Hybrid DCT-SVD Based Digital Watermarking Scheme with Chaotic Encryption for Medical Images

Ahmed A Mohammed\textsuperscript{1}\textsuperscript{*}, Bilal A Jebur\textsuperscript{1} and Karam M Younus\textsuperscript{1}

\textsuperscript{1}College of Electronics Engineering, Ninevah University, Nineveh, Iraq

\textsuperscript{*}E-mail: ahmed.mohammed@uoninevah.edu.iq

Abstract. The quality of medical image is crucial due to the sensitivity of medical diagnoses. Nowadays medical images are commonly shared between various entities across the medical sector to improve the quality of diagnoses. Thus, watermarking process is usually applied on these images to embed patient’s private information. One of the key challenges is preserving image quality, keeping it clean of distortions after the watermarking process, and sustaining robustness. In this work, a hybrid Discrete Cosine Transform (DCT) and Singular value decomposition (SVD) based image watermarking scheme with chaotic encryption is proposed. The obtained results have demonstrated that the proposed scheme is secure and robust compared to the present schemes. In particular, the results show decent robustness and excellent imperceptibility of watermarked host medical images. Moreover, Peak signal to noise ratio (PSNR), and Normalized Correlation (NC) are used to evaluate the performance of the scheme. The scheme has shown a minimum PSNR of 59 dB and an NC value of 1 with no attacks applied, and not less than 0.5 with the presence of various attacks.

1. Introduction

Recently, Medical images are being circulated between two or more doctors for accurate diagnoses and exchange of expertise. On the other hand, access to multimedia has witnessed a noticeable increase due to the Internet growth. Consequently, the copyright protection of digital images, video, etc., becomes more vulnerable to be unauthorized access. One of the most recent solutions to the aforementioned problem is digital watermarking. Two types of watermarking could be used, visible and invisible, however, invisible watermarking is preferred for privacy and security\cite{1}. Subsequently, invisible watermarking will be used in this research. The use of watermarking has been adopted since 1990. The early algorithms were based on two main categories, spatial domain and transform domain. However, the spatial domain watermarking is less robust than the transform domain watermarking, the main reason behind that is the image under attack is usually prone to pixel value alteration which leads to loss of embedded payload information, and that makes it irretrievable\cite{2}, on the contrary, using the transform domain as a watermarking embedding environment will provide more robustness since the original payload is inserted within the modified coefficients of the transform and not directly to the image pixels\cite{3}. There are several main watermarking requirements in which the designer takes into account when designing a watermarking algorithm. The most common is robustness and transparency\cite{4}. The watermarked image has to be robust against attacks like signal processing attacks, geometric attacks amongst other attacks.

The SVD has been used by researchers for watermarking, although the SVD has the problems such as false-positive, still very reliable in watermarking when combined with other transforms (i.e. hybrid domain) like the discrete wavelet transform (DWT), DCT and discrete Fourier transform (DFT)\cite{5}. Transparency on the other hand is crucial and must be taken into consideration in parallel with robustness, depending on the type of data and application, a fair trade-off between robustness and transparency must be realized\cite{6}. The main issue with medical images is that they are case-sensitive when it comes to medical decisions. Most present medical image watermarking schemes focus on
robustness alongside with transparency but still not paying enough attention to keeping the medical image fully undistorted. In this study we propose a hybrid domain watermarking scheme in DCT-SVD domain and our aim is to achieve highest transparency possible with robust algorithm against various attacks.

2. Related Work
The authors in [7] employed a Hybrid Transform scheme, which comprises DWT, DCT, and SVD, to ensure the security of the electronic patient record (EPR) transfer between health sector institutions. Although their scheme robustness is high, low transparency is noticed regarding the embedded binary payload. The DWT-SVD was proposed in [8] as a dual watermarking technique to secure the transmitting of the medical images. Moreover, Hamming error correction code was used to reduce the effect of channel noise, which in return improved the security level as Hamming code usually adds extra bits for error detection and correction to data to be transmitted, in this case watermarked image, results were acceptable transparency and robustness-wise compared to the scheme proposed in [9]. A wavelet-based watermarking technique was proposed in [10] to conceal the ECG signals in a QR code, which has shown performance that surpasses in terms of retrieval quality and embedding capacity compared with works proposed in [11] and [12]. An optimized and robust watermarking technique has been proposed in [13] combined with a firefly algorithm of Lifting Wavelet Transform (LWT). Additional Security has been added by scrambling the watermark before embedding the fusion of DWT, sanitization Algorithm and Oppositional Grasshopper Optimization Algorithm (OGAO) embedded the secret bits in an optimized locations and shown that this technique offers enhanced imperceptibility when put into comparison with proposed works in [14] and [15]. Ali et al. presented a reliable for the transmission-secure watermarking scheme of images [16]. The Redistributed Invariant DWT, Artificial Bee Colony (ABC) optimization with SVD has been used to obtain transmission secure watermarking technique and the human visual system has been used to embed the Watermarks in blocks. Authors in [17] presented an SVD robust watermarking algorithm using colored images and also used the human visual system along with Particle Swarm Optimization (PSO) for automatic selection of embedding position. In [18] a mix between LWT and SVD with Arnold Cat Map (ACM) for upgrading the security algorithms have been used in for color images with secure watermarking for copyright protection. For improving the trade-off amid perceptual quality and robustness, Grey Wolf Optimization (GWO) technique has been used also, in [19] the presented scheme used SVD-PSO with Improved Discrete Wavelet Transform (IDWT) for a reliable embedding of the watermark , the entropy adapted to locate the suitable embedding environment. the compensation between robustness and perceptual quality is managed using PSO as an optimization algorithm.

