International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Undecimated Wavelet Transform Technique for the Security Improvement In the Medical Images for the Atatck Prevention

Dr. Rajneesh Tyagi[1], Dr. Rajveer K. Shastri[2], Dr. Kumarasamy M[3], M.Ramkumar Prabhu[4], Dr. Mohan Laavanya[5], Dr. Usha C. Pawar[6]

Submitted: 01/11/2022 **Accepted:** 02/02/2023

Abstract: Watermarking is effective technology for processing for secure image through transform domain. With ever increases in security threats demands for security in medical images. This paper proposed a Undecimated Discrete Wavelet Transform (SVDUWT) for evaluation of watermarking in medical images. The proposed model is incorporated in two stages. At first, SVD – DWT is performance of embedding of the watermarking in an medical images. Secondly, entrophy scheme is incorporated for computation of pixels in an images, With normal embedding watermarking scheme involved in transformation of low-frequency sub-band of images. The proposed low-frequency bands are classified in to non-overlapping blocks. The experimental evaluation expressed that proposed scheme significant performance in performance analysis of watermarked method. Also, performance of proposed method is evaluated for attack scenario such as noise and scaling attack. The analysis confirmed that proposed model exhibits good performance for medical image watermarking.

Keywords: *Watermarking, Encryption, attacks, embedding, entropy, UDWT*

1. Introduction

The realm of insertion for the mark is related to the numerous watermarking picture methods accessible across the literature (spatial, frequential, multi-resolution, etc). There are several performance choices available for each picture representation region [1]. The selection of the insertion domain is thus a crucial stage in development of watermarking methods. Spatial domain insertion is accomplished by altering image's pixel values directly. This domain's key advantage is that insertion as well as detection operations are computationally cheap, allowing it to be utilized in real-time watermarking applications [2]. The biggest downside is that, following integration, the visual quality of the image declines. Subsequently, these methods are vulnerable to attacks. In frequency domain insertion, mark is injected into converted domain rather than image Discrete Fourier Transform or Discrete Cosine Transform [3] is utilized to obtain the image's frequency representation. The selection of the marked coefficients is the most difficult aspect of this type of scheme. The most effective methods for achieving a good robustness-invisibility compromise frequently position the mark in the image's middle frequencies to enhance imperceptibility simultaneously minimising the likelihood that the mark will be eliminated by compression or noise addition if situated in high frequencies[4]. Despite domain's inherent advantages of translation as well as scale invariance, computing costs for this technique are high also susceptible to windowing and tiny local deformations[5]. It is distinguished by sub-banding of image, It makes it possible to separate low-frequency components, creating a portion of the insertion that is less sensitive[6]. A multi-resolution translation of the image preserves its spatial content, which may then be used to find a mark after a geometric shift.

Digital picture watermarking methods aredivided into two groups based on domain in which watermark is introduced: spatial along with transform domain approaches.Using spatial domain approaches, watermark is quickly applied to

[1] Dean, Deapartment of Agriculture, Sanskriti University, Mathura, Uttar Pradesh, India.
dean.soa@sanskriti.edu.in
0000-0002-8571-6221
[2] Professor, Department of E&TC, Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, India. Savitribai Phule Pune University, Pune, India.
rajveer.shastri@vpkbiet.org
[3] Assistant Professor, Department of Computer Science, College of Engineering and Technology, Wollega University, Nekemte, Oromia Region, Ethiopia.
drmksamy115@gmail.com
[4] Professor, Department of Electronics and Communication Engineering, PERI Institute of Technology, Chennai, Tamil Nadu, India.
ramkumarprabhu@gmail.com
[5] Vignan's Foundation for Science, Technology and Research, Electronics and Communication Engineering, Vignan's Foundation for Science, Technology and Research, Guntur.
laavanvijay@gmail.com
0000-0001-7656-2913
[6] Assistant professor, Mechanical Engineering, Datta Meghe College Of Engineering, Airoli, Navi Mumbai, Maharashtra, India.
usha.pawar@dmce.ac.in
0000-0002-6516-5354

overlay a picture by changing the pixel values[7]. They are beneficial due to their brevity and ease of execution, however, they are frequently vulnerable to geometrical attacks.

2. Related Works

The realm of insertion for the mark is related to the numerous watermarking picture methods accessible across the literature (spatial, frequential, multi-resolution, etc). There are several performance choices available for each picture representation region [8]. The selection of the insertion domain is thus a crucial stage in development of watermarking mechanisms.The key advantage of this realm is that insertion and detection operations are computationally cheap, enabling its implementation in real-time watermarking software [9]. Spatial domain insertion is accomplished through altering image's pixel values directly. The biggest downside is that, following integration, the visual quality of the image declines. Subsequently, these methods are vulnerable to attacks. In frequency domain insertion, mark is injected into converted domain rather than the picture.A DFT or a DCT is utilized to determine the image's frequency representation [10]. Selection of indicated coefficients is the most difficult aspect of this approach. The best techniques for achieving an appropriate robustness-invisibility balancing frequently position the mark in the image's middle frequencies to enhance imperceptibility simultaneously minimising the likelihood of the mark being dislodged by compression or noise addition if situated in higher frequency[11].

