© 2017 IJSRSET | Volume 3 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

An Efficient Multiple Data Hiding Technique for Medical Images Using QR Code Authentication

Navjot Singh*[1], Deepak Sharma[2]

[1,2]Computer Science and Engineering, Adesh Institute of Engineering and Technology, Faridkot, Punjab, India

ABSTRACT

The paper proposes an efficient algorithm using second-generation wavelet (SWT) and SVD based hybrid feature extraction methods for used for medical images watermarking. Combining the strong feature of embedding and extraction techniques like stationary wavelet transform(SWT) and Singular Value Decomposition(SVD), enables the selection of the regions in an in an image which provides high level of imperceptibility after embedding the watermark. The algorithm provides a double level of security by embedding the QR code of the hospital along with its logo for the purpose of content authentication. The evaluation of imperceptibility has been done using performance metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), correlation.

Keywords: QR code, SWT, SVD, Biorthogonal Wavelets

I. INTRODUCTION

With the rapid advancement in technology, there has also been a rapid increase in the need for security of any data that is transmitted or received. Since, digital images can be manipulated or duplicated easily, there is an increased necessity for copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In medical images, this ensures that the diagnosis carried out by one doctor and one hospital cannot be legally claimed by another doctor or another hospital. Data hiding in medical images also plays a key role in forensics involving fingerprints and palm prints. While they can be used as an authentication mechanism for accessing the data base of patients, they can also be used to detect any tampering that has been done with the records in order to destroy them. The same concept of medical data base management could be extended to creation and management of a criminal data base record for retrieval and matching purposes. When done on a global scale in a centralized mechanism, they drastically reduce time.

Intellectual property protection remains the biggest concern and challenge today with the intrusion of internet in everyday life thus providing everyone with an illegal right to copy. However to counter this threat, a lot of measures and techniques have been developed to protect the multimedia data from piracy. Various techniques which have been developed to secure the data include cryptography, steganography and watermarking. Out of all these techniques, watermarking techniques have shown to be more secure and robust than steganographic and cryptographic techniques. Watermarking is used in different types of application such as copyright protection, data monitoring and data tracking.

Watermarking is a technique of embedding the authentication data into the data which needs to be secured [1]. Multimedia watermarking is to embed the copyright information in a multimedia data (text, images or video) and make it secure using key (watermark), so that nobody can copy the data and distribute it illegally. The watermark should be resistant to malicious attacks and common signal processing operations e.g., filtering, noise, and video compression. Watermark may contain the information about origin, status or recipient of host data. If the existence of the hidden information is known it is difficult for the attacker to destroy the watermark, even if the principles of embedding watermark are known to the attacker. In cryptography this law is known as Kirchhoff's law [2].

Watermark should be imperceptible and convey as much information as possible. A block diagram of basic watermarking technique is illustrated in figure 1.1. As authentication and content protection is an integral part of the watermarked images, they protect the rights of their owner in variety of ways, including: Copyright identification User identification, Authenticity determination, Frame dropping, frame swapping.

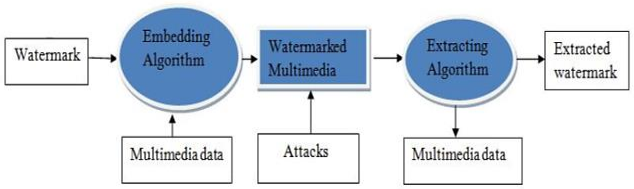

Figure 1. Basic Block Diagram of Watermarking Scheme

A. Types of watermarking

1) According to Human perception

- Visible Watermarking: In this type of watermarking, the embedded information (watermark) is visible in the host data.
- Invisible Watermarking: The embedded information (watermark) is not visible in the host data; however it can be detected algorithmically.

2) According to Type of Document

- This Text Watermarking: In this watermarking, the host data is a text document.
- Image Watermarking: In this watermarking, the Watermark information is embedded in the Image as a multimedia document.
- Audio Watermarking: In this watermarking, the Watermark information is embedded in the Audio as a multimedia document.
- Video Watermarking: In this watermarking, the Watermark information is embedded in the Video as a multimedia document.

