Puvvadi Aparna* and Polurie Venkata Vijay Kishore

A Blind Medical Image Watermarking for Secure E-Healthcare Application Using Crypto-Watermarking System

https://doi.org/10.1515/jisys-2018-0370
Received September 12, 2018; previously published online August 27, 2019.

Abstract: A reliable medical image management must provide proper security for patient information. Protecting the medical information of the patients is a major concern in all hospitals. Digital watermarking is a procedure prevalently used to secure the confidentiality of medical information and maintain them, which upgrades patient health awareness. To protect the medical information, the robust and lossless patient medical information sharing system using crypto-watermarking method is proposed. The proposed system consists of two phases: (i) embedding and (ii) extraction. In this paper, we securely share three types of patient information, medical image, electronic health record (EHR), and face image from one hospital to another hospital. Initially, all the three inputs are encrypted and the information is concordant. In order to enhance the robustness of the crypto-watermarking system, the obtained bit stream is compressed, and the compressed bit streams are embedded into the cover image. The same process is repeated for the extraction process. The experimentation result is carried out using different medical images with EHR, and the effectiveness of the proposed algorithm is analyzed with the help of peak signal to noise ratio.

Keywords: Crypto-watermarking, electronic health record, SHA-256, embedding, extraction, face image, advanced encryption standard (AES), segmentation and active contour.

1 Introduction

During the last few years, the medical information of the patient is transferred from one doctor to another doctor for better health solution and treatment. It becomes a challenge to make a distinction between the original content and the content from copied versions. On the other hand, diverse possibilities of threat that severely affect its authenticity, integrity, and confidentiality are instigated by the transmission of medical data over an open communication channel [6]. The process of embedding an imperceptible and detectable mark in digital content such as an image to confirm copyright protection and to avert un-authorized access is declared as digital watermarking [6, 8, 15]. A dedicated communication standard known as digital imaging and communications in medicine is used to exchange electronic patient record (EPR) between hospitals. The significant security requirements with EPR data exchange through open channels are confidentiality, authentication, integrity, and availability.

Appropriate watermarks are used to bear out all these security requirements. Depending on the type of document, watermark techniques are categorized into four categories: text, image, audio, and video watermarking [5]. A digital watermark, which can be detected later for buyer/seller identification, ownership proof, and so forth [7], is an indiscernible signal added to digital data called cover work. The image is provided with a sense of ownership or authenticity as it plays the role of a digital signature. The content is not distinguishable from the watermark, and this is a primary benefit of watermarking. These comprise that the watermark is hard to perceive, endures common distortions, resists malicious attacks, carries numerous bits

***Corresponding author: Puvvadi Aparna,** K L University, Vijayawada, Andhra Pradesh, India, e-mail: aparnap0882@gmail.com. https://orcid.org/0000-0002-9400-340X
Polurie Venkata Vijay Kishore: Department of Electronics and Communication Engineering, K L University, Vijayawada, Andhra Pradesh, India

of information, is capable of coexisting with other watermarks, and demands little computation to insert or detect [5]. The usefulness of the watermark depends on the robustness toward a variety of possible attacks by pirates. Furthermore, the item braces robustness against compression such as JPEG, scaling and aspect ratio changes, rotation, cropping, row and column removal, the addition of noise, filtering, cryptographic and statistical attacks, and insertion of other watermarks [27].

Two types of watermarking techniques are available, (i) spatial domain and (ii) frequency domain based on the method of embedding data inside an image. In spatial domain-based watermarking technique, the data is embedded directly into the host image [9, 27]. In frequency domain-based watermarking technique, the data is embedded into the renovated host image [3, 25]. Reversible and irreversible techniques are the other classifications of watermarking techniques. Reversible watermarking techniques [25] are used to attain the original image without loss from the watermarked image while lossless recovery of the original image is not possible with irreversible watermarking techniques [27]. Thus, reversible watermarking is more suitable for medical images [12]. The watermarking method is explored in many research articles [11, 14, 16, 17, 21, 24]. In the spatial domain [17, 21, 24] some methods hide the watermark pattern, and in the frequency domain [14, 16, 21] others embed the watermark pattern. Discrete wavelet transform (DWT) and discrete cosine transform (DCT) for video watermarking are the most popular frequency domain techniques. Low frequency and high energy content in images [10] are recognized by using DCT in watermarking techniques. Efficient spatial localization, frequency spread, and multi-resolution [14] of DWT make it a very attractive transform. The combined DWT-DCT methods are instigated by embedding and/or grayscale watermarking into the grayscale host image [1].

The objective of this study is to securely send the patient's original information to the receiver without losing any information using the crypto-watermarking system. The crypto-watermarking system improves the security of medical images by modifying or modulating image pixels in an unnoticeable way. In this paper, three types of input, namely, medical image, electronic health record (EHR), and patient face image are utilized. From the first input, the region of interest (ROI) is segmented using an active contour algorithm. Then, the ROI part is encrypted using an SHA-256 algorithm, and the obtained output is converted into the hexadecimal format. After that, the second input EHR is encrypted using advanced encryption standard (AES) algorithm, and the output is converted into the hexadecimal format. Similarly, from the third input (face image), features are extracted using the histogram of oriented gradients (HOG) descriptor, and the output is converted into the hexadecimal format. From that, all the hexadecimal values are concatenated and the attained hexadecimal value is converted into the binary bit. To increase the security of the crypto-watermarking system, the attained bit stream is compressed using an arithmetic encoder. Finally, the compressed bit (CB) streams are embedded into the medical image. The same process is repeated in the extraction process. The main contribution of the research is explained below:

- For secure medical information sharing, the crypto-watermarking system is presented in this paper. Using this system, the embedding and extraction process is calculated. Based on the crypto-watermarking system, the information is securely transferred.
- The developed crypto-watermarking system is robust against diverse types of attacks.
- The performance of this proposed approach is evaluated in terms of peak signal to noise ratio (PSNR) and normalized correlation (NC). Compared to the existing approaches such as [18] and [2], PSNR of the proposed approach has been improved by 5% and 16%, respectively.

The rest of the paper is organized as follows: Section 2 provides a literature review of the relational watermarking systems. Section 3 describes the technical preliminaries of the proposed approach. The proposed crypto-watermarking scheme is presented in Section 4, and Section 5 presents results and discussion. Finally, conclusions are made in Section 6.

2 Related Work

Lot of researchers have developed the watermarking system. Among them some of the works are analyzed here. Combined cryptography and digital watermarking for the secure transmission of medical images in

EHR systems is described by Pooja Prakash et al. [19]. Clinical health care from a distance is provided by telemedicine which uses telecommunication and information technology. Telemedicine is continuously overwhelmed by information privacy and security issues specifically due to the extensive use of new communication technologies like a wireless network in today's world. Very sensitive information which should not be made accessible to unauthorized persons is encompassed by the medical images in order to protect patient privacy, integrity, and confidentiality. The confidentiality and authenticity of the medical images are provided by using encryption and digital watermarking. At this juncture, for medical image transmission, they combine cryptography and digital watermarking techniques. The watermarking technique uses the DWT and DCT combination, and the cryptographic technique used is the elliptical curve Diffie-Helman algorithm.

