DOI 10.29042/2018-3600- 3606

Helix Vol. 8(5): 3600- 3606

Reversible Joint Blind Watermarking for Medical Images and Videos

[1]Kavitha K. J, [2]Dr. B. Priestly Shan

[1]Asst. Prof., Jain Institute of Technology, Davangere & Research Scholar, CSE Dept, Sathyabama University, Chennai, India

[2]Principal, Eranad Knowledge City-Technical Campus, Manjeri, Kerala, India

Email: kavithakj219@gmail.com

Received: 20th June 2018, Accepted: 08th August 2018, Published: 31st August 2018

Abstract

Digital Watermarking system is been practiced widely in the health care centers to secure the patient's records. India is adapting the telemedicine technology to provide facility of easy access to the medical records by the patients and doctors. It makes easy for the doctors to diagnose the patient disease and in turn it saves the time and amount to be spent unnecessarily. With the avail of such facility, it is required to protect the Medical Health Records (MHR) by the respective health care centers being used by the frauds whose intention is to make illegal money. In this regard many measures are adopted by health care centers and one of them is the use of Digital watermarking (DWM). Digital watermarking is implemented in mainly two domains: one at the pixel level usually called as the spatial domain and the other is at the frequency level called as the frequency domain. Frequency domain techniques are more preferable as these techniques are more robust than the spatial methods. Discrete Wavelet Transform is one of the efficient frequency domain techniques and the other variation of this technique is Lifting Wavelet Transform (LWT). In this paper LWT is mainly used for the decomposition purpose and the patient detail in Quick Response (QR) code form is used as the watermark to reduce the payload capacity.

Keywords: Lifting Wavelet Transforms, Integer, Quick Response Code, Payload Capacity

Introduction

Diagnosing the patient's diseases from a remote place has become easy now because of development in the health care systems which provide various ways of data transmissions like telemedicine, telemetry etc. As a result of such technologies the patient's security becomes the major concern [4], and to achieve this, the digital watermarking technology plays a major role with the implantation of security or authentication measures.

Digital watermarking is a process of hiding or embedding some useful information in cover information. In this work, the cover information is medically scanned image such as ultra sound (US), magnetic resonance imaging (MRI), computed tomography (CT) etc and medically scanned ultra sound 2-D video. The patient details is taken as the watermark and converted to QR code. This conversion is done to reduce the data payload in terms of number of bits to be embedded in to the cover information so that there is no or less degradation of the cover information which is an essential requirement in the field of medicine to avoid unnecessary conflicts.

The QR code is an easy way of representation of the data and also it results in high accuracy and consumes less space compared to other previous methods such as barcode [8]. Along with the use of QR code, a secret key is used to enhance the security [2] [3] at the watermark Embedder and decoder side.

As we know that the digital watermarking may be implemented in two domains: spatial and frequency domains and the latter method are more frequently used by most of the researchers because of its accuracy. One of the frequently used techniques in frequency domain is discrete wavelet transform (DWT) and its other variations like lifting wavelet transform (LWT) and integer wavelet transform (IWT).

The Discrete Wavelet Transform (DWT) discretely undergoes sampling and gives the details about both frequency and location/time [1]. As stated above, LWT is substituting DWT as it is more suitable for real time applications and the second generation fast wavelet transform.

The different wavelets used for decomposition method are Haar wavelet, dual-tree complex wavelet transform (DCWT), Daubechies wavelets , non-decimated wavelet transform, Wavelet packet transforms etc.

The Table 1 lists the main properties of these wavelets.

Haar	Daubechies	DCWT
Stores the difference and passes the sum	Generate progressively finer discrete samplings of an implicit mother wavelet function	Shift invariant and directionally selective in two and higher dimensions
Any continuous real function with compact support can be approximated uniformly	Produce smoother scaling functions but larger the size of the filter, vanishing moment is high	Cannot arbitrarily choose the scaling and wavelet filters in the dual tree
Orthogonality in the form	Orthogonality in the form	More directional selectivity

Table1: Properties of Different Wavelet Transforms

From the above table, based on the properties, Haar wavelet is chosen for decomposition with LWT. The main property of LWT is its time invariance but very receptive to the alignment of signal in time. The main application of LWT is in the signal coding in order to represent the discrete signal in more redundant form probably in the data compression form.