3) According to Recipient Application

- Blind Watermarking: The receiver does not require the original watermark while extracting the watermark from watermarked data.
- Non-Blind Watermarking: The receiver requires the original watermark while extracting the watermark from watermarked data.

4) According to Type of Domain

- Spatial Domain: Early watermarking worked in spatial domain, where the watermark is added by modifying the pixel values. Watermarking in spatial domain is simple and low complexity methods are used. The watermark is usually embedded in the luminance component and color component of the image. Watermarking in spatial domain is easy to implement, but it is too fragile as it is incapable of resisting various attacks.
- Frequency Domain: Due to limitations in spatial domain watermarking, the researchers directed towards frequency domain watermarking. In this domain the watermark is embedded not to intensity pixels of frame but to the transform and to embed into frequency coefficient. Various techniques to embed watermark in frequency domain are DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform) which are robust against many intentional and unintentional attack.

B. Video watermarking

Video watermarking is to embed the data or text in video is called video watermarking this is the invisible type of watermarking which can be detected algorithmically. The following aspects are important for designing of video watermarking systems:

- Imperceptibility: Watermark should be unable to detect with naked eyes
- Robustness: Watermark must be robust against various common signal processing attacks.
- Security: The embedded information must be secure against illegal users.
- Capacity: The amount of embedded information that can be hidden in video and be large enough to uniquely identify the owner of the video.

The basic philosophy in majority of the transform domain watermarking schemes is to modify transform coefficients based on the bits in the watermark image. Most of the domain transformation watermarking schemes works with DCT and DWT. However, SVD is one of the most powerful numerical analysis technique and used in various applications. The paper is organized as follows. Section 2 gives a detailed description of various concepts used for implementation. Section 3 explains in detail the proposed algorithm. Section 4

describes the outcomes and results and also provides an analysis of the same. The conclusion and future scope is presented in Section 5.

II. METHODS AND MATERIAL

1. Introduction of Techniques Used

A. Singular Value Decomposition (SVD)

Singular value decomposition is a mathematical technique to decompose a matrix A into three matrices USV, U and V are orthogonal matrices and S is a singular matrix. Mathematically theorem is represented as $A_{mn}= U_{mm}S_{mn}V_{nn}^{T}$. In the paper[3] proposed that when the embedding of watermark was done in both U and V components of SVD, it will increase the embedding capacity and invisibility[4]. The paper proposed that SVD technique is used in frequency domain to make it robust against various attacks and increased the amount of hidden information by embedding the information in singular matrix of SVD.[5]Proposed that to embed the information by modifying the least significant bit of singular value matrix to increase security of watermarking.

B. Stationary Wavelet Transform(SWT)

A multi-layer stationary wavelet transform (SWT) [11] was adopted to overcome the limitation of the traditional wavelet transform

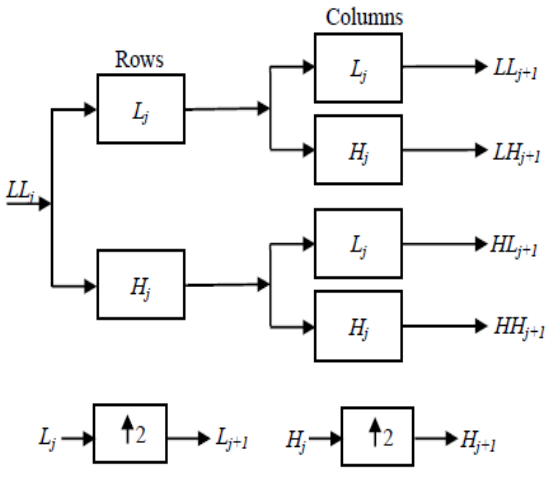

Figure 2. decomposition operation of SWT.