The digital image watermarking based DWT is explained in Chitrasen and Kashyap [4]. In their innovative method, the random segmentation and modernization of engrained confidential information were performed without any preceding notion concerning the innovative host video. The confidential information was embedded in discrete video frames engaging the DWT's frequency domains in the sequence of the inserting process. Moreover, the information is fortified by efficiently projecting a Haar wavelet-based digital watermark method. In the Haar wavelet, the copyright information in video bit streams is attached by engaging the dyadic equation. Besides, electronic patient security using a watermarking algorithm has been elucidated by Vidya and Padmaja [22]. In hospitals, the security of 'electronic patient record' (EPR) data gains prime importance for the safety of hospital records and wireless transmission of medical information. The internet image/medical data have led to the efficient, secure, and quicker transmission of confidential EPR. An EPR navigating between hospitals through the network goes through security issues, losses in data, and high confidentiality issues which concern the integrity, authenticity, and security of EPR transmission in telediagnosis. The uniqueness lies in watermarking by embedding EPR into the facial photograph of the patient, using the least significant bit technique and MATLAB implementation, and then transmitting it over the internet. The forefinger tip of the patient provides the photoplethysmography (PPG) signal, and the watermarked information is embedded and extracted by using a feature as a password. The first level of security uses the augmentation index as a security password from the PPG signal, and the second level of watermarking doubles the security.

Correspondingly, in the transform domain, Selvam et al. [20] have explicated a novel reversible watermarking technique for medical images without any additional key information. The embedding capacity was less and also entails additional key information for lossless recovery of the original image at the extraction side in traditional transform-based watermarking method. A novel hybrid reversible watermarking algorithm is used by this paper to overcome that difficulty in the transform domain to increase the embedding capacity. A secure and reversible medical image watermarking is developed by using the integer wavelet transform and the discrete Gould transform (DGT). At the sender side, DGT was used to embed the watermark information within a wavelet subband, and at the receiver side, the embedded watermark was extracted and the exact original medical image was reconstructed without any additional information.

Furthermore, the joint fingerprint/encryption/dual watermarking system using spatial fusion has been elucidated by Viswanathan and Krishna [23] for verifying the security issues of teleradiology. With confidentiality, availability, integrity, and its origin, this paper aims to give access to the outcomes of medical images. In the protection stage, the watermarking, encryption, and fingerprint enrollment are conducted jointly such that the extraction, decryption, and verification are applied independently. The difficulty in maintenance of multiple documents like authentication data, personnel and diagnosis data, and medical images are reduced by the dual watermarking system which introduces two different embedding schemes: one used for patient data and other for fingerprint features. The exact rules of fusion are followed by the spatial fusion algorithm, which determines the region of embedding using threshold from the image to embed the encrypted patient data resulting in better quality than other fusion techniques. The robustness of the medical information is improved by the four-step stream cipher algorithm which uses a symmetric key for encrypting the patient data with a fingerprint verification system using algebraic invariants.

Also, Yassin et al. [26] reveal the quantization index modulation (QIM) blind video watermarking system on the basis of wavelet transform and principal constituent analysis. In the recovery of the watermark, the refuge of the system was reputable with the help of one secret key. DWT was implemented on each video frame disintegrating it into a number of subbands. Principal component analysis (PCA) nominates and distorts the

maximum entropy blocks. The maximum coefficient of the PCA blocks of each subband is quantized by using the QIM. At that juncture, the nominated appropriate quantize values implant the watermark.

3 Technical Preliminaries

The background of the proposed crypto-watermarking system is explained here. After the background explanation, the proposed part is deeply explained.

3.1 Active Contour-Based Segmentation

The crucial thought of active contour model (ACM) is the dynamic movement of a parametric bend under the action of certain control forces present in the image spatial domain [13]. The two types of these forces are the internal and external forces. The internal force is capable of contour (or snake) smoothness, and the external one is capable of pushing the snake toward the object limit. The snake (ACM curve) is characterized by $P(a, b) = (u(a, b), v(a, b))^T$, where $a \in [0, 1]$, and b is the discrete time between two consecutive steps. The cost capacity is the snake total energy, and its minimum is found when the snake develops near the desired contour; that equation is specified as follows.

$$\mathrm{SE}_{\mathrm{snake}} = \int_0^1 \mathrm{SE}_{\mathrm{int}}(P(a, b) + \mathrm{SE}_{\mathrm{ext}}(P(a, b)))\, da \tag{1}$$

where $\mathrm{SE}_{\mathrm{int}}$ signifies the internal energy term and $\mathrm{SE}_{\mathrm{ext}}$ characterizes the external energy term. Equation (2) gives the internal energy, and equation (3) is used to calculate the external energy.

$$\mathrm{SE}_{\mathrm{int}}(P(a, b)) = \frac{1}{2}\left[\varepsilon(a, b)\left\|\frac{\partial P(a, b)}{\partial a}\right\|^2 + \varphi(a, b)\left\|\frac{\partial^2 P(a, b)}{\partial b^2}\right\|^2\right] \tag{2}$$

where ε epitomizes the elasticity component and φ is blending by the rigidity component

$$\mathrm{SE}_{\mathrm{ext}}(P(a, b)) = \lambda_{\mathrm{line}}\,\mathrm{SE}_{\mathrm{line}}(a, b) + \lambda_{\mathrm{edge}}\mathrm{SE}(a, b) + \lambda_{\mathrm{term}}\,\mathrm{SE}_{\mathrm{term}}(a, b) \tag{3}$$

$$= \lambda_{\mathrm{line}} D(a, b) - \lambda_{\mathrm{edge}}|\nabla G * I(P(a, b))|^2 + \lambda_{\mathrm{term}}\left|\frac{D_{jj}D_i^2 - 2D_{ij}D_iD_j + D_{ii}D_j^2}{\left(D_i^2 + D_j^2\right)^{3/2}}\right|_{(a,b)} \tag{4}$$

where λ_{line} λ_{edge} and λ_{term} are the external energy components which control the curve tension. The external energy term is composed by-line ($\mathrm{SE}_{\mathrm{line}}$), edge ($\mathrm{SE}_{\mathrm{edge}}$) and termination ($\mathrm{SE}_{\mathrm{term}}$) energy functions, determined using $D(a, b) = \mathrm{G} * I(P(a, b))$ and its first and second order partial derivatives (i.e. D_x, D_y, D_{xx}, D_{xy} and D_{yy}), where G is the Gaussian function and I is the image. The customary arrangement of this issue consists of the numerical computing of the Euler condition in (4) until the equation is fulfilled.

$$\nabla \mathrm{SE}_{\mathrm{ext}} - \varepsilon(a, b)\frac{\partial^2 P(a, b)}{\partial a^2} + \varphi(a, b)\frac{\partial^4 P(a, b)}{\partial a^4} = 0 \tag{5}$$

The minimum energy arrangement related to the energy steadiness state is compared by this condition. In other words, the external energy component gets to be equivalent to the internal one or the other way around.

