., Clinical assessment of watermarked medical images. *J. Comput. Sci.*, 2009, **5**(11), 857–863.

19. Kundu, M. K. and Das, S., Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. In Proceedings of the 20th International Conference on Pattern Recognition, 2010, pp. 1457–1460.
20. Memon, N. A., Gilani, S. A. M. and Ali, A., Watermarking of chest CT scan medical images for content authentication. In Proceedings of the International Conference on Information and Communication Technologies, Karachi, Pakistan, 2009, pp. 175–180.
21. Li-Qun, K., Yuan, Z. and Xie, H., A medical image authentication system based on reversible digital watermarking. In Proceedings of the International Conference on Information Science and Engineering, Qatar University, Doha, Qatar, 2004, pp. 1047–1050.
22. Badran. E. F., Sharkas, M. A. and Attallah. O. A., Multiple watermark embedding scheme in wavelet spatial domains based on ROI of medical images. In National Radio Science Conference, New Cairo, Egypt, 17–19 March 2009, pp. 1–8.
23. Nambakhsh, M. S., Ahmadian, A., Ghavami, M., Dilmaghani, R. S. and Karimi Fard, S., A novel blind watermarking of ECG signals on medical images using EZW algorithm. In Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS, New York City, USA, 2006, pp. 3274–3277.
24. Zhang, C., Wang, J. and Wang, X., Digital image watermarking with double encryption by Arnold transform and logistic. In Fourth International Conference on Networked Computing and Advanced Information Management, Seoul, South Korea, 2008, pp. 329–334.
25. Stallings, W., Cryptography and Network Security, 2010.
26. Guo, X. and Zhuang, T., A lossless watermarking scheme for enhancing security of medical data in PACS, medical imaging PACS and integrated medical information systems design and evaluation. The International Society for Optical Engineering, San Diego, CA, USA, 2003, pp. 350–359.
27. Tian, J., Reversible data embedding using a difference of expansion. *IEEE Trans. Circuits Syst. Video Technol.*, 2008, **13**(8), 890–896.
28. Coatrieux, G., le Guillou, C., Cauvin, J. and Roux, Ch., Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE Trans. Inf. Technol. Biomed.*, 2009, **13**(2), 158–165.
29. Kaur, S., Kaur, S. and Singh, B., Data hiding technique for secure transmission of medical images. *Int. J. Innov. Res. Adv. Eng.*, 2014, **1**(8), 157–162.
30. Sharma, A., Singh, A. K. and Ghrera, S. P., Secure hybrid robust watermarking technique for medical images. *Proc. Comput. Sci.*, 2015, **70**(1), 778–784.
31. Bhardwaj, R. and Khanna, D., Enhancing the security of image steganography through image encryption. In Proceedings of the Annual IEEE India Conference, Delhi, 2015, pp. 1–4.

Received 2 December 2017; revised accepted 29 April 2019

doi: 10.18520/cs/v117/i3/412-421