A Robust Hybrid Digital Watermarking Approach Using DCT-Fast RSVD For Medical and Non-Medical Applications

Sajeer.M
Department of ECE
NIT, Calicut
sajeer_p210095ec@nitc.ac.in

Ashutosh Mishra
Department of ECE
NIT, Calicut
ashutosh@nitc.ac.in

2022 IEEE 6th Conference on Information and Communication Technology (CICT) | 978-1-6654-7312-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/CICT56698.2022.9997855

***Abstract*—Medical image watermarking (MIW) is a widely used method today to confirm the validity of medical data. This paper proposes a hybrid, robust, semi-blind and imperceptible MIW system using the Discrete Cosine System (DCT) and Fast Randomized Singular Value Decomposition (FRSVD) with less computational complexity and computational time; relevant to both medical and non-medical images. Multiple scans and assessment matrices are used to evaluate the efficacy of the suggested technique, and it is compared to cutting-edge methodologies. The procedure obtained a maximum Peak Signal to Noise Ratio (PSNR) of 81.71 dB, Structural Similarity Index (SSIM) of 1, and Normalized Coefficient (NC) value of 1 for all the attacks. The suggested scheme achieved a meager embedding time and extraction time; 0.1638 seconds and 0.0955 seconds, respectively.**

***Index Terms*—Medical Image Watermarking (MIW), hybrid technique, DCT, fast RSVD, chaotic encryption, PSNR, SSIM, NC.**

I. Introduction

Telemedicine, is becoming popular in the innovative health care system, where doctors can diagnose a patient at a distance. The main issue related to this scenario is ensuring the privacy and security of medical data. An attacker can easily hack the system and modify these records, leading to misdiagnosis, delay in treatment, or even the patient's death. Encryption is a technique that can be used for medical data protection [1], but the intruder alters that once he decrypts the information. Medical Image Watermarking (MIW) can be effectively used in this situation, which authenticates the integrity of the data. Here a watermark is inserted into the original data from the sending side; later, it can be retrieved by the receiver. Mainly there are three critical features of a MIW system-imperceptibility, robustness, and embedding capacity. There is always a trade-off between these parameters. Imperceptible indicates the visibility of the watermark in the original cover data; robustness is the ability to withstand watermarking attacks, and capacity gives the idea regarding the amount of information that can be inserted into the original data [2]. MIW may be of the spatial, transform, or hybrid type. The pixels of the original data are modified to embed the watermark; in the case of the spatial domain (Least Significant Bit (LSB) watermarking). The transformed coefficients of the host data are altered in the transform environment MIW (DCT, Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) based watermarking). The spatial type has the advantages like high imperceptibility and less computational time, but it is vulnerable to most watermarking attacks. Transform domain watermarking schemes have the benefit of high robustness against watermarking attacks. A hybrid domain scheme combines various transform domains or spatial domains or a combination of both transform and spatial domain approaches. It has advantages over all the domain techniques, like high invisibility, better robustness, and less computational time.

Recently there have been different MIW techniques suggested by various authors. A zero watermarking strategy was presented for medical data protection in [3]. The approach used the Multi-Level Discrete Cosine Transform and Dual-Tree Complex Wavelet Transform to collect the host medical image's low-frequency sub-band. Hessenberg Decomposition (HD) obtains the visual feature vector. They employed logistic chaotic position shuffling of the binary watermark picture to beef up security. Yang Xiu Fang *et al.* [4] developed an algorithm for medical image watermarking. Here they used Scale Invariant Feature Transform for the feature extraction of the cover image. The watermark security is further enhanced by chaotic system tent map encryption. The visual feature vector of the original image is obtained using Bandelet-DCT (BDCT). The technique used zero-watermarking for the embedding and retrieval process. In [5] the authors presented a dual watermarking system for E-Healthcare applications. In this scheme, they used Redundant Discrete Wavelet Transform (RDWT) and RSVD for the watermarking, where the scaling factor for the embedding is determined using some optimization techniques. Finally, the marked image is encrypted utilizing various encryption methodologies. In [6], the author suggested a watermarking scheme using Lifting Wavelet Transform (LWT) and DWT, where the patient fingerprint is utilized as the watermark. Local binary pattern values of the cover image are used for finding the embedding factor, and the method was tested using various x-ray and Computed Tomography