3.2 Face Image Feature Extraction

The face is an image used for authentication purposes. In this, HOG descriptors are used to extract the important features. HOG features are local descriptors which are used to compute the local direction of the gradient. The edge information of a human is well designated by the proposed descriptors; also the method is robust to illuminate variations and small offsets. Equations (6) and (7) represent the gradient of the pixel of (x, y) in an image as

$$G_x(x, y) = H(x + 1, y) - H(x - 1, y) \tag{6}$$

$$G_x(x, y) = H(x, y + 1) - H(X, Y - 1) \tag{7}$$

where $G_x(x, y)$ denotes the horizontal direction gradient of the input image pixel, $G_y(x, y)$ signifies the vertical direction gradient, and $H(x, y)$ symbolizes the pixel values. Then equation (8) embodies the gradient magnitude and direction of (x, y) as

$$G_x(x, y) = \sqrt{G_x^2(x, y) + G_y^2(x, y)} \tag{8}$$

$$\alpha(x, y) = \tan^{-1}\left(\frac{G_y(x, y)}{G_x(x, y)}\right) \tag{9}$$

The procedure for calculating the HOG feature is explained below:

Step 1: Consider the patient face image I captured by a web camera. Initially, the gradient is calculated for the image. At this juncture, [−1, 0, 1] and [−1, 0, 1] median filter is used for filtering. Then, the vertical gradient and horizontal gradient of the image are calculated; likewise, the gradient direction and gradient magnitude of each pixel are calculated.

Step 2: Then, divide the input image into average small cells (including $256 * 256$ pixels) and combine four cells into a small block; one block is constituted by a cell of $2 * 2$.

Step 3: Subsequently, here, the $+90°$ to $-90°$ region is divided into 13 equal parts that are 13 channels in total. So, there are $4 * 13 = 52$ features in each block.

Step 4: From the orientated gradient histogram of each cell statistics of each pixel is calculated. The abscissa of the histogram characterizes the 13 direction channels selected in step 2, and the ordinate exemplifies the summation of the gradient, belonging to a certain direction channel. As a result, a set of vectors are obtained.

Step 5: At this juncture, the vectors in blocks are normalized in which pixels correspond with the vectors. Block normalization normalize local contrast variations and histogram of each block. In this paper, equation (8) proposes the hog descriptor implemented by the L2-norm.

$$f = \frac{v}{\sqrt{\|v\|_2^2 + e^2}} \tag{10}$$

Step 6: As a final point, combine all the vectors processed above and then form a set of vectors which are the HOG features.

3.3 Advance Encryption Standard

The AES algorithm is used for the encryption process. It is an iterated block cipher which contains a block size of 128 with a variable key length. The different transformation operates on the intermediate results, known

as a state; the state is basically in the form of a rectangular array of bytes. When the block size is 128 bits or 16 bytes, the dimension of the rectangular array is 4×4.

A State

S0, 0	S0, 1	S0, 2	S0, 3
S1, 0	S1, 1	S1, 2	S1, 3
S2, 0	S2, 1	S2, 2	S2, 3
S3, 0	S3, 1	S3, 2	S3, 3

A Key

Y0, 0	Y0, 1	Y0, 2	Y0, 3
Y1, 0	Y1, 1	Y1, 2	Y1, 3
Y2, 0	Y2, 1	Y2, 2	Y2, 3
Y3, 0	Y3, 1	Y3, 2	Y3, 3

Here, we map the cipher input onto the state bytes in the order of S0, 0, S1, 0, S2, 0, S3, 0, S1, 1, S2, 1, S3, 1…and the bytes of the cipher text are mapped onto the array in the order of Y0, 0, Y1, 0, Y2, 0, Y3, 0, Y1, 1, Y2, 1, Y3, 1…. After the completion of the cipher operation, the cipher output from the state is extracted by taking the state bytes in the same order. In addition to this, the AES uses a different number of rounds based on the key size which is given in Table 1.

The state contains some operations at every round. The operations are as follows:

- Sub-bytes
- Shift row
- Mix column
- Add round key

Add Round Key

In add round key, we apply a round key to the state by bitwise XOR. The round key can be derived from the cipher key using the key schedule.

S0,0	S0,1	S0,2	S0,3		Y0,0	Y0,1	Y0,2	Y0,3	
S1,0	S1,1	S1,2	S1,3	XOR	Y1, 0	Y1,1	Y1, 2	Y1, 3	=
S2,0	S2,1	S2,2	S2,3		Y2,0	Y2,1	Y2,2	Y2,3	
S3,0	S3,1	S3,2	S3,3		Y3,0	Y3,1	Y3,3	Y3,3	

A0, 0	A0, 1	A0, 2	A0, 3
A1, 0	A1, 1	A1, 2	A1, 3
A2, 0	A2, 1	A2, 2	A2, 3
A3, 0	A3, 1	A3, 2	A3, 3

It can be written simply as $\mathrm{Aij} = \mathrm{S_{ij}XOR\,Y_{ij}}$

Shift Row Operation

In shift row operation, every row of the state is cyclically shifted to the left. This is dependent on the row index.

- First row to zero position to the left

Table 1: Rounds for corresponding key size.

Key size	Round
128	10
192	12
256	14

– Second row to one position to the left
– Third row to two positions to the left
– Fourth row to three positions to the left

S0,0	S0,1	S0,2	S0,3		S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3	→	S1,1	S1,2	S1,3	S1,0
S2,0	S2,1	S2,2	S2,3		S2,2	S2,3	S2,0	S2,1
S3,0	S3,1	S3,2	S3,3		S3,3	S3,0	S3,1	S3,2

Sub-bytes Operation
The sub-bytes operation is a non-linear byte substitution. It operates on each byte of the state in an independent manner. The substitution table (S-Box) is invertible and is constructed using two transformations.
(i) Take the multiplicative inverse in Rijndael's finite field.
(ii) Apply the affine transformation; they have been documented in the Rijndael documentation.

Here, the pre-calculation is utilized when the S-box is independent of any input. Then, we substitute each byte of the state in the S-box whose index corresponds to the value in the state S (i,j) = S box [s(i,j)].

Mix-column Operation
The mix column operation makes use of the advanced mathematical calculations in the Rijndael's finite field. It corresponds to the matrix multiplication with the following:

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

The addition and multiplication used here are different from the normal calculation.

Rijndael Key Schedule
In Rijndael key schedule, the key schedule is responsible for expanding a short key into a large key, whose part can be used in different iterations. The possibilities of expanding to a different size are as follows:
– A 128-bit key is expanded to 176-byte key.
– A 192-bit key is expanded to 208-byte key.
– A 256-bit key is expanded to 240-byte key.

4 Proposed Crypto-Watermarking System

The intention of the proposed methodology is to transfer medical information through the internet with high security. In the field of medical diagnosis, trading of data among different healing centers and diagnostic communities for mutual availability of diagnostic and therapeutic case analyses is very normal. During medical image transportation, some of the information should be hidden because of high security. In this paper, a medical image watermarking approach using different methods is developed, and this enforces integrity, authenticity, and confidentiality of the medical information. Here, face image is utilized for authentication, cryptosystem for confidential data, and reversible watermarking for integrity. The proposed reversible watermarking system helps to watermark embedding and extraction in a medical image with large data hiding capacity, security, and high watermarked quality. The overall proposed methodology is explained in two stages which are (i) watermark embedding and (ii) extraction. The overall process of the proposed system is explained in Figure 1.