They offer a hybrid watermarking method in [12] that combines visual cryptography with watermarking (WPT).A WPT is used to segment image as well asdetermine smallest energy band in which watermark text is incorporated for the incorporation of a watermark transmitting the information of the one who owns a medical image.Anand& al propose a technique for combining numerous watermarks in medical photographs. The watermark that is embedded consists of both text and a picture. To boost security, the watermarked picture is subsequently encrypted using the HyperChaotic encryption method.[13] proposes a blind watermarking system that utilises DWT along with SVD. A quick Walsh Hadamard transformation is implemented to each block. Blocks of the LL sub-band are subjected to singular value decomposition created by Hadamard transform.To improve security, watermark image is scrambled utilizing Arnold Transform. Khare and Srivastava offer DWT, singular value decomposition,homomorphic transform as well as Arnold transform [14]. After that, watermark bits are incorporated into unique values obtained.The HL subband is first dissected into illumination plus reflectance factors using a DWT, and then the homomorphic transform is used to deconstruct it into illumination and reflectance components in this work. The watermark is jumbled using Arnold transform. The reflectance component's singular values are then used in the integration procedure.Zhou& al present a watermarking system that is both strong and hybrid [15]. In this work, DWT is applied.After applying singular value decomposition to HL also LH subbands, a watermark is integrated by changing direct current coefficients. Based on DWT and DCT, Benoraira& al offer a blind as well as durable image watermarking method[16]. DCT is utilized initially in this method. The watermark bits are then embedded using two DCT sub-vectors. Original sub-vectors are found by subsampling approximation coefficients of host picture's DWT transform.

3. Undecimated Discrete Wavelet Model for Image Security

The improved watermarking scheme involved in construction of SVDUWT scheme for robustness. Usually, the performance of network is incorporated to protect documents those involved for medical images. Also, the implementation of watermarking scheme offers possible solution against the attacks. The developed watermark fragile concentrated to protect the images those need to be protected along with integrity check. Along with an integrity checker, the suggested SVDUWT ensured robustness against attacks. The proposed SVDUWT has three steps: watermark creation, integration, and extraction. Due to the fact that the SVD and DWT are components of the proposed SVDUWT architectural paradigm process for watermarking with entrophy estimation within the medical images.

3.1 Integrated SVD with the UDWT

SVD comprises of the matrix with (DWT). The product of SVD considered for 3 matrices is defined as U, S and V. The identity matrix of I illustrate the matrix size of $m \times n$ those can be decomposed in to r. The identity matrix of I the matrices are therefore written as in equation (1)

$$I = U * S * V^t = \sum_{i=1}^{n} \left(\sigma_i * u_i * v_i^f\right) \quad (1)$$

Where, the matrix size is represented as S, the diagonal positive terms is defined as r. The singular matrix I for non-zero element is denoted as s_i. In consideration of linear algebra MRI image can be computed as scalar non-negative elements. The image I matrix is shown as in equation (2)

$$\mathrm{I} = \mathrm{USV}^{\mathrm{T}} \quad (2)$$

In above equation left and right singular vector is denoted as U and V. The diagonal matrix component of element S represented as singular value of I. The element eigen values of the MRI images are denoted as in equation (3)

$$S = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 \\ 0 & \sigma_2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma_M \end{bmatrix} \quad (3)$$

Where $\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \cdots \geq \sigma_r \geq \cdots \geq \sigma_M = 0$ 1 represented as larger value of element with rank r of matrix I. The principal component (PI) matrix of the elements is obtained for matrices U and S. The unique feature components of the matric is evaluated based on false positive value as in equation (4)

$$PC = U \times S \quad (4)$$

The variation in coefficients of DWTrepresentation of images is evaluated based on image contours and texture components. The regions related to the domain specific wavelet coefficient. In figure 1 illustrated the overall architecture of the proposed SVDUWT for watermarking of medical images are presented.

The overall steps involved in extraction of the images watermark are presented in following steps:

Step 1: Four sub-bands are applied to the input MRI medical images for processing.

Step 2: Medical image sub-band LL1 is classified as non-overlapping block size of 8×8

Step 3: The coefficients of each blocks are evaluated with DWT

Step 4: To derive the watermark from copyright center

Step 5: With incorporation of secret bits extraction is performed for watermark bits using equation (5)

$$ew_2(i) = \mathrm{mod}(n, 2) \quad (5)$$

where n is evaluatedusing equation (6):

$$n = \mathrm{floor}\left(\frac{\mathrm{abs}\,(\Delta)}{\delta_2}\right)$$

$$\Delta = B_i'(1,2) - B_i'(2,1) \quad (6)$$

where B i is ith blocks denoted by secret sequence K6, δ2 is embedding factor

Step 6: Similarly, decryption of watermark performed using equation (7)

$$sw_2 = K_5 \oplus ew_2 \oplus zw \quad (7)$$

In above equation, encrypted watermark is defined as ew_2, the scramble decrypted watermark is denoted as zw with the sequence of K_5.