978-1-6654-7312-5/22/$31.00 ©2022 IEEE

(CT) images. Ashima Anand *et al.* [7] initiated a cloud-based watermarking system for healthcare applications. The final watermark was generated using DWT and turbo code encryption. The algorithm used Integer Wavelet Transform (IWT), Schur, and RSVD techniques for the watermark embedding; fuzzy based optimization technique for selecting scaling factor. Hanaa A. Abdallah *et al.* [8] provided a watermarking system for the protection of transmitted medical images, which used DWT and DCT for the watermarking using some embedding and extraction rules. The scheme used the Double Random Phase (DRP) algorithm as encryption. Priyank Khare *et al.* [9] developed a methodology based on homomorphic transform, RDWT, and Singular Value Decomposition (SVD). A 2-dimensional chaotic encryption technique is applied to the watermark to give added security to the system. Ali Alzahrani *et al.* [10] introduced a hybrid MIW scheme to protect medical data. The authors incorporated different transform domain techniques like DWT and DCT along with SVD for the watermarking. Rohit Thanki *et al.* [11] framed a MIW technique using Non-Sub Sampled Contourlet Transform (NSCT) and RDWT. They performed the watermarking for medical and non-medical images with embedding and extraction rules. Since the above methods use multiple domain techniques, the computational complexity of the system will be very high with more embedding and extraction time. These are very crucial in a watermarking system.

The main contributions of the suggested technique are

- The proposed scheme utilizes a DCT-FRSVD hybrid approach for the MIW purpose and is relevant to non-medical data.
- The developed procedure is semi-blind since it requires only a part of the carrier information to extract the mark image.
- The False Positive Problem occurring in the SVD-based methods is eliminated since it does not require singular vectors at the receiving side for the watermark retrieval.
- The hybrid method provides high invisibility, excellent robustness, less computational complexity, and computational time.
- The security of the system is enhanced by chaotic encryption.
- The comparison results with the current state of art techniques indicate that the implemented methodology can be used for real-time e-health care applications for medical data transmission with increased integrity and security.

The remainder of the work is structured as follows. The background information in section II, suggested procedure in section III, research findings, and discussions are all explained in section IV. Section V brings the article to a finish.

II. Background information

A. Variance in Discrete Cosine Transform (DCT) domain

2-D forward DCT of $N \times N$ block of an image $f(i,j)$ is given by [12]

$$F(p,q) = \frac{2\alpha(p)\alpha(q)}{N} \times \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(f(i,j)\times cos\frac{(2i+1)p\pi}{2N} \times cos\frac{(2j+1)p\pi}{2N}) \quad (1)$$

where $p = q = 0, 1, \ldots, N-1$

$$\alpha(p) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } p = 0 \\ 1, & \text{otherwise} \end{cases} \quad (2)$$

The 2-D Inverse DCT (IDCT) is calculated using equation

$$f(i,j) = \sum_{p=0}^{N-1}\sum_{q=0}^{N-1}(\frac{2\alpha(p)\alpha(q)}{N} \times F(p,q)\times cos\frac{(2i+1)p\pi}{2N} \times cos\frac{(2j+1)p\pi}{2N}) \quad (3)$$

where $i = j = 0, 1, \ldots, N-1$.
In (1), $F(0,0)$ is the DC coefficient and $F(p,q)$ are AC coefficients of the DCT block. The sum of the squared normalized AC coefficient of the DCT block allows one to precisely determine the variance (σ^2) of a $N \times N$ block of pixels from its DCT coefficients and is given by

$$\sigma^2 = \sum_{p=0}^{N-1}\sum_{q=0}^{N-1}\frac{F^2(p,q)}{N^2} - \hat{F}^2(0,0) \quad (4)$$

In this equation(4), the first term is the normalized AC coefficient, and the second is the normalized DC coefficient. For complex structures, the variance should be high. The human visual system is less sensitive in this region, increasing imperceptibility. Hence the suggested strategy utilized high variance regions for watermarking.

The low-order DCT coefficients represent an image's complete information, and fine details are described using high-frequency components [13]. If we use low frequency for embedding, its imperceptibility will be less with an increase in robustness. Similarly, for high frequency, high invisibility with low robustness against watermarking attacks. So usually, we watermark middle-frequency components to obtain better imperceptibility and robustness.