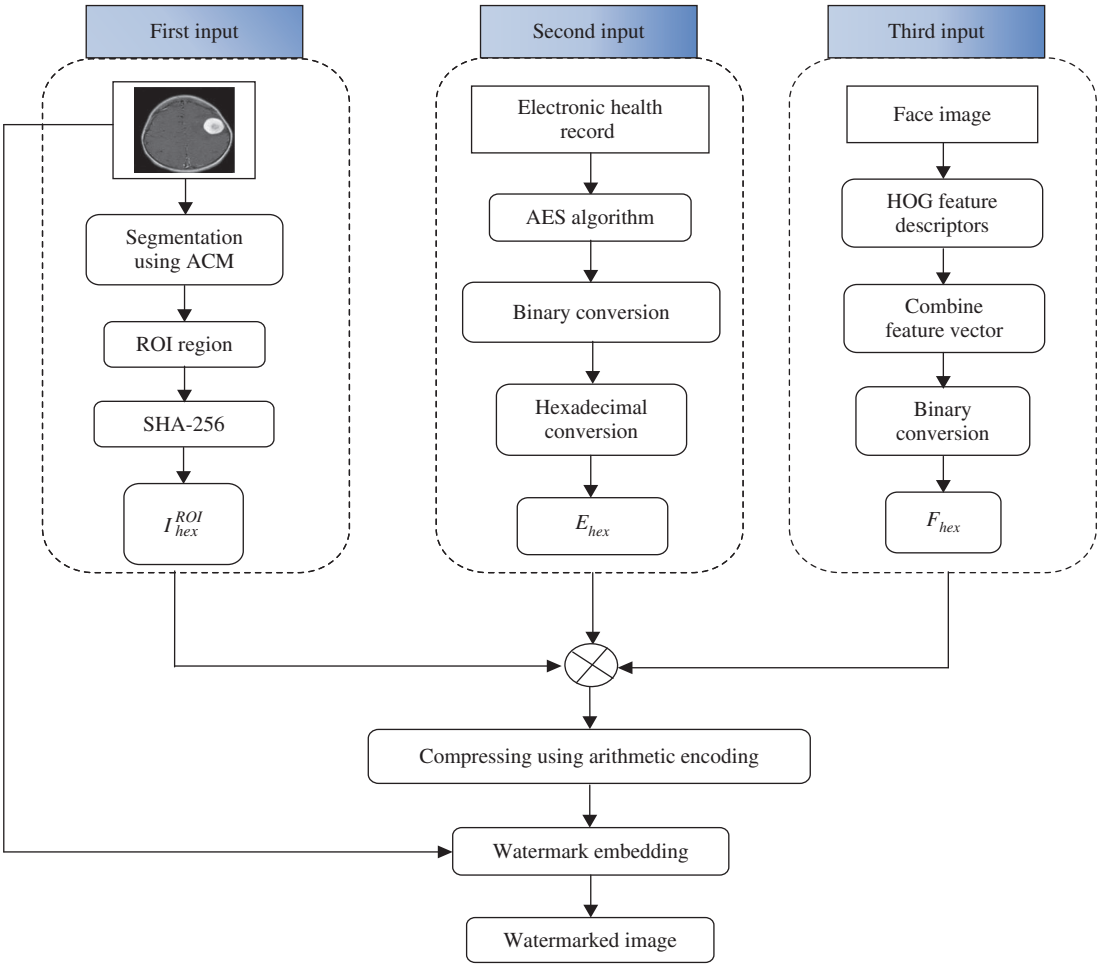


Figure 1: Proposed Crypto-Watermarking System.

4.1 Watermark Embedding Procedure

Embedding is an essential method for image watermarking which converts the image into another format. For embedding process, the watermark bit is inserted into the original image. This process secures information while transferring through networks. This paper proposed a novel method to enforce integrity, authenticity, and confidentiality of the medical information, by embedding two different watermarks in the medical image. The embedding process mainly consists of the following four steps:

- Select the first input (medical image) and apply segmentation and encryption.
- Select the second input (EHR) and encrypt it.
- Select the third input (face) and extract the features.
- Concatenate the three inputs.
- Apply arithmetic encoding algorithm to compress the bit.
- Apply the embedding process.
- Obtain the watermarked image.

Here, initially, the ROI part is segmented from the input image I^{in} with the help of active contour segmentation algorithm (refer to section 1). Then, the obtained ROI I^{ROI} is given to the encryption process. In this paper, SHA-256 algorithm is utilized for encrypting I^{ROI} which obtained a hash image $I_{\text{Hash}}^{\text{ROI}}$. Then, the $I_{\text{Hash}}^{\text{ROI}}$ is changed into hexadecimal $I_{\text{hex}}^{\text{ROI}}$. After that second input EHR is considered. Using AES, the data is encrypted and the output is converted into hexadecimal format E_{hex}. After that, the third part of the input is the face

image (F). Here, the face image features are extracted using the HOG descriptor and the feature value is converted into hexadecimal format F_{hex}. Then, the image information, EHR, and face image information are concatenated and HI^{con} is obtained. After that, the HI^{con} is compressed using the arithmetic coding algorithm which increases the security of the proposed methodology. At last, a CB is obtained. Then, the attained bit is embedded into the original input image I^{in}. The embedding process is given in Table 2.

The watermarked image is now ready to be stored in the hospital's database system or can be sent to another medical institution.

4.2 Watermark Extraction Procedure

Watermark extraction is a reverse procedure of the embedding process. In this, the original information is extracted from the watermarked image. In this section, ROI, EHR, and face images are extracted from the watermarked image without loss of any original information. The watermarked image I^{water} is given to the input of the extraction operation to generate the random matrix RM (refer to Table 1). Subsequently, equation (11) is used to calculate the correlation coefficient RM_{cor} between the watermarked image I^{water} and the generated random matrix RM.

$$\text{RM}_{\text{cor}} = \frac{\sum_m \sum_n (\text{I}_{\text{mn}}^{\text{water}} - \overline{\text{I}^{\text{water}}})(B_{mn} - \overline{B})}{\sqrt{\left(\sum_m \sum_n (\text{I}_{\text{mn}}^{\text{water}} - \overline{\text{I}^{\text{water}}})^2\right)\left(\sum_m \sum_n (B_{mn} - \overline{B})^2\right)}} \tag{11}$$

where $\text{I}_{\text{mn}}^{\text{water}}$ denotes the watermarked image, B_{mn} embodies the random matrix RM, $\overline{\text{I}^{\text{water}}}$ signifies the mean value of I^{water}, and $\overline{B}$ is the mean value of B. After that, we divide the correlation coefficient RM^{cor} by 2 and repeat the process and store the resultant value in a vector VR_Z.

$$R_Z = R_{\text{cor}}/2 \tag{12}$$

$$\overline{\text{VR}}_Z = \sum_{i=1}^{k} \text{VR}_Z^i/k; \text{ where k} = |\text{VR}_Z| \tag{13}$$

where $\overline{\text{VR}}_Z$ is a mean value of the resultant vector. Then, the elements of the vector VR_Z are compared with $\overline{\text{VR}}_Z$ to extract watermark image pixels. If the element's value is greater than the mean value, the extracted

Table 2: Embedding Procedure.