Hj and Lj represent high-pass and low-pass filters at scale j, resulting from interleaved zero padding of filters Hj-1 and Lj-1 (j>1). LL0 is the original image and the output of scale j, LLj , would be the input of scale j+1. LLj+1 denotes the low-frequency (LF) estimation after the stationary wavelet decomposition, while LHj+1, HLj+1 and HHj+1 denote the high frequency (HF) detailed information along the horizontal, vertical and diagonal directions, respectively.

These sub-band images would have the same size as that of the original image because no down-sampling is performed during the wavelet transformation.

C. QR Code

Quick Response code (2 D matrix Code). It contains the information to which it is attached. The QR code system became popular due to its faster readability and greater storage capacity as compared to bar code. Internal Structure of the same has been described in [9]. The proposed technique has been compared to the technique described in [9] for performance assessment.

2. Proposed Technique

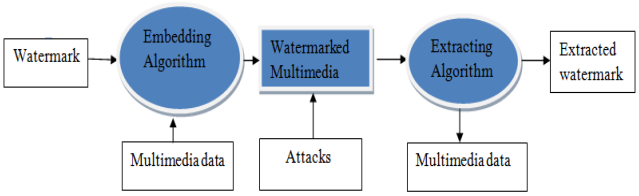

Figure 3. Block diagram of proposed image watermarking

A. Embedding process

The entire process of embedding the QR code and the logo into the medical is described in Fig. 4. In embedding process SWT image is applied on the B frame of image after separating the R, G, B components and then SVD is applied for the purpose of feature extraction of the image.

In a similar manner, the same process is applied on the logo and QR code. The singular values of logo are embedded inside the B frame to generate an intermediate image. Thereafter the QR code is embedded into the singular values of intermediate image. Finally after embedding both QR code and logo, the inverse transform is taken and images are concatenated to generate the watermarked image.

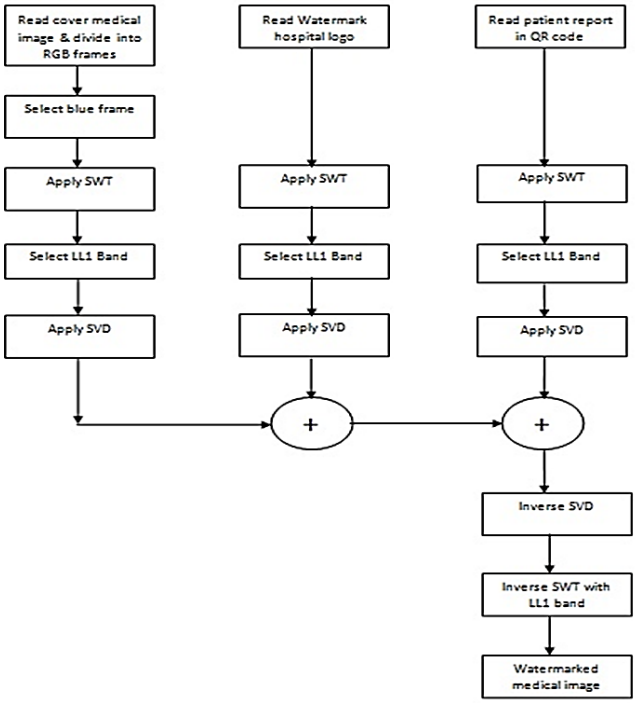

Figure 4. Flowchart of the proposed embedding process

1) Embedding Algorithm:

i. Read the medical image file.

ii. Separate the RGB channels of image. (I_{host}) = (*IR*,*IG*,*IB*).

iii. Apply SWT on *IB* and consider LL Sub-band IB_{LL}

iv. On the IB_{LL} take SVD.

$$[IB_{LL}]_{m*n} = U_{Host_{[m*n]}} * S_{Host_{[m*n]}} * V_{Host[m*n]}$$

v. Take the watermark logo l_{logo} and similarly apply the SWT

vi. On l_{logoLL}. take SVD.