From the aforementioned works, we notice that the main concern with medical images is perceptual quality and being case-sensitive which emphasizes that distortions are not allowed i.e., preserving the perceptual quality of the image is crucial and that was the major drawback in all previously listed works since they’ve always focused on robustness as an equal match for imperceptibility and tried to sustain that state of equilibrium. In this developed work, we combined the SVD with DCT for a hybrid embedding domain to achieve better transparency.

3. Preliminaries and Performance Evaluation
3.1. Discrete Cosine Transforms (DCT):
DCT is a transformation technique that is usually used in a large number of image processing schemes. In essence, DCT and IDCT transforms are used to transform images from the spatial domain to the DCT domain. Moreover, the two-dimensional DCT and IDCT are given as
\[
F(m, n) = \frac{2}{\sqrt{MN}} C(m) C(n) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \times \cos \left( \frac{(2x + 1)m\pi}{2M} \right) \cos \left( \frac{(2y + 1)n\pi}{2N} \right)
\]

\[
F(x, y) = \frac{2}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C(m) C(n) f(m, n) \times \cos \left( \frac{(2x + 1)m\pi}{2M} \right) \cos \left( \frac{(2y + 1)n\pi}{2N} \right) \]

3.2. Singular Value Decomposition (SVD)
Singular value decomposition (SVD), is a matrix decomposition technique that has been employed in various signal processing schemes such as (a general tool for numerical linear algebra, data reduction, Digital Watermarking, etc.). The SVD converts any \( N \times M \) rectangular matrix into three matrices, i.e., \( U \), \( S \), and \( V \) such that \[ A = UV^H \]

where \( U \) is an \( N \times M \) matrix that satisfies:

\[
U^H U = I_{N \times N}
\]

and \( V \) is an \( N \times M \) matrix that satisfies:

\[
V^H V = I_{M \times M}
\]

This has made the SVD very useful in size reduction algorithms along with several other algorithms.

3.3. Peak Signal to Noise Ratio (PSNR)
PSNR is one of the most common performance metrics that is usually used to evaluate the effectiveness of image processing algorithms. In particular, it is an empirical measurement that is obtained by dividing the peak signal power by the noise power, which is given as

\[
PSNR = 10 \log \left( \frac{255^2}{MSE} \right)
\]

where, \( MSE \) denotes the mean-square-error, which is expressed as

\[
f(x) = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} |C(x, y) - WC(x, y)|^2
\]

3.4. Normalized Correlation (NC)
The Normalized-Correlation (NC) is a quantitative measurement that is mainly used to compute the similarity between the original and the extracted watermarks. Consequently, it is used as an indication of the effectiveness and robustness of the watermarking algorithms. The NC can be computed as in equation (7).

\[
NC(W, W') = \frac{\sum_{x=0}^{M} \sum_{y=0}^{N} [W(x, y)W'(x, y)]}{\sqrt{\sum_{x=0}^{M} \sum_{y=0}^{N} W(x, y)^2} \sqrt{\sum_{x=0}^{M} \sum_{y=0}^{N} W'(x, y)^2}}
\]

4. Proposed Scheme
In this work, we present a non-blind scheme for medical image watermarking, the medical image is transformed into the DCT domain to get different frequency coefficients, the mid-frequency coefficients are selected using the zig-zag method, next the selected coefficients vector is reshaped into an
$N \times N$ matrix then SVD is applied on the selected coefficients. The SVD diagonal matrix is selected as the embedding domain but before embedding the payload, we encrypt it with a special key along with chaotic scrambling to add another security level to the proposed scheme. The embedding and extracting procedures are explained in the next sub-sections.