Input: Compressed bit stream CB,
Original image I^{in}
Output: Watermark image I^{water}
1. Get the input image I^{in}
2. Calculate the I_{Seed} using pixel values
$\text{I}_{\text{seed}} = \sum_{i=1}^{n} \sum_{j=1}^{n} I_{ij}^{in}$
3. Generate the random matrix R
$R = \text{PRMG}\,[I_{\text{seed}}]_{(2\times 2)}$
4. Calculate the resultant matrix R_t
$R_t = (R - 0.5) \times 2$
5. Calculate the intended random matrix RM
$\text{RM} = \text{PRMG}[R_t]_{(2\times 2)}$
6. If the bit is 0, it means
$\left[I_{(i,j)}^{in}\right] = \left[I_{(i,j)}^{in}\right] + (\beta * [\text{RM}])$
7. If the bit is 1, it means no operation is performed
8. Repeat steps 3 and 7 until all the watermark pixels are embedded.
9. Output: Watermarked image I^{water}

watermark image pixel is '0'; otherwise, the pixel value is '1'. The above process is designated as follows:

$$E_{BS}(x,y) = \begin{cases} 0, & \mathrm{VR}_Z^i > \overline{\mathrm{V}}\mathrm{R}_Z \\ 1, & \text{Otherwise} \end{cases}; \quad \text{where n} = |\mathrm{VR}_Z| \tag{14}$$

Then, the bit stream E_{BS} is compressed using an arithmetic decoder method to attain the original bit stream D_{BS}. From the original bit stream D_{BS}, we extract H_{ROI}, H_{EHR}, and H_{fin}, and convert H_{EHR} into their corresponding bit stream representation as B_{EHR}. Then change B_{EHR} into the original representation as $E_{encrypt}$. Decrypt $E_{encrypt}$ using K with the elliptic-curve cryptography (ECC) method to get EHR. Correspondingly, we compute the Hash for H_{ROI} to obtain the original ROI image.

5 Results and Discussion

The proposed crypto-watermarking system is executed in a windows machine containing configurations Intel (R) Core i5 processor, 3.20 GHz, 4 GB RAM, and the operating system platform is Microsoft Windows 7 Professional. The software used for implementation is MATLAB. In this paper, for experimentation, 40 medical images which are publically available on the internet are utilized. The experimental sample images used are given in Figure 2.

5.1 Performance Measure

By utilizing the performance measures, namely, sensitivity, specificity, accuracy, PSNR, and NC, the performance of the proposed work is estimated. The performance is analyzed in two stages, namely, segmentation stage and watermarking stage. Experimental used images are presented in Figure 2. The sample EHR is given in Table 3 and sample face image is given in Figure 3.

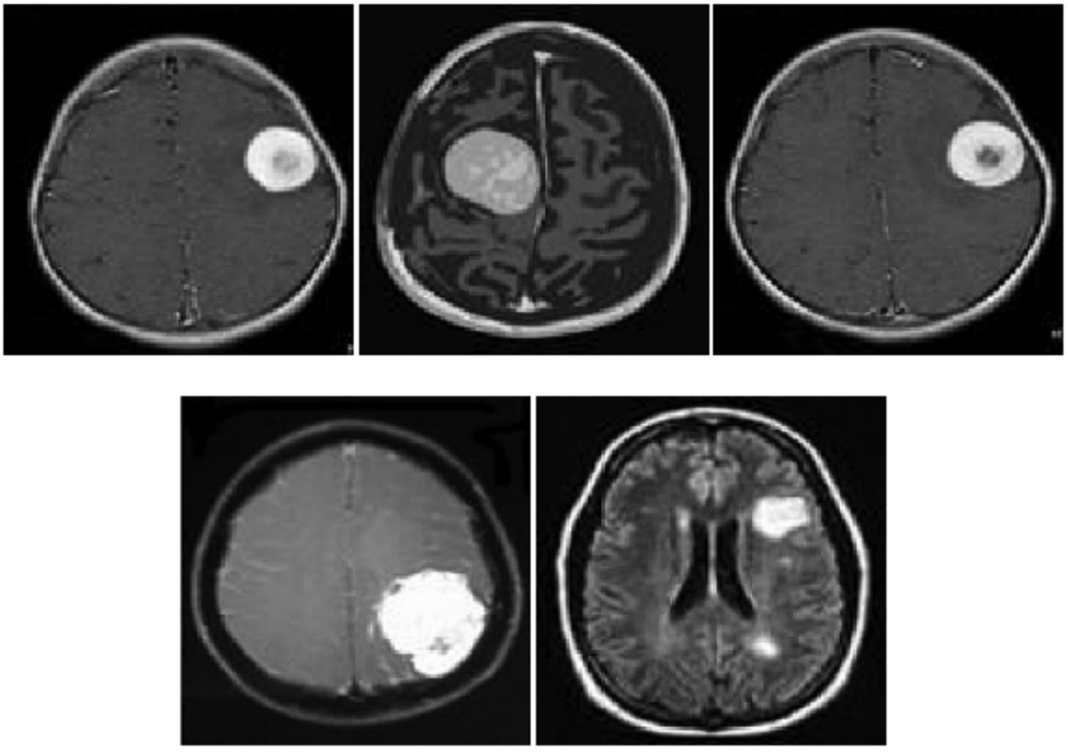


Figure 2: Experimentally Used Images.

Table 3: Sample Electronic Healthcare Record.

The heart foundation: Kolkata
Patient Reference number: 019181918
Name of the doctor: Dr. Pratap Singh
Name of the patient: Ms. Rakhi
Age in years: 45
Date of admission: 12.09.2008

Figure 3: Sample Patient Face Image.

5.1.1 Results of Segmentation Evaluation

In this study, for segmentation, an active contour algorithm is utilized. The segmentation performance is compared with the help of sensitivity, specificity, and accuracy measures. The basic count values such as true positive (TP), true negative (TN), false positive (FP), and false negative (FN) are used in these measures.

Sensitivity
The proportion of actual positives which are correctly identified is the measure of the sensitivity. It relates to the ability of the test to identify positive results.

$$\text{Sensitivity} = \frac{\text{Number of true positives}}{\text{Number of true positives} + \text{Number of false negatives}} \times 100$$

Specificity
The proportion of negatives which are correctly identified is the measure of the specificity. It relates to the ability of the test to identify negative results.

$$\text{Specificity} = \frac{\text{Number of true negatives}}{\text{Number of true negatives} + \text{Number of false positives}} \times 100$$

Accuracy
The accuracy measure is calculated from the measures of sensitivity and specificity as specified below.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \times 100$$

The segmentation results for brain tumor images are given in Table 4. In our work, a total of five images are considered to provide the results of sensitivity, specificity, and accuracy. Here the effectiveness of segmentation is compared with the region-growing method. The results are tabulated below.