The algorithm 1 provides the information embedding within the medical images is presented. Similarly, in algorithm 2 encryption process performed by the proposed SVDUWT for security is presented.

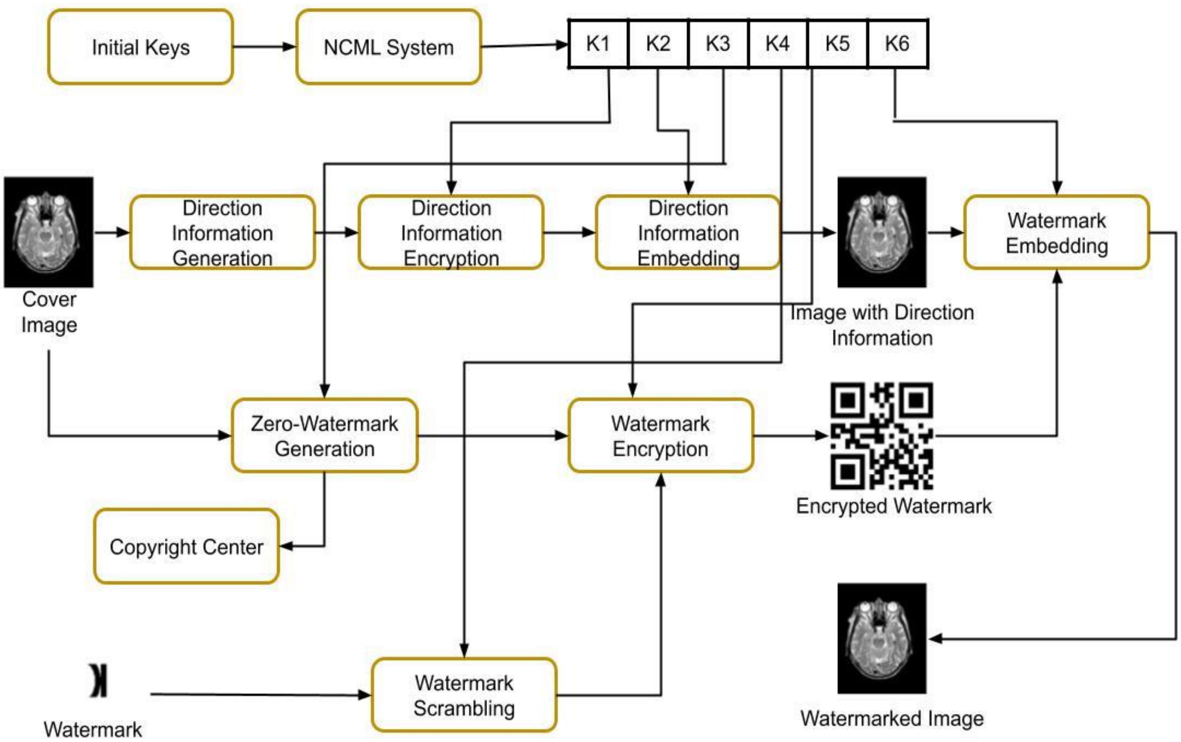


Fig. 1: Overview of developed SVDUWT scheme

Algorithm 1:undecimated wavelet transform

Require: Cover image P,

secret sequences: K_1, K_2.

direction information w_1

Ensure: Cover image with direction information embedded P'

1: $ew_{q1} = w_1 \oplus K_1$

2: L =length(ew_1)

3: $Z = \text{CalRHFMs}\ (P)$;

4: for $i = 1$ to L do

5: $j = K_2(i)$:

6: $\lambda = \text{round}\left(\frac{|Z(j)|}{\delta_1}\right)$

7: if mod $(\lambda + ew_1(j), 2) == 0$ then

8: $|Z'(j)| = (\lambda + 0.5) \times \delta_1$

9: else if $\lambda > 0.5$ then

10: $|Z'(j)| = (\lambda - 0.5) \times \delta_1$

11: else

12: $|Z'(j)| = (\lambda + 1.5) \times \delta_1$

13: end if

14: end for

15: $R_1 = \text{Reconstruct}\ (Z)$;

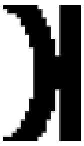
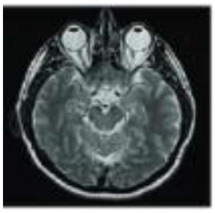
16: $R_2 = \text{Reconstruct}\ (Z')$;

17: $P' = P - R_1 + R_2$:

4. Simulation Results

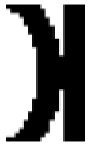
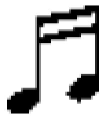
For the computation of original picture to watermarked image, performance of suggested SVDUWT is tested. In table 1 presented computation of the PSNR and SSIM for the watermarked image is presented. Extracted watermark from an images is also evaluated with computation of the BER values and NC values that are shown in table 1.

Table 1: Comparison of extracted watermark