![Figure 1. Proposed Scheme](image)

4.1. Watermark Encoding Process
- Read input host image $I$ of size 1024X1024
- Read watermark image $W$, size 64X64
- Encrypt $W$ using chaotic scrambling + key
- Apply DCT on host image: $DCT_{image} = dct2(I)$
- Perform SVD on selected mid-frequency coefficients: $[U S V] = SVD(selected\ mid\ -\ frequencies\ of\ DCT_{image})$
- Embed encrypted $W$ within the diagonal matrix $S$ with a scaling factor of 0.1: $S_{modified\ diagonal\ matrix} = S_{diagonal\ matrix} + scaling\ factor\ k * W_{encrypted}$
- Perform the inverse SVD: $SVD_{modified} = U S_{modified\ diagonal\ matrix} V_{transposed}$
- Finally, apply the Inverse DCT to get the watermarked image $I^*$: $I^* = idct2(DCT_{modified})$

4.2. Watermark Decoding Process
- Read $I^*$ (could be attacked)
- Apply DCT on host image: $DCT = dct2(I^*)$
- Apply SVD on mid-frequencies: $[U_2 S_2 V_2] = SVD(selected\ mid\ -\ frequencies\ of\ DCT\ of\ I^*)$
- Extract watermark $W_{extracted}$: $W_{extracted} = \frac{(S_2 - S)}{scaling\ factor\ k}$

5. Results and Simulation
This section presents the simulation results and analysis. First, two medical images were selected to be the main test host. These images are a Magnetic Resonance Imagining (MRI) of the spine and a Computed Tomography (CT) of the brain. The watermark image is a binary logo that represents an
abbreviation of Ninevah University. Figure 2 shows the watermark image before and after scrambling. On the other hand, figure 3 shows the original test images and their watermarked versions for various PSNR values after the embedding process. In general, A 45 dB of PSNR is the performance threshold above which the performance is considered to be good. In the proposed scheme we attained a minimum of 59 dB in both test images. This implies high transparency and therefore undistorted medical images.

![Figure 2](image1.png)

(a) Watermark, (b) Chaotic Scrambled Watermark

![Figure 3](image2.png)

(a) Host Image 1, (b) Host Image 2, (c) Watermarked Image 1, PNSR= 59.98 dB, (d) Watermarked Image 2, PNSR= 59.01 dB

Figure 3. Original Host Images and Watermarked images

Moreover, figure 4 and 5 show that the attacked images and the extracted watermarks after each attack. They also show the extracted watermark with both objective and evaluations. In essence, different attacks were chosen to test the robustness of the proposed scheme, some are geometric attacks, others are common signal processing attacks.

Gaussian noise attack is applied twice, the variance of the first one was 0.01 and the extracted watermark has an NC value of 0.9774, while the second gaussian attack had a variance of 0.1 and yet the extracted watermark was visible with an NC value of 0.6367. Next, JPEG lossy compression, which is commonly used by most of today’s apps such as; Facebook messenger, Viber, etc., to compress the images before sending them to other parties, can be considered as one of the signal processing attacks. Hence, we investigated the impact of the JPEG lossy compression on the performance of the proposed
scheme, and the extracted watermark after the JPEG attack with a quality factor of 25% has shown an NC value of 0.9951, which implies the robustness of our scheme.

Gaussian Noise, M=0, Variance=0.01, PSNR=21.41 dB

Gaussian Noise, M=0, Variance=0.1, PSNR=12.27 dB

JPEG Q=25%, PSNR=40.1 dB

Histogram Equalization, PSNR=8.77 dB

Random Crop, PSNR=10.89 dB

Rotation 45 degree, PNSR=8.4084 dB

**Figure 4.** Attacks vs. Extractions
Gaussian Noise, $M=0$, Variance=0.01, PSNR= 21.56dB

Gaussian Noise, $M=0$, Variance=0.1, PSNR= 12.1 dB

JPEG Q=25%, PSNR= 39.12 dB

Histogram Equalization, PSNR=9.6 dB

Random Crop, PSNR= 11.1578 dB

Rotation 45 degrees, PSNR=14.54 dB

Figure 5. Attacks vs. Extractions
Finally, the random crop attack was also considered to thoroughly examine the performance of the proposed scheme as the attacker could remove any part/s of the image. The attained results have proved the robustness of the proposed scheme against such a random attack with a minimum NC of 0.7532. More random crop results are illustrated in figure 6.

![Attack Results](image)

**Figure 6.** Attacks vs. Extractions

Tables 1 and 2 show the obtained results for various attack scenarios. A closer inspection of these results shows that the proposed scheme has proved to be resistive against these attacks.

| Attack                           | PSNR in dB | NC   |
|----------------------------------|------------|------|
| Salt & Pepper Noise, Density=0.1 | 13.8907    | 0.7573 |
| Mean Filter 3X3                  | 41.46      | 0.9726 |
| Gemma correction                 | 21.72      | 0.9774 |
| Motion Blur                      | 31.25      | 0.9702 |

| Attack                           | PSNR in dB | NC   |
|----------------------------------|------------|------|
| Salt & Pepper Noise, Density=0.1 | 14.05      | 0.6067 |
Next, Table 3 shows the comparison of the performance of the proposed scheme with those proposed in [7], [10], and [19] in terms of PSNR and NC values.