Table 4: Sensitivity Comparison of the Proposed Segmentation.

Images	Sensitivity	
	Active contour algorithm	Region-growing algorithm
Image 1	0.988	0.976
Image 2	0.884	0.879
Image 3	0.999	0.989
Image 4	0.975	0.973
Image 5	0.882	0.857

The results of five brain tumor images are shown in Table 4, which are helpful to prove the effectiveness of the proposed segmentation work. Here, the performance of the proposed active contour algorithm-based segmentation and existing region-growing algorithm-based segmentation are analyzed. When analyzing Table 4, the sensitivity value of image 1 is 0.988 which means that our proposed work provides good sensitivity value compared to the existing method. For image 2, the proposed sensitivity value is 0.884, but the existing region-growing method achieves the sensitivity value of 0.879. For image 3 and image 4 the proposed technique attains the sensitivity value of 0.999 and 0.975, which is a higher value when compared to the existing method. The sensitivity value of image 5 is 0.882 which is a higher value when compared to the region-growing method. The experimental result shows that our proposed work provides good sensitivity value when compared to the existing method. The graphical representation of Table 4 is given in Figure 4.

The specificity comparison of the proposed work is tabulated in Table 5. Here, the proposed active contour method with a region-growing algorithm is compared.

When analyzing Table 5, it is clear that our proposed segmentation method reaches a higher specificity value when compared to the existing region-growing method. Here, image 1 reaches the higher specificity value of 0.9999, which is 0.9820 when using region-growing algorithm. The specificity value for image 3 and image 4 is a higher value when compared to the existing method. For image 5 the proposed method attains the specificity value of 0.9999, which is a higher value when compared to the existing method which attains the specificity value of 0.989. The graphical representation of Table 5 is given in Figure 5.

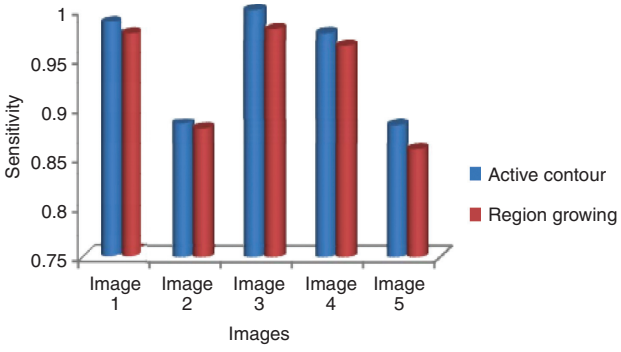


Figure 4: Sensitivity Comparison of the Proposed Segmentation.

Table 5: Specificity Comparison of the Proposed Segmentation Method.

Images	Specificity	
	Active contour algorithm	Region-growing algorithm
Image 1	0.9999	0.9820
Image 2	0.9995	0.9894
Image 3	1	0.9859
Image 4	1	0.985
Image 5	0.9999	0.989

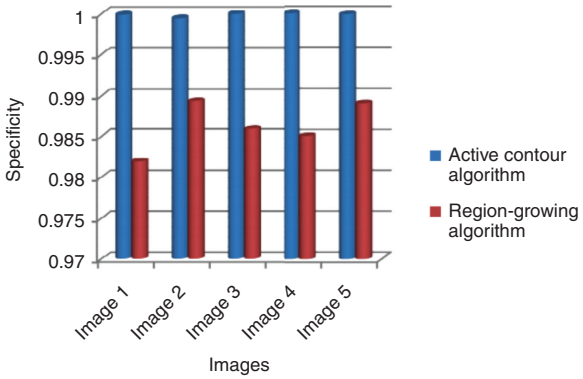


Figure 5: Specificity Comparison of the Proposed Segmentation.

The accuracy comparison of the proposed work is tabulated in Table 6. Accuracy is an important measure of the segmentation process. Here, our proposed active contour algorithm is compared with a region-growing algorithm.

The accuracy value of image 1 is 0.988 which shows that our proposed work provides good accuracy value when compared to the existing method. For image 2, the proposed method attains the maximum accuracy of 0.997, which is 0.975 for the region-growing algorithm. For image 3 and image 4, the proposed technique attains the accuracy values of 0.998 and 0.999 which are higher values compared to the existing method. From the results, it clearly shows that the proposed segmentation method attains better results compared to the region-growing algorithm. The graphical representation of Table 6 is given in Figure 6.

5.1.2 Results of Watermark Evaluation

Watermarking is an important stage for this work. Here, for watermarking, three types of inputs are used. The first input is encrypted using the SHA-256 algorithm, and the second input is encrypted using the AES algorithm. The watermarking performances are measured using PSNR and NC measures. Visual representation of segmentation output is given in Table 7.

Table 6: Accuracy Comparison of Proposed Segmentation.

Images	Accuracy	
	Active contour algorithm	Region-growing algorithm
Image 1	0.998	0.978
Image 2	0.997	0.975
Image 3	0.998	0.978
Image 4	0.999	0.910
Image 5	0.9906	0.978

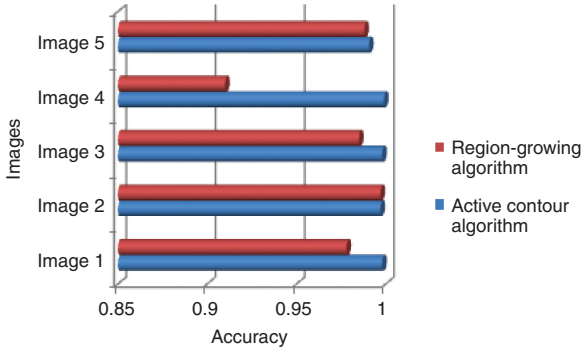
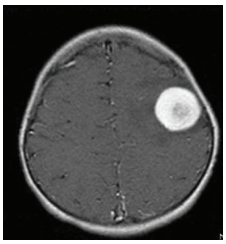
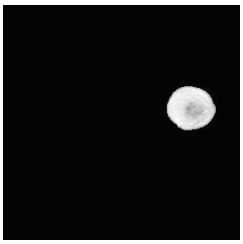
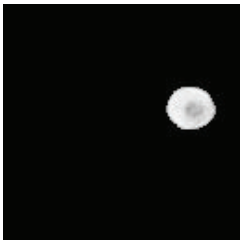
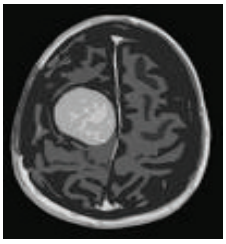
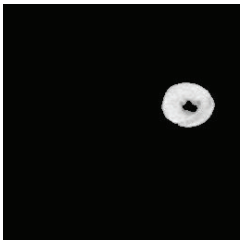
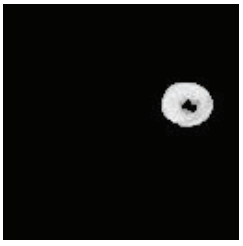
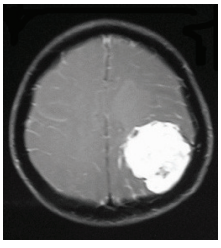
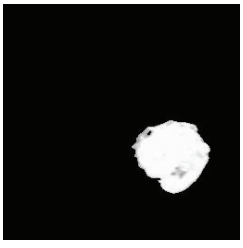
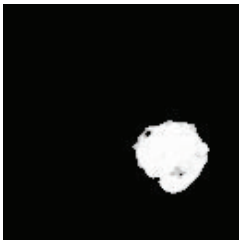
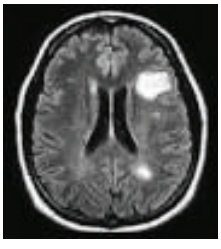
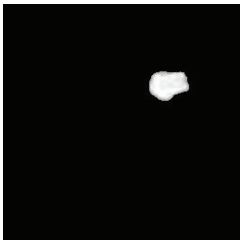
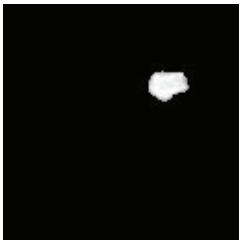