B. Fast Randomized Singular Value Decomposition (FRSVD)

RSVD is a method used for matrix decomposition whose computational complexity is less than that of SVD, with high robustness. RSVD is performed using random sampling, resulting in a reduced matrix, reducing the computational time, followed by SVD operation. FRSVD is similar to RSVD but faster than RSVD and is described in [14]. It can be represented using the mathematical expression. For a matrix B

$$[B] = [rU \;\; rS \;\; rV^T] \quad (5)$$

Here are rU and rV^T are orthogonal matrices; rS is the singular matrix that consists of singular values in decreasing order.

C. Chaotic image encryption

Chaotic encryption is an effectual image encryption scheme with high randomness and irreversibility. It consists of the following steps: the creation of logistic function, confusion, and diffusion operations. During the confusion operation, we change the pixel position of an image. Individual variation of the gray pixel values occurs during the diffusion process [1]. A secret key is generated during the encryption process, which is used to decrypt the image successfully.

III. Proposed Method

Here, a medical image of size 512 x 512 is used as the host image, decomposed into 8 x 8 blocks, and the DCT of each block is calculated. Then select the blocks with the highest variance; the number of blocks depends on the watermark size. The (x, y) coordinates of the selected blocks are saved, which can be used for the retrieval process. To create a matrix, select a centre frequency coefficient (5,4) that was obtained through experimentation, from each block. Then, fast RSVD is applied towards the matrix. A binary logo of size 32 x 32 is taken as the watermark, which can be implanted into the original carrier image using embedding rules. The reverse process is used for the watermark retrieval. The algorithm used for the embedding and extraction is as follows and is shown in Fig. 1 and 3 respectively.

A. Watermark embedding algorithm

Step1: Read the host medical image (I_H) size of $m \times n$ and binary logo watermark (I_W) size of $a \times b$
Step2: Divide the cover image into 8 x 8 blocks
$B\_I_H \leftarrow I_H$

$$\text{Number of blocks, } b = \frac{m \times n}{8 \times 8} \tag{6}$$

Step3: Calculate the 2D-DCT of each block
$\{DC_B, AC_{B,1}, \ldots, AC_{B,63}\} = DCT2(B\_I_H)$ for $B = 1 : b$, where b is the number of 8 x 8 blocks
Step4: Find the variance of each block
$(V_1, \ldots, V_B) = Var\{DC_B, AC_{B,1}, \ldots, AC_{B,63}\}$ for $B = 1 : b$
Step5: Select appropriate blocks with the highest variance
$(V_1, \ldots, V_N) = Highest(V_1, \ldots, V_B)$ for $B = 1 : b$, where N is the number of blocks selected
Step6: Select the middle-frequency coefficient to form a matrix $[AC_1, \ldots, AC_N]$
Step7: Apply fast RSVD to the formed matrix
$[rU \;\; rS \;\; rV^T] \leftarrow FRSVD[AC_1, \ldots, AC_N]$
Step8: Embedding of binary logo watermark

$$rS' = (1 - G) \times (rS) + (G \times I_W) \tag{7}$$

where G is the Gain factor
Step9: Apply inverse fast RSVD

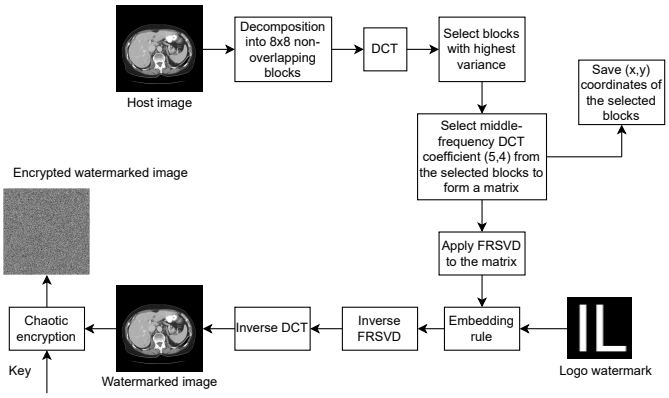

Fig. 1: Watermark embedding process with encryption

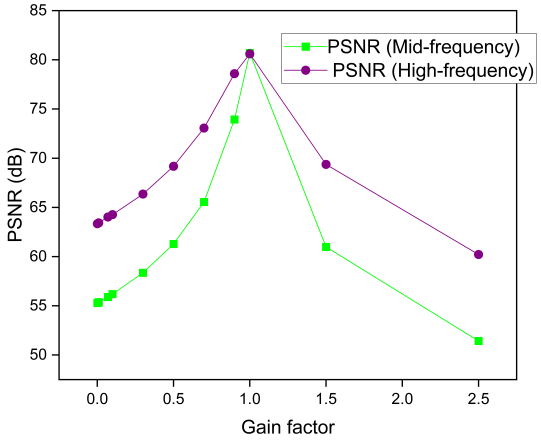

Fig. 2: Difference in the PSNR values due to change in the DCT coefficient for watermarking