In the medical field, the report of a patient is very much essential and a small modification or tampering is not tolerable as it leads to disastrous decisions even by the expertise doctors. If the watermark size is large, it would damage the important content of the scanned image or video. To avoid such damage to the image or video; the watermark size should be very much small and is done by converting watermark in to QR code [5] using QR code generator using the zxing library. The QR code is embedded in the cover information either image or video. At the receiver the QR code is decoded once again using zxing QR code decoder and the embedded data may be validated.

The main advantage of using QR code is [6] [7]; it can encode a larger data i.e. 7089 digits or 4296 characters which includes a combination of punctual marks, special characters, numbers and control codes; it has a high fault tolerance property, i.e. even if the QR is damaged, the data may be read from 30-35% of the damaged data

To avoid the unauthenticated access, a secret key is used both at the embedding and extraction side. There are various ways to use the key such as; Symmetric key i.e. using the same key both at the embedding and extraction side or asymmetric key i.e. a different key can be used at the transmitter and receiver side. The use of the symmetric key at transmitter and receiver side provides more security to the data. The general block diagram for the implementing DWM embedding and extraction for medical scanning image is shown in figure 1 and figure 2 respectively.

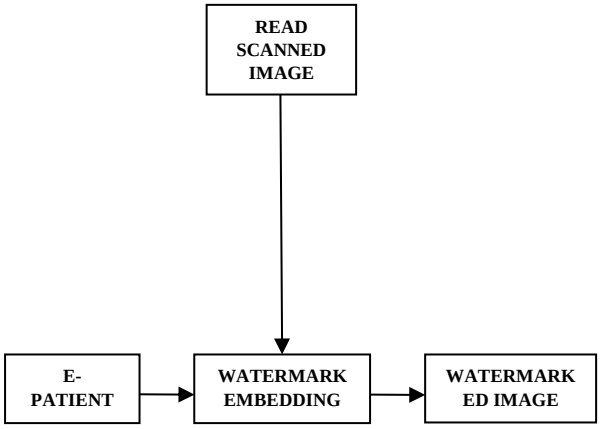


Figure 1. Block Diagram of Watermark Embedding Process

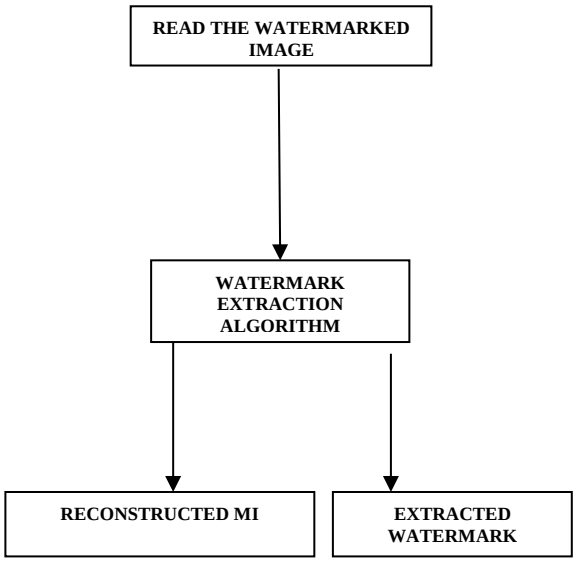


Figure 2. Block Diagram of Watermark Extraction Process

In the Figure 1, the initial step is to read the cover image to be watermarked from the database or directly from the scanning instrument and the second step is to embed watermark information in the cover information using embedding algorithm to get the watermarked information. Along with the watermark, a secret key is generated and is embedded in the cover information. The secured watermarked image can be stored either in the

centralized data base or if required for higher diagnosis it can be transmitted to the specialists.
To perform the embedding process, the alpha blending embedding algorithm is used. Alpha Blending can be proficient in image processing by merging each pixel from the cover source image with the corresponding pixel in the watermark image and is accomplished using the formula:

$$\text{wmi} = (\text{k} \times \text{HHc of CI}) + (\text{q} \times \text{HHw of WM}) \ldots 1$$