$I_{logoLL\,[m*n]} = U_{Logo[m*n]} * S_{Logo[m*n]} * V_{Logo[m*n]}$

vii. Embed the S_{Logo} into S_{Host} using

$S_{IW}=S_{Host}+\alpha\, S_L$

viii. Consider the QR code as watermark I_{QR} Apply the SWT.

ix. On $I_{QR_{LL}}$ apply SVD

$$I_{QR_{LL}} = U_{QR[m*n]} * S_{QR[m*n]} * V_{QR[m*n]}$$

x. Embed the QR code into the intermediate watermarked

$$SW = SIW + (a\ )SQR$$

to make it watermarked B frame $I_{Watermark}$ by using ISWT

xi. Concatenate all frames and make the watermarked image.

B. Extraction Process

The entire process of extraction of the embedded QR code and the logo into the video is described in Fig. 5. In extraction process is completely reverse of the embedding process.

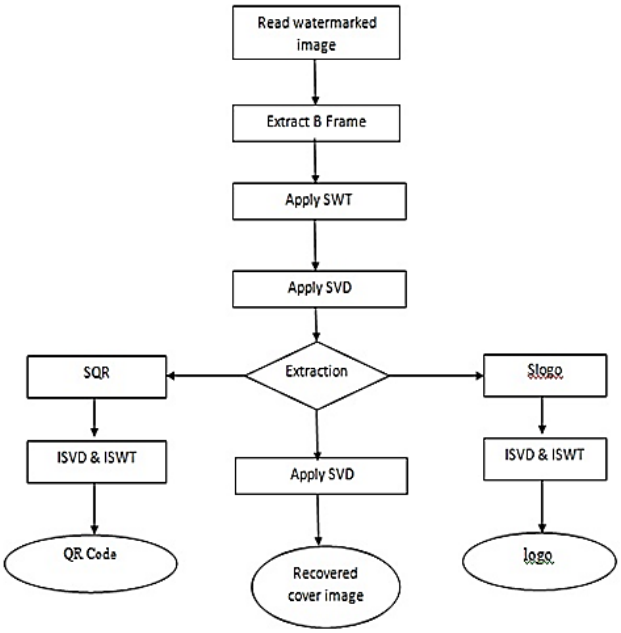

Figure 5. Flowchart of the proposed extracting process

1) **Extraction Algorithm:**

i. Receive the watermarked image.

ii. Separate the RGB channels of selected frame

$$Iwatermark = (l_{WR}, l_{WG}, l_{WB})$$

iii. Take the frame l_{WB} apply SWT and consider LL sub-band .

iv. On sub-band l_{WB} LL apply SVD

v. Extract the singular values of QR code

$$S_{QR} = S_W - S_{IW} / a \ \text{S}$$

vi. Apply ISWT on S_{QR} and extract QR code.

vii. Extract the singular values of Logo $S_{logo} = S_{IW} - S_{Host} / \alpha$

Apply ISWT and extract the logo

III. RESULTS AND DISCUSSION

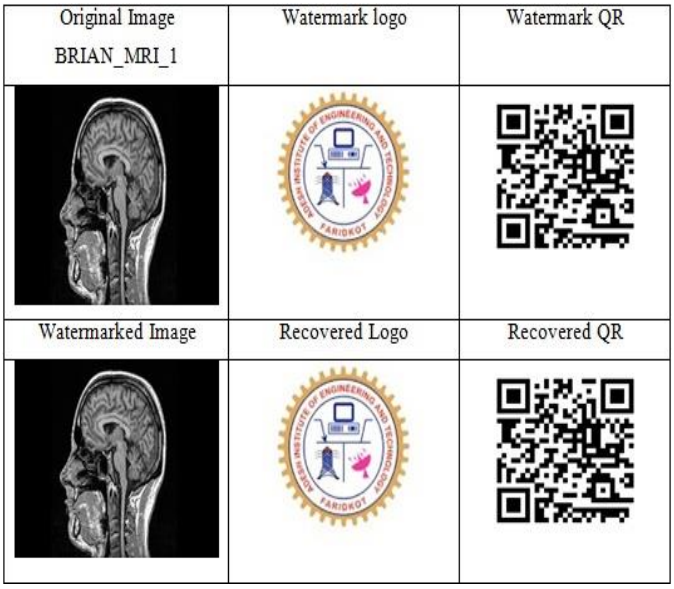

Figure 6. Pictorial representation of original and watermarked medical image

BRIAN_MRI_1	Existing algorithm		Proposed algorithm	
K	PSNR	COR	PSNR	COR
0.02	52.743550	0.9314	68.7172	1.000
0.05	51.916029	0.9867	61.2689	1.000
0.8	42.421644	0.9999	45.2089	1.000
1	40.906702	1.0000	45.0521	1.000