$[AC'_1, \ldots, AC'_N] = [rU \;\; rS' \;\; rV^T]$
Step10: Place the modified coefficients in the original place
Step11: Apply 2D-IDCT to form the watermarked image

$$I_{HW} = IDCT\{DC_B, AC_{B,1}, \ldots, AC'_1, \ldots, AC'_N, AC_{B,N}, \ldots, AC_{B,63}\} \tag{8}$$

Step12: Apply chaotic encryption to the I_{HW} to improve the system's security.

In equation (7), the embedding rule is formulated by considering the brightness variation of each pixel of the host image instead of using the traditional method, increasing the picture imperceptibility [15].

Fig. 2 shows the variation in PSNR values if we choose the middle and high-frequency coefficients for watermark insertion. This shows that the PSNR value is high if we decide the high-frequency coefficients for watermarking with a decrease in robustness since they are lost during compression. To compromise between PSNR and robustness, the proposed procedure used mid-frequency coefficients for watermarking.

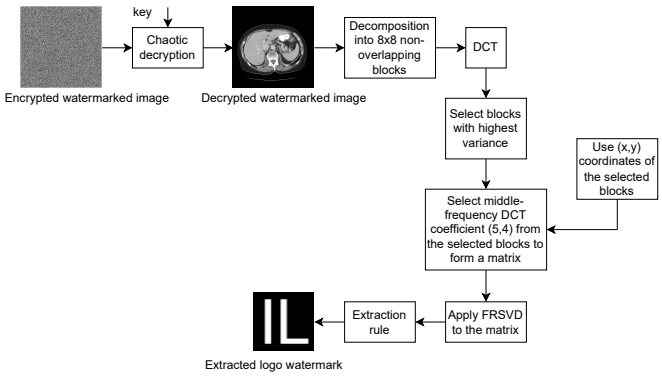

Fig. 3: Watermark retrieval process with encryption

B. Watermark extraction algorithm

Here, the encrypted watermarked image is decrypted using the secret key; the resultant image is separated into 8 x 8 blocks, and 2D-DCT is applied to each block. Then use the (x,y) coordinates for retrieving the image blocks with the highest variance and determine the middle-frequency coefficient of each block to form a matrix. Apply fast RSVD to the new matrix to see the singular value matrix. Finally, extract the logo watermark using the extraction rule. Here the False Positive Problem occurring in the general SVD-based techniques is eliminated since it does not require the singular vectors, and a part of the host image details is needed for extraction; the suggested scheme is semi-blind.

Step1: Decryption of I_{HW} using a secret key
Step2: Read the decrypted watermarked image (I'_{HW})
Step3: Divide the watermarked image into 8 x 8 blocks $B\_I_{HW} \leftarrow I'_{HW}$
Step4: Calculate the 2D-DCT of each block $\{DCW_B, ACW_{B,1}, \ldots, ACW_{B,63}\} = DCT2(B\_I_{HW})$ for $B = 1 : b$, where b is the number of 8 x 8 blocks
Step5: Find the variance of each block $(VW_1 : VW_B) = Var\{DCW_B, ACW_{B,1}, \ldots, ACW_{B,63}\}$ for $B = 1 : b$
Step6: Select appropriate blocks using (x,y) coordinates $(VW_1, \ldots, VW_N) = Highest(VW_1, \ldots, VW_B)$ for $B = 1 : b$, where N is the number of blocks selected
Step7: Select the middle-frequency coefficient to form a matrix $[ACW_1, \ldots, ACW_N]$
Step8: Apply fast RSVD to the formed matrix $[rwU \;\; rwS \;\; rwV^T] \leftarrow FRSVD[ACW_1, \ldots, ACW_N]$
Step9: Extraction of binary logo watermark using singular matrix rwS and rS' from the embedding side

$$I_{WE} = \frac{rS' - (1 - G) \times rwS}{G} \tag{9}$$

(a) (b) (c)