Where, wmi = watermarked image
HHc = High Frequency Component of the Original Image
HHw = High Frequency Component of the Watermarked Image
k,q = Scaling Factors for the Original Image and Watermark respectively

In the Figure 2, the watermark extraction block diagram is shown. In this process, the watermarked medical image and secret key are needed. Since this method does not involve the use of original cover image and also the CI and WM can be reconstructed, this technique can be considered as blind and reversible.
The alpha blending extraction watermark algorithm is applied in order to reconstruct the original medical image and also to extract the watermark. If any of the information is not available, it is not possible to extract the information which ensures high security.
To perform the extraction process, alpha blending extraction algorithm is used. According to the formula of the alpha blending the recovered image is given by

$$RCI = (k \times WMI - q * HH\ of\ CI) \ldots 2$$

Where
RCI = Approximation of Recovered Watermark
WMI = High Frequency Approximation of wmi
HH = High Frequency Approximation generated at the receiver side

Proposed Methodology

1. For Medical Image

The proposed DWM technique for medical images and videos implemented with alpha blending algorithm using 3-level LWT is shown in Figure 3.
The steps followed for watermark embedding is explained below:

1) The cover medical image to be authorized is read either from the database or scanning machine and resized.
2) The information to be secured and embedded is read and resized to the same size as that of step 1.
3) The 3-level LWT is applied to cover and watermark information as the deeper level contains more information and less noise.
4) Embed the watermark information (patient detail) and the key generated using pseudorandom sequence in to the cover image using alpha blending algorithm.
5) Apply 3-level inverse LWT to get the watermarked image.

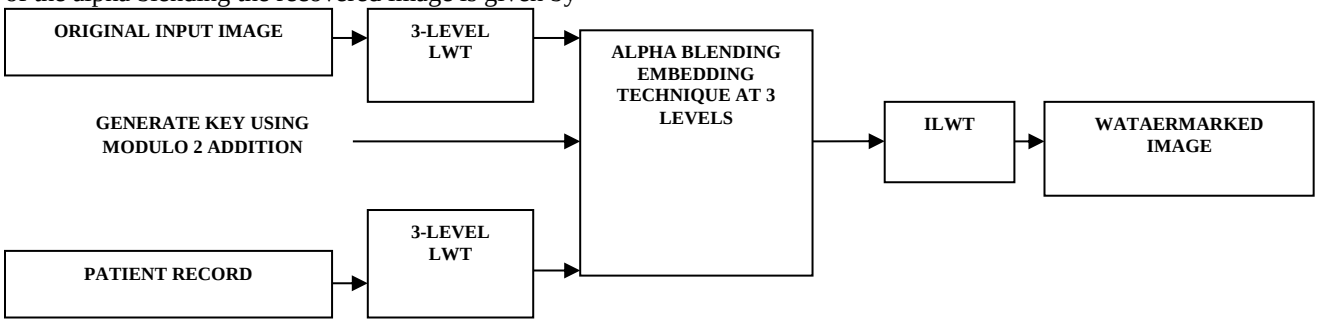


Figure 3. Proposed Block Diagram of Watermark Embedding System

In the traditional watermarking process, an approach of hiding the patient detail as watermark into the input medical cover and the generation secured watermarked image is explained.

- The source scanned medical image is read and subjected to 3-level LWT decomposition to form low and high frequency elements.
- The patient information is read and converted to QR code to reduce the number of bits to be embedded.
- 3-level LWT is applied on QR code of water mark image and it also results in the formation of low and high frequency components.