Table 3. Performance comparison

| Scheme          | PSNR in dB |
|-----------------|------------|
| Our Scheme      | 59.98      |
| [10]            | 58.85      |
| [19]            | 48.25      |
| [7]             | 50.88      |

A closer look at Table 3, shows that our scheme has compromising results with the PSNR value of more than 59 dB in both test images. Subsequently the proposed scheme has managed to keep higher transparency with adequate robustness.

6. Conclusion

Digital Watermarking plays an important role in image copyright protection, for the medical application it can be used to embed patient information within the medical data while keeping high privacy of that information. In this paper, we proposed a robust, reliable, and transparency preserver technique for medical image watermarking. In terms of transparency, the obtained results have shown a minimum PSNR of 59 dB, which is excellent to keep the medical data as original as possible and guarantees no medical decision interference. Moreover, almost all extracted watermarks have shown NC values of 0.9 and more after these attacks, which demonstrate the robustness of the proposed scheme.

7. References

[1] Narayan R 2018 Encyclopedia of Biomedical Engineering. Elsevier
[2] Preedanan W, Kondo T, Bunun P and Kumazawa I 2018 Image quality assessment for medical images based on gradient information in 5th Int. Conf. on Business and Industrial Research (ICBIR) pp 189-94.
[3] Nai Y, Schaefferkoeetter J D, Fakhry-Darian D, Conti M, Shi X, Townsend D W, Sinha A K, Tham I, Alexander D C and Reilhac A 2018 Improving Lung Lesion Detection in Low Dose Positron Emission Tomography Images Using Machine Learning in IEEE Nuclear Science Symp. and Medical Imaging Conf. Proc. (NSS/MIC) pp 1-3.
[4] Mohammed A, Maraş H H and Elbasi E 2014 A new robust binary image embedding algorithm in discrete wavelet domain in IEEE 8th Int. Conf. on Application of Information and Communication Technologies (AICT) pp 1-7.
[5] Segars W P, Tsui B M, Cai J, Yin F-F, Fung G S and Samei E 2017 Application of the 4-D XCAT phantoms in biomedical imaging and beyond IEEE Transactions on Medical Imaging 37 680-92.
[6] Sullivan B J, Ansari R, Giger M L and MacMahon H 1994 Relative effects of resolution and quantization on the quality of compressed medical images in Proc. of the 1st Int. Conf. on Image Processing pp 987-91.
[7] Kumar G P, Saranya M, Tamilselvan K, JL M I and Kavitha S 2020 Investigation on Watermarking Algorithm for Secure Transaction of Electronic Patient Record by Hybrid Transform in Fourth Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) pp 379-83.
[8] Anand A and Singh A K 2020 An improved DWT-SVD domain watermarking for medical information security Computer Communications 152 72-80.

[9] Singh A K, Kumar B, Dave M and Mohan A 2015 Robust and imperceptible dual watermarking for telemedicine applications Wireless Personal Communications 80 1415-33.

[10] Sanivarapu P V, Rajesh K N, Reddy N R, Reddy N C 2020 Patient data hiding into ECG signal using watermarking in transform domain Physical and Engineering Sciences in Medicine 43 213-26.

[11] Jero S E and Ramu P 2016 Curvelets-based ECG steganography for data security Electronics Letters 52 283-5.

[12] Mathivanan P, Jero S E, Ramu P, Ganesh A B 2018 QR code based patient data protection in ECG steganography Australasian Physical & Engineering Sciences in Medicine 41 1057-68.

[13] Chaturvedi A K, Shukla P K 2020 Effective watermarking technique using optimal discrete wavelet transform and sanitization technique Multimedia Tools and Applications 79 13161-77.

[14] Ingale S P, Dhone C 2016 Digital watermarking algorithm using DWT technique International Journal of Computer Science and Mobile Computing 5 1-9.

[15] TN S, Ramesha K and Raj C P 2014 A New Technique to Digital Image Watermarking Using DWT for Real Time Applications International Journal of Engineering Research and Applications 4 102-107 .

[16] Ali M, Ahn C W, Pant M and Siarry P 2015 An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony Information Sciences 301 44-60.

[17] Ahmadi S B B, Zhang G and Jelodar H 2019 A robust hybrid SVD-based image watermarking scheme for color images in IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON) pp 0682-8.

[18] Pandey M K, Parmar G, Gupta R, Sikander A 2019 Lossless robust color image watermarking using lifting scheme and GWO International Journal of System Assurance Engineering and Management 11 320-31

[19] Gangadhar Y, Akula V G, Reddy P C 2018 An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation Biomedical Signal Processing and Control 43 31-40.