Fig. 4: Medical cover scans used (a) Mammogram (b) Abdomen (c) Fundus

IV. Experimental analysis and performance evaluation

The studies are conducted utilizing 512x512 medical scans, a 32x32 binary watermark logo, using Intel (R) Xeon (R) processor with 64GB of RAM in MATLAB 2022a, as illustrated in Fig. 4. Several matrices are employed to evaluate how well the given strategy performs. The parameters PSNR and SSIM are utilized to calculate the imperceptibility, are given by (10) and (13) respectively . NC is used to assess the performance against various image processing attacks, and is given by (12).

$$PSNR = 10log\frac{255^2}{MSE} \tag{10}$$

where MSE is the Mean Square Error and is given by

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(f_w(i,j) - f(i,j))^2 \tag{11}$$

$$NC = \frac{\sum_{i=1}^{m1}\sum_{j=1}^{n1} I_w(i,j)I(i,j)}{\sqrt{\sum_{i=1}^{m1}\sum_{j=1}^{n1}|(I(i,j)|^2|(I_w(i,j)|^2}} \tag{12}$$

here $f_w(i,j), f(i,j), I_w(i,j), I(i,j)$ are the watermarked image, original cover image, extracted mark, and original mark respectively.

$$SSIM(i,w) = \frac{(2\mu_i\mu_w + c_1)(2\sigma_{iw} + c_2)}{(\mu_i^2 + \mu_w^2 + c_1)(\sigma_i^2 + \sigma_w^2 + c_2)} \tag{13}$$

$\mu_i, \mu_w, \sigma_i, \sigma_w$ are the mean and variance values of the cover image and the marked image respectively. σ_{iw} represents the cross covariance between host image and watermarked image, c_1, c_2 are the constants with small values.

Table I depicts the performance of the proposed system using various cover medical images without any attack at a gain factor of 1. The table shows that the suggested watermarking scheme has superior imperceptibility and robustness, obtained a maximum PSNR of 81.71 dB, SSSIM, and NC values of 1 for image 1.

The performance of the suggested methodology against various image processing attacks (Gaussian Noise (GN), JPEG (JPEG compression), Median Filter (MF), Rotation (RO), Cropping (CR), Translation (TR), Rescaling (RS), Image Sharpening (SH), Salt and Pepper Noise (S & P), Speckle Noise (SN), Histogram Equalization (HE), Average Filtering (AF), Wiener Filtering (WF), and Poisson Noise (PN)) is given

TABLE I: Performance of the developed approach using various medical host images

Images	PSNR(dB)	SSIM	NC
Image1 (Mammogram)	81.71	1	1
Image2 (Abdomen)	80.70	1	1
Image3 (Fundus)	68.98	0.9995	1
Image4 (X-ray)	58.01	0.9978	1
Image5 (Brain)	51.16	0.9956	1

TABLE II: Performance of the implemented scheme against various image processing attacks

Type of Attacks	NC (Extracted watermark)
S & P(0.001)	1
S & P(0.01)	1
S & P(0.03)	1
GN (0.01)	1
GN (0.1)	1
GN (0.3)	1
SN(0.003)	1
SN(0.03)	1
SN(0.3)	1
PN	1
MF [3 3]	1
MF [7 7]	1
AF [3 3]	1
WF [3 3]	1
RO(10 degree)	1
RO(40 degree)	1
JPEG (Q=2)	1
JPEG (Q=10)	1
JPEG (Q=30)	1
SH	1
HE	1
RS(0.8)	1
RS(2)	1
TR	1
CR	1

in Table II. The table shows that the NC values of the retrieved watermarks are 1 for all the watermarking attacks, and the suggested plan is robust against all attacks.

Fig. 5 indicates the comparison results with the existing schemes regarding NC values of the retrieved watermark. The Tongyuan's system [3] uses cover pictures that are 128 × 128 and a binary watermark logo that is 64 x 64; the Yangxiu's scheme [4] uses cover images that are 512 x 512 and a binary watermark logo that is 32 x 32. The results imply that the suggested method is superior to the current state-of-the-art techniques. The embedding and extraction times of the implemented scheme are 0.1638 seconds and 0.0955 seconds, respectively, significantly less than the existing approaches, shown in Table III.