Figure 6: Accuracy Comparison of Proposed Segmentation.

Table 7: A Visual Representation of Segmentation Output.

Input image	Active contour	Region growing
		
		
		
		
		

Peak Signal to Noise Ratio

The PSNR is used to measure the quality of the watermarked image. The PSNR is the ratio between the source image and the watermarked image. The PSNR is identified using the mean square error (MSE). The MSE gives the cumulative squared error between the corrupting noise and the maximum power of the signal. Higher PSNR and lower MSE values improve the quality of watermarking.

$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{M * N} \sum_{x=1}^{M} \sum_{y=1}^{N} [I(i,j) - I'(i,j)]^2$$

where, $I(i, j) \rightarrow$ Original image and
$I'(i, j) \rightarrow$ Watermarked images.

Normalized Correlation
NC measures the similarity between the original watermark image and the watermark extracted from the attached image. Here, $I(i, j)$ is the pixel value of the original image, and $I'(i, j)$ is the pixel value of the embedded image.

$$\mathrm{NC} = \frac{\sum_{x=1}^{n} \sum_{y=1}^{m} I(i, j) * I'(i, j)}{\sum_{x=1}^{n} \sum_{y=1}^{m} I^2(i, j)}$$

In Table 8, the performance of the proposed watermarking system is analyzed based on PSNR measure. In this paper, the AES algorithm is used for EHR encryption. To prove the effectiveness of the proposed AES algorithm, the AES is compared with the ECC algorithm. For comparing these two algorithms, AES-based watermarking attained the maximum PSNR of 44.54 db, which is 44.00 db when using ECC-based embedding processes. Here, the used embedding capacity is 75,456 bits. Table 9 shows the attack-based EHR performance. After applying attack also, our proposed method gives better accuracy. This reflects the robustness of the proposed approach. The result clearly shows the performance of the proposed methodology.

5.2 Comparative Analysis

In this section, the proposed medical image watermarking systems with existing works are compared. The performance of the proposed crypto-watermarking system is evaluated on the input medical image using PSNR and NC measures. Here, our proposed work is compared with [18] and [2]. In [18], the author explained the medical image watermarking system for E-healthcare applications. Here, they used two different watermarking algorithms. At first, they embed the digital watermark and electronic patients' record (EPR) in both

Table 8: Performance of the Proposed Approach Using PSNR Value and Embedding Capacity (bits).

Images	File format	PSNR (db)		Embedding capacity (bits)
		ECC	AES	
Image 1	JPEG	42.87	43.57	75456
Image 2	JPEG	41.67	42.36	75456
Image 3	JPEG	44.00	44.54	75456
Image 4	JPEG	41.73	42.41	75456
Image 5	JPEG	42.14	42.67	75456

Table 9: Attack-Based EHR Performance.

Attack-based results		Accuracy
Original data	The Heart Foundation, Kolkata Patient Reference Number: 019181918 Name of the Doctor: Dr. Pratap Singh Name of the patient: Ms. Rakhi. Age in Years: 45 Date of admission: 12.08.2008	1
5 bit changed	The Heart Foundation, Kolkata Patient Reference Number: 019181918 Name of the Doctor: Dr. Pratap Singh Name of the patient: Ms. Rakhi. Age in Years: 45 Date of admission: 12.08.2008	0.9862
10 bit changed	The Heart Foundation, Kolkata Patient Reference Number: 019181918 Name of the Doctor: Dr. Pratap Singh Name of the patient: Ms. Rakhi. Age in Years: 45 Date of admission: 12.08.2008	0.9624
15 bit changed	The Heart Foundation, Kolkata Patient Reference Number: 019181918 Name of the Doctor: Dr. Pratap Singh Name of the patient: Ms. Rakhi. Age in Years: 45 Date of admission: 12.08.2008	0.9481

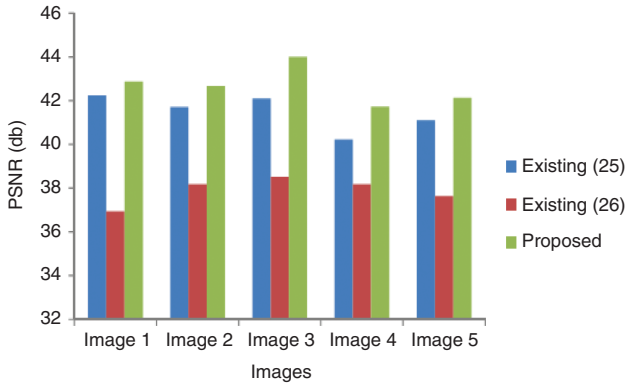


Figure 7: Comparative Analysis Based on PSNR Measure.

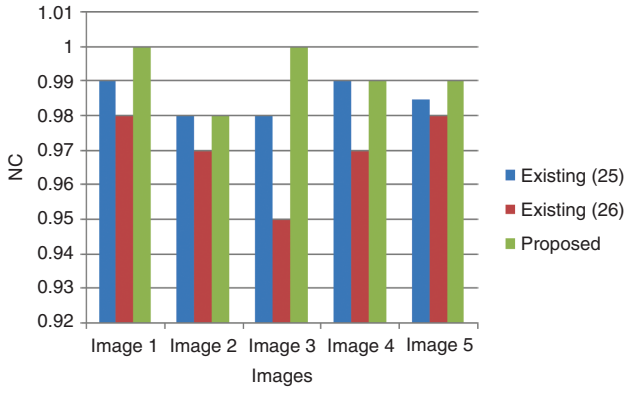


Figure 8: Comparative Analysis Based on NC Measure.

ROI and region of non-interest (RONI). Second, they used RONI to hide the digital watermark and EPR. In [2], medical image watermarking is performed based on compression and cryptography algorithms. This work is the same as our proposed approach but the difference is that the existing work does not include the fingerprint information for watermarking. And also, this system only gives confidentiality and reliability. In this proposed approach, confidentiality, reliability, and authentication are achieved. Using fingerprint as one of the inputs of watermarking, this will give the authentication to the watermarking system. Figures 7 and 8 show the comparative results based on PSNR and NC measures.