- The output of 3-level LWT of cover and watermark information is considered as ll3, lh3, hl3, hh3 and ll33, lh33, hl33, hh33 respectively.
- Using high frequency components the keys are generated using modulo 2 addition process as:

$$key1 = hh1 \oplus hh11$$
$$key2 = hh2 \oplus hh22$$
$$key3 = hh3 \oplus hh33$$

- The 3-level watermark and the keys generated are embedded in to the cover information using equation 1 as:
  1. key1 is embedded at the 1-level LWT of CI.
  2. key2 is embedded at the 2-level LWT of CI.
  3. key3 is embedded at the 3-level LWT of CI
- The embedding process is followed by ILWT to form the watermarked image.
- The system will be provided with the password protection which will be known only to the authorized members of the data.

If the report is required either by the patient or doctor, they may get access to the data using the pass word and also to validate the data they need to proceed with the extraction process. The process of watermark extraction is described below:

1. Read the watermarked medical image and apply 3-level LWT.
2. In case of cover image reconstruction, the keys are extracted and these keys are used in the alpha blending extraction algorithm to reconstruct the original image.
3. To construct the watermark, the LWT frequency components of watermarked image are used in the extraction algorithm.
4. The step 2 or 3 is followed by the inverse LWT to construct either watermark or cover image.

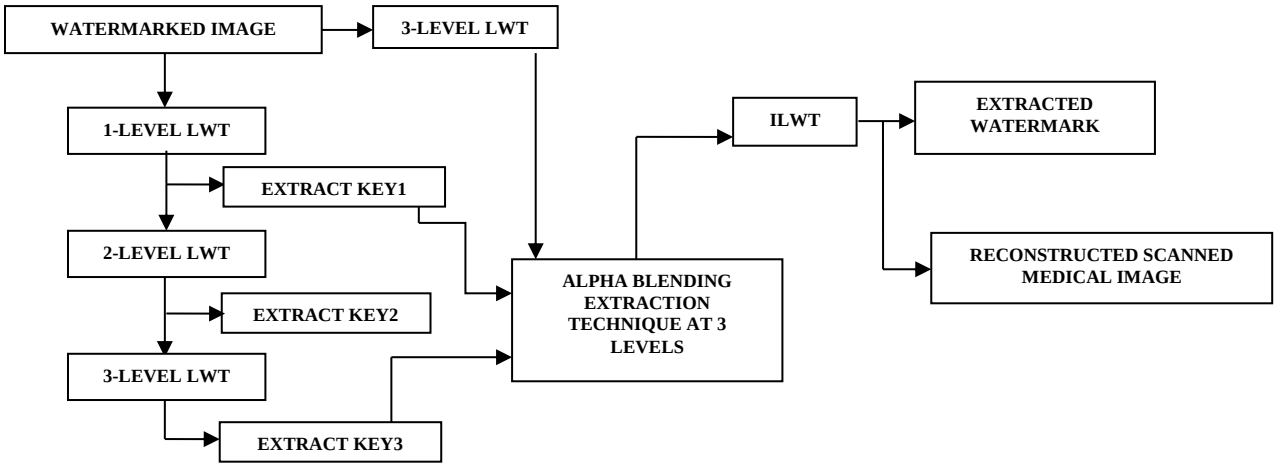


Figure 4. Proposed Block Diagram of Watermark Extraction System

The watermark extraction processes involves the reconstruction of watermark and cover information and is described below:

- In the case of construction of watermark, the watermarked medical image is read and subjected to 3-level LWT to get low and high frequency components.
- The 3-level frequency component is used in the extraction algorithm and the result is followed by inverse LWT to get watermark.
- In the case of reconstruction of cover image, the keys are extracted at each level by applying LWT and the frequency components are generated using modulo 2 subtraction process.

$$hh'3 = key3 \ominus hh'33$$

$$hh'2 = key2 \ominus hh'22$$

$$hh'1 = key1 \ominus hh'11$$

- These frequency components are use by equation 2 and followed by inverse LWT to reconstruct cover image.

The same algorithms are used by in the medical videos watermark embedding and extraction process. The process of video to frame conversion is described below:

2. For 2-D Medical Video

Video to frame conversion, embedding and extraction process:

- 2-D Medical videos are read from the data base in the form of mp4, mpg, and avi format.