TABLE III: Comparison of the developed methodology with current techniques in terms of computational time (in seconds)

Process	Ref [16]	Ref [17]	Proposed
Embedding	0.2188	84.3218	**0.1638**
Extraction	0.1250	25.5313	**0.0955**

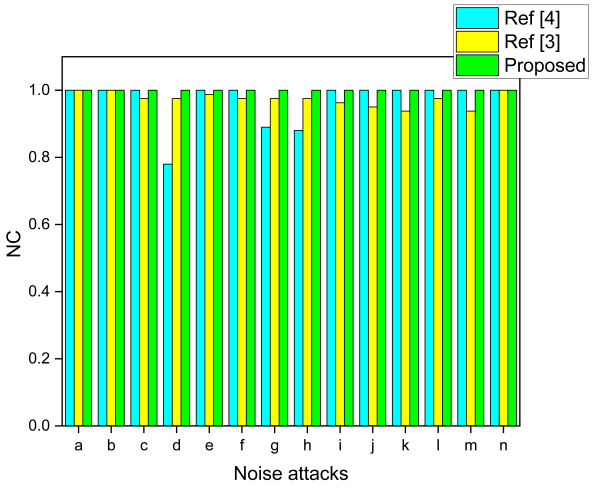

Fig. 5: Comparison of introduced scheme with the recent schemes in terms of NC values (extracted watermark) for medical image (a)GN (0.01) (b)GN (0.05) (c)GN (0.15) (d)GN (0.3) (e)JPEG (Q=2) (f)MF [3 3] (g)MF 5 5] (h)MF [7 7] (i)RO (10°) (j)RO (20°) (k)RO (20°) (l)CR (m)TR (n)RS (2)

(a) (b) (c)

Fig. 6: Non-medical cover scans used (a) Lena (b) Sail boat (c) Pepper

A. *Experimental analysis with non-medical images*

The experiments were also performed using various non-medical cover images, as shown in Fig. 6. The results were compared with current non-medical watermarking schemes shown in Fig. 7; all the procedures used gray cover scans of size 512 x 512 and watermark of size 32 x 32 in binary form. The Ferda's scheme [18] modified the selected coefficients of DWT-DCT transform for the watermarking with an embedding algorithm. The Dhani's system [16] used five middle-frequency DCT coefficients of the highest variance blocks assigned with specific rules for the watermarking. The Ernawan's method [17] used RDWT-SVD for watermarking by considering the Human Visual System characteristics. The comparison results demonstrate that the developed approach has impressive robustness in getting the NC value of 1 (for the retrieved watermark) for all the image processing attacks and outperforms non-medical cover images with less computational time.

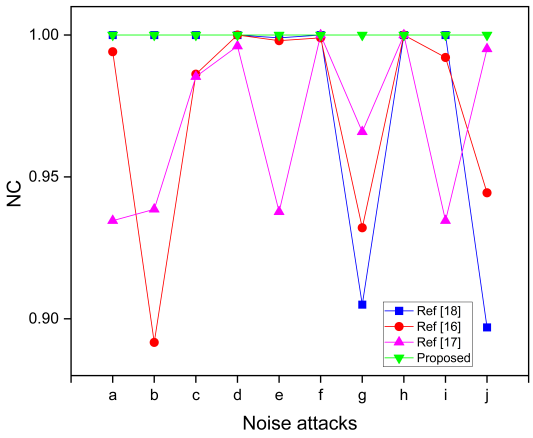

Fig. 7: Comparison of introduced scheme with the current schemes in terms of NC values (extracted watermark) using Lena image (a)GF[3 3] (b)JPEG(Q=30) (c)JPEG(Q=40) (d)JPEG(Q=50) (e)MF[3 3] (f)SH (g)SP(0.01) (h)HE (i)AF[3 3] (j)PN