Figure 7 shows the comparative analysis of the proposed approach against the existing approach using PSNR measures. Here, our proposed approach achieves the maximum PSNR of 43.87 dB for image 1, 43.52 dB for image 2, 44.6 dB for image 3, 41.73 for image 4, and 43.14 dB for image 5. Moreover, the existing system [18] achieves the maximum PSNR of 42.23 dB for image 1, 41.71 dB for image 2, 42.102 dB for image 3, 40.22 for image 4, and 41.1405 db for image 5. Similarly, the existing system [2] achieves the maximum PSNR of 36.94 dB for image 1, 38.17 dB for image 2, 38.53 dB for image 3, 38.18 for image 4, and 37.65 dB for image 5. Figure 8 shows the comparative analysis of proposed against existing approaches using NC measures. When analyzing Figure 8, our proposed approach achieves the maximum NC. The result section clearly shows that the proposed approach achieves higher PSNR and NC compared to the other two methods.

6 Conclusion

In this paper, crypto-watermarking-based medical image watermarking in E-healthcare applications is proposed. An efficient crypto-watermarking system is designed with a combination of cryptographic algorithm and embedding process. This method can be used for different modalities of medical images. It can be applied to a variety of digital medical images with different sizes, formats, and bit depths. The face image is utilized

to improve the security of the crypto-watermarking system. Here, region-growing algorithm, SHA-256, AES, arithmetic encoding algorithm, embedding, and extraction process are analyzed. The proposed scheme maintains the watermarked image quality with an average PSNR value of 44.6 dB, embedding capacity of 75,456 bits, and NC of 1. Experimental results also show that the proposed method provides better watermarked image quality and increases the embedding performance. In the future, we will use another biometric like iris and palm prints, which will be taken as a watermark for the video, audio, or text watermarking techniques.

Bibliography

[1] S. K. Amirgholipour and A. R. NaghshNilchi, Robust digital image watermarking based on joint DWT-DCT, *JDCTA* **3** (2009), 42–54.

[2] P. Aparna and P. V. V. Kishore, An efficient medical image watermarking technique in E-healthcare application using hybridization of compression and cryptography algorithm, *J. Intell. Syst.* **27** (2018), 115–133.

[3] K.-H. Chiang, K.-C. Chang-Chien, R.-F. Chang and H.-Y. Yen, Tamper detection and restoring system for medical images using wavelet-based reversible data embedding, *J. Digit. Imaging* **21** (2008), 77–90.

[4] Chitrasen and T. Kashyap, Digital video watermarking using DWT for data security, *IJARCCE* **4** (2015), 307–309.

[5] A. Giakoumaki, S. Pavlopoulos and D. Koutouris, A medical image watermarking scheme based on wavelet transform. in: *Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE*, 1, pp. 856–859, 2003.

[6] H. Golpira and H. Danyali, Reversible blind watermarking for medical images based on wavelet histogram shifting, in: *2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2009)*, pp. 31–36, 2009.

[7] B. Kumar, H. V. Singh, S. P. Singh and A. Mohan, Secure spread-spectrum watermarking for telemedicine applications, *J. Inf. Secur.* **2** (2011), 91.

[8] S. Lee, C. D. Yoo and T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform, *IEEE Trans. Inf. Forensics Secur.* **2** (2007), 321–330.

[9] S.-C. Liew and J. M. Zain, Reversible medical image watermarking for tamper detection and recovery, in: *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10)*, 5, pp. 417–420, 2010.

[10] S. Lin and C. Chin, A robust DCT-based watermarking for copyright protection, *IEEE Trans. Consum. Electr.* **46** (2000), 415–421.

[11] S. Low and N. Maxemchuk, Performance comparison of two text marking methods, *IEEE J. Sel. Areas Commun.* **16** (1998), 561–572.

[12] X. Luo, Q. Cheng and J. Tan, A lossless data embedding scheme for medical images in application of e-diagnosis, in: *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 1, pp. 852–855, 2003.

[13] K. V. Mahesan, S. Bhargavi and D. Jayadevappa, Segmentation of MR images using active contours: methods, challenges and applications, *Int. J. Innov. Res. Adv. Eng.* **2** (2014), 13–21.

[14] K. Matsui, J. Ohnishi and Y. Nakamura, Embedding a signature to pictures under wavelet transform, *IEICE Trans.* **J79-D-II** (1996), 1017–1024.

[15] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, Reversible data hiding, *IEEE Trans. Circuits Syst. Video Technol.* **16** (2006), 354–362.

[16] R. Ohbuchi, H. Masuda and M. Aono, Watermarking three-dimensional polygonal models through geometric and topological modifications, *IEEE J. Sel. Areas Commun.* **16** (1998), 551–560.

[17] J. Ohnishi and K. Matsui, Embedding a seal into a picture under orthogonal wavelet transform, in: *The Proceedings of IEEE International Conference on Multimedia Computing and Systems*, pp. 514–512, 1996.

[18] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan and G. M. Bhat, Information hiding in medical images: a robust medical image watermarking system for E-healthcare, *Multimed. Tools Appl.* **76** (2017), 10599–10633.

[19] M. Pooja Prakash, R. Sreeraj, F. AthishMon and K. Suthendran, Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems, *Int. J. Pure Appl. Math.* **118** (2018), 265–269.

[20] P. Selvam, S. Balachandran, S. P. Iyer and R. Jayabal, Hybrid transform based reversible watermarking technique for medical images in telemedicine applications, *Optik-Int. J. Light Electron Optics* **145** (2017), 655–671.

[21] M. D. Swanson, B. Zhu and A. H. Tewfik, Transparent robust image watermarking, in: *The Proceedings of IEEE International Conference on Image Processing*, 3, pp. 211–214, 1996.

[22] M. J. Vidya and K. V. Padmaja, Enhancing security of electronic patient record using watermarking technique, *Mat. Today: Proc.* **5** (2018), 10660–10664.

[23] P. Viswanathan and P. V. Krishna, A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology, *IEEE J. Biomed. Health Inform.* **18** (2014), 753–764.

[24] G. Voyatzis and I. Pitas, Applications of toral auto morphisms in image watermarking, in: *The Proceedings of IEEE International Conference on Image Processing*, 2, pp. 237–240, 1996.

[25] J. H. K. Wu, R.-F. Chang, C.-J. Chen, C. L. Wang, T. H. Kuo, W. K. Moon and D. R. Chen, Tamper detection and recovery for medical images using near-lossless information hiding technique, *J. Digit. Imaging* **21** (2008), 59–76.
[26] N. I. Yassin, N. M. Salem and M. I. El Adawy, QIM blind video watermarking scheme based on wavelet transform and principal component analysis, *Alex. Eng. J.* **53** (2014), 833–842.
[27] J. M. Zain and A. R. M. Fauzi, Medical image watermarking with tamper detection and recovery, in: *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '06)*, pp. 3270–3273, September, 2006.