Figure 7. Comparison of Existing & Proposed Algorithm at various intensity values

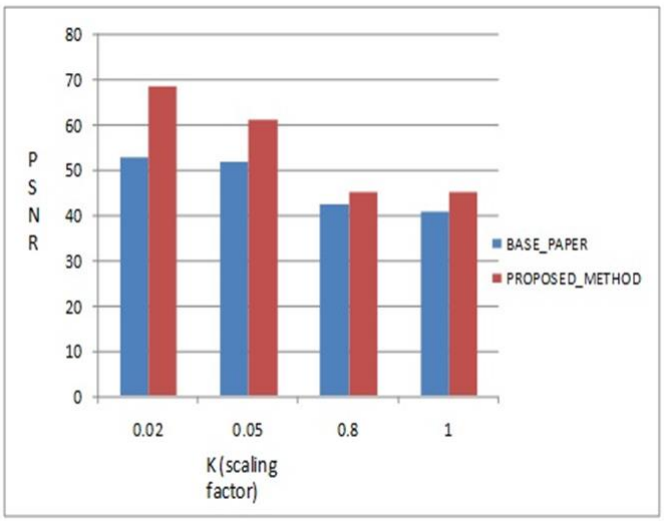

Figure 8. Pictorial comparison of various performances metrics of existing and proposed method.

IV. CONCLUSION

The proposed technique has combined many powerful feature extraction techniques and thus improved the performance considerably of the existing algorithm. The improvement in performance has been corroborated with results obtained as depicted through tables and graphs.

V. REFERENCES

[1]. R. Christian, A. Sophia, "A Survey of Watermarking Algorithms for Image Authentication" EURASIP Journal on Applied Signal Processing, Vol. 6, pp. 613–621, 2002.

[2]. H. Frank, K. Martin, "Multimedia Watermarking Technique", Proc. of the IEEE, Vol. 87, No. 7, pp. 1079-11096, 1999.

[3]. C. Kuo-Liang, Y. Wei-Ning, et al , "On SVD Based Watermarking Algorithm", ELSEVIER Journal of Applied Mathematics and computation, Vol. 188, pp 54-57, 2007.

[4]. H. Suhad, A. Moussa, et al , "Digital Image Watermarking using localized Biorthogonal wavelets", European Journal Of Scientific Research, Vol.26, No.4, pp 594-608, 2009.

[5]. D.Sengul, T.Turker et al, "A robust color image watermarking with Singular Value Decomposition method", ELSEVIER Advances in Engineering Software, pp 336-346, 2011

[6]. Sweldens, W, "The lifting scheme: A New Philosophy in Biorthogonal Wavelet Constructions" Proc. of SPIE, pp. 68-79, 1995.

[7]. I. Daubechies, W. Sweldens, "Factoring Wavelet Transforms into Lifting Schemes", The Journal of Fourier Analysis and Applications, Vol. 4, pp. 247–269, 1998

[8]. M. Arya, R. Siddavatam. "A Novel Biometric Watermaking Approach Using LWT-SVD." Information Technology and Mobile Communication. Springer Berlin Heidelberg, pp. 123-131, 2011.

[9]. N. Kor Ashwini, N.M . Kazi, "A Watermark Technique Based On SVD And DWT Composite Function With QR code", International Journal Of Application Or Innovation in Engineering & Management , Vol. 3, No. 7, pp 20-28, 2014

[10]. Abhilasha Sharma et al, "Secure Hybrid Robust Watermarking Technique for Medical Images", 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015 Elsevier