V. Conclusion

This paper implemented a highly robust MIW scheme with impressive imperceptibility, less computational complexity, and computational time using the DCT-Fast RSVD method. Here the cover image is separated into 8 x 8 blocks, and DCT is performed on each block. The blocks with the highest variance are selected depending on the watermark size. The middle frequency coefficient is determined from each block to form a matrix whose length is equal to the binary watermark logo size; Fast-RDWT is used to find the singular matrix. The logo watermark is inserted into the singular matrix using an embedding algorithm to form the watermarked image. Chaotic encryption is used to enhance the security of the system. The reverse process is done for the watermark retrieval. Here the False Positive Problem occurring in the general SVD-based techniques is eliminated since it does not require the singular vectors for watermark retrieval, and a part of the host image information is needed for extraction; the suggested scheme is semi-blind. The suggested procedure is also applied to non-medical images. The technique's performance is evaluated using different parameters; obtained a maximum value of PSNR of 81.71 dB, SSIM of 1, and NC value of 1 for all the attacks on medical and non-medical images. The implemented approach obtained less embedding time of 0.1638 seconds and a retrieval time of 0.0955 seconds. The suggested scheme achieved better imperceptibility, robustness, and computational time performance than the existing techniques. The watermark capacity is 1024 bits, which can be improved by selecting more DCT middle frequency coefficients. In the future, multiple watermarks can be employed with some optimization techniques for the vital security of medical data in e-healthcare applications.

References

[1] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, W. J. Buchanan *et al.*, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140 876–140 895, 2020.

[2] M. Sajeer, A. Mishra, and P. Sathidevi, "Recent advances in transform and hybrid domain digital watermarking techniques—a survey," *Soft Computing for Security Applications*, pp. 841–857, 2022.

[3] T. Huang, J. Xu, Y. Yang, and B. Han, "Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and hessenberg decomposition," *Mathematics*, vol. 10, no. 7, p. 1154, 2022.

[4] Y. Fang, J. Liu, J. Li, J. Cheng, J. Hu, D. Yi, X. Xiao, and U. A. Bhatti, "Robust zero-watermarking algorithm for medical images based on sift and bandelet-dct," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16 863–16 879, 2022.

[5] A. Anand and A. K. Singh, "Hybrid nature-inspired optimization and encryption-based watermarking for e-healthcare," *IEEE Transactions on Computational Social Systems*, 2022.

[6] S. P. Vaidya, "Fingerprint-based robust medical image watermarking in hybrid transform," *The Visual Computer*, pp. 1–16, 2022.

[7] A. Anand and A. K. Singh, "Cloud based secure watermarking using iwt-schur-rsvd with fuzzy inference system for smart healthcare applications," *Sustainable Cities and Society*, vol. 75, p. 103398, 2021.

[8] H. A. Abdallah and D. H. ElKamchouchi, "Signing and verifying encrypted medical images using double random phase encryption," *Entropy*, vol. 24, no. 4, p. 538, 2022.

[9] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, p. e3918, 2021.

[10] A. Alzahrani and N. A. Memon, "Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images," *IEEE Access*, vol. 9, pp. 113 714–113 734, 2021.

[11] R. Thanki, A. Kothari, and S. Borra, "Hybrid, blind and robust image watermarking: Rdwt–nsct based secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, no. 18, pp. 27 593–27 613, 2021.

[12] M. B. A. Haghighat, A. Aghagolzadeh, and H. Seyedarabi, "Multi-focus image fusion for visual sensor networks in dct domain," *Computers & Electrical Engineering*, vol. 37, no. 5, pp. 789–797, 2011.

[13] X. Nie, B. Xiao, X. Bi, W. Li, and X. Gao, "A focus measure in discrete cosine transform domain for multi-focus image fast fusion," *Neurocomputing*, vol. 465, pp. 93–102, 2021.

[14] X. Feng, W. Yu, and Y. Li, "Faster matrix completion using randomized svd," in *2018 IEEE 30th International conference on tools with artificial intelligence (ICTAI)*. IEEE, 2018, pp. 608–615.

[15] M.-J. Zuo, S. Cheng, and L.-H. Gong, "Secure and robust watermarking scheme based on the hybrid optical bi-stable model in the multi-transform domain," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 17 033–17 056, 2022.

[16] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," *Multimedia Tools and Applications*, vol. 79, no. 17, pp. 12 041–12 067, 2020.

[17] F. Ernawan and M. N. Kabir, "A block-based rdwt-svd image watermarking method using human visual system characteristics," *The visual computer*, vol. 36, no. 1, pp. 19–37, 2020.

[18] F. Ernawan, D. Ariatmanto, and A. Firdaus, "An improved image watermarking by modifying selected dwt-dct coefficients," *IEEE Access*, vol. 9, pp. 45 474–45 485, 2021.