- The medical video consisting number of frames is read using video reader command and stores the properties of the video.
- Initialize the video parameters and create empty frames.
- Resize the frame to a square matrix as the calculation of LWT values needs a standard size and also resize watermarking image to the size video frame.
- RGB video frames are transformed to individual components, Red, Green and blue and evaluated by way of Channel separation.
- Convert RGB watermark image to gray scale.
- Perform 3-level LWT on individual channels R, G and B.
- Now the embedding process can be carried out in the similar way as that of medical image.
- Now the watermarked frames are converted into watermarked video by converting the frames to video using frames to video converter.
- For extraction process the same procedure is followed as that of the medical except that watermarked video is converted to frame and after the extraction process frame to video conversion is followed.

Results and Discussion

Performance of the proposed system is evaluated based on the consistency and efficiency using the performance PSNR, MSE and NCC [10]:-

Mean Square Error (MSE): Mean Square Error (MSE) is used to measure the average of the squares of the errors or deviations in terms of the difference between the estimator and what is estimated.

Peak Signal to Noise Ratio (PSNR): PSNR is used to analyze quality of image and video files in decibels.

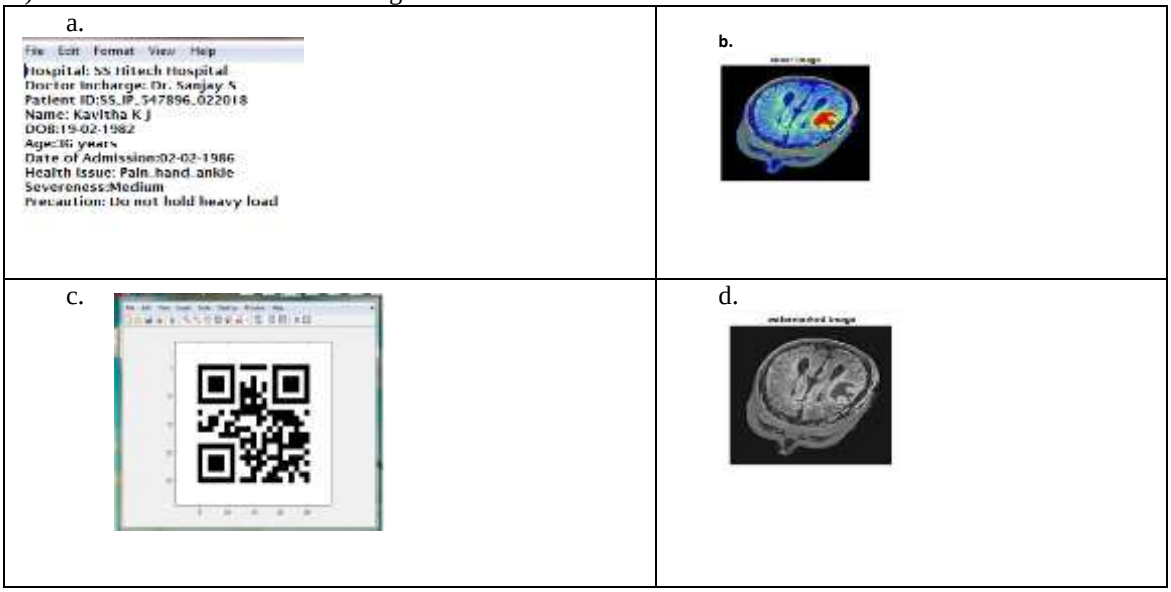
$$\mathbf{MSE} = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\left(|\mathbf{mi_{ij}} - \mathbf{wmi_{ij}}|\right)^2}{\mathbf{m \times n}} \quad \text{-------3}$$

$$\boldsymbol{PSNR} = \mathbf{10}\log_{10}\frac{\mathbf{255^2}}{\boldsymbol{MSE}} \quad \text{----------4}$$

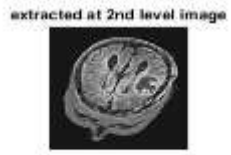
Normalized Cross Correlation (NCC): The NCC measures the similarity between the original and extracted images as:

$$\boldsymbol{NCC} = \frac{\boldsymbol{\sigma mi, wmi}}{\boldsymbol{\sigma mi \sigma wmi}} \quad \text{----------5}$$

Where **mi** and **wmi** represents the original cover image/video and watermarked image, respectively; and where $\boldsymbol{\sigma mi}, \boldsymbol{\sigma wmi}$, and $\boldsymbol{\sigma mi, wmi}$ denote standard deviations and covariance respectively. NCC values near unity indicate high correlation and thus high robustness. The system is also evaluated between the constructed watermark/cover information and the original data. The proposed algorithm is executed in MATLAB 2015a and the parameters are evaluated to check the robustness. The result obtained for the embedding and extraction process is shown in figure 5.



e.



f.

Figure 5. (a) Patient Detail(b) Cover Image (c)QR Code of (b) (d)Watermarked Image (e) Reconstructed Image (f) Extracted Watermark.

The Table1 shows the performance evaluation for invisible watermarking process.

COVER IMAGE SIZE=256×256 AND WATER MARK IMAGE SIZE=40x40					COVER IMAGE SIZE=512×512 AND WATER MARK IMAGE SIZE 40x40				COVER IMAGE SIZE=1024×1024 AND WATER MARK IMAGE SIZE=40x40			
Q	K=0.8 to 1											
	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE
0.00001To 0.1	77.2854	0.0012	0.9078	0.0997	77.1175	0.0013	0.9942	0.0997	77.0034	0.0013	0.901	0.997

Table 1: Original Cover Image and the Watermarked Image when wm is used as a QR Code

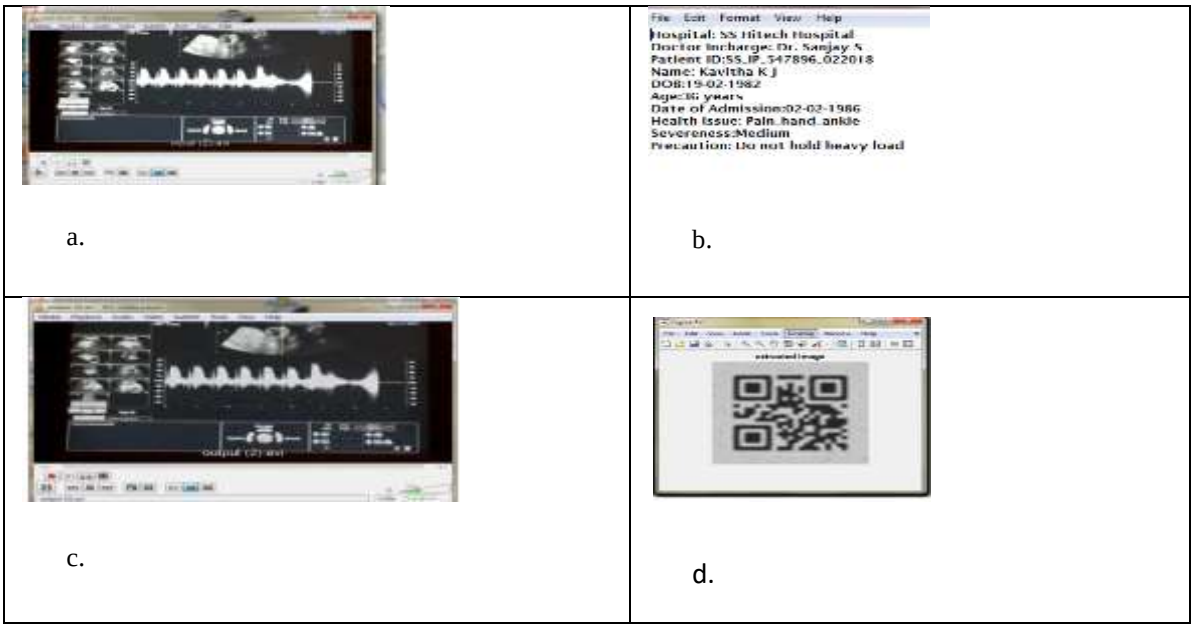
COVER IMAGE SIZE=256×256 AND WATER MARK IMAGE SIZE 40x40					COVER IMAGE SIZE=512×512 AND WATER MARK IMAGE SIZE 40x40				COVER IMAGE SIZE=1024×1024 AND WATER MARK IMAGE SIZE 40x40			
Q	K=0.8 to 1											
	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE
0.00001 To 0.1	86.9327	0.00013	0.999	0.081	94.9866	0.000206	0.9999	0.003	100	0.000005	1.00	0.002

Table 2: Original QR Image and the Extracted QR Image

COVER IMAGE SIZE=256×256 AND WATER MARK IMAGE SIZE 40x40					COVER IMAGE SIZE=512×512 AND WATER MARK IMAGE SIZE 40x40				COVER IMAGE SIZE=512×512 AND WATER MARK IMAGE SIZE 40x40			
Q	K=0.8 to 1											
	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE	PSNR	MSE	NCC	NAE
0.00001 To 0.1	79.498	0.0000007	0.9981	0.0327	84.015	0.0000257	0.999	0.0185	90.28	0.000006	0.9997	0.0078

Table 3: WM Image and the Extracted WM Image

The results of video watermarking are as shown below:



a. b.

c. d.

Figure 6. (a) Input Video Frame (b) Watermark (c) Watermarked Video Frame (d) Extracted Secret Image.

In this proposed system, QR code of patient details is embedded into the medical image and medical videos. The keys generated using the frequency components increase the security and robustness of the information. The system is evaluated using the quality metric parameters. The comparison is shown between the cover image, watermarked image, QR code, extracted QR code and we can see that the proposed system gives better results. The elapsed time for performing the process is also less and is 62.19 seconds for images and 102 seconds for videos.

Conclusion

In this paper a joint blind watermarking approach based on QR code [9] is proposed for providing the security, authentication of the medical scanning images and medical videos. The algorithm is implemented using the high frequency components which contains less information/details. The algorithm is implemented is using MATLAB 2015a. The maximum PSNR obtained is more than 90 db. And also MSE, NCC and NAE values are optimal. In future, we can improve the tolerance of the algorithm by developing some new encryption and QR code generation technologies and implementing the blind watermarking in the low frequency components to increase the robustness.

References

1. Ai-haj, "Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images," 2016.
2. C. Engineering and C. Engineering, "A security technique based on watermarking and encryption for MI," pp. 3–6, 2015.
3. A. Babu, "A Reversible Crypto-Watermarking System for Secure Medical Image Transmission," pp. 1–6, 2015.
4. C. Su, J. Huang, C. Shih, and Y. Chen, "Reversible and Embedded Watermarking of Medical Images for Telemedicine," pp. 145–150, 2015.
5. M. S. Hassanein, "Secure Digital Documents Using Steganography and QR Code," no. November, 2014.
6. D. Cho, "A Study on Effective Digital Watermarking Method Suitable for QR code," vol. 51, pp. 94–97, 2014.
7. J. Waleed, H. D. Jun, S. Saadoon, and S. Hameed, "An Immune Secret QR-Code Sharing based on a Twofold Zero- Watermarking Scheme," vol. 10, no. 4, pp. 399–412, 2015.
8. J. Chen, W. Chen, and C. Chen, "Identification Recovery Scheme using Quick Response (QR) Code and Watermarking Technique," vol. 596, no. 2, pp. 585–596, 2014.
9. L. Laur, P. Rasti, M. Agoyi, and G. Anbarjafari, "A Robust Color Image Watermarking Scheme Using Entropy and QR Decomposition," vol. 24, no. 4, pp. 1025–1032, 2015.
10. N. I. Yassin, N. M. Salem, and M. I. El Adawy, "Medical Video Watermarking Scheme for Electronic Patient Records," vol. 76, no. 1, pp. 12–17, 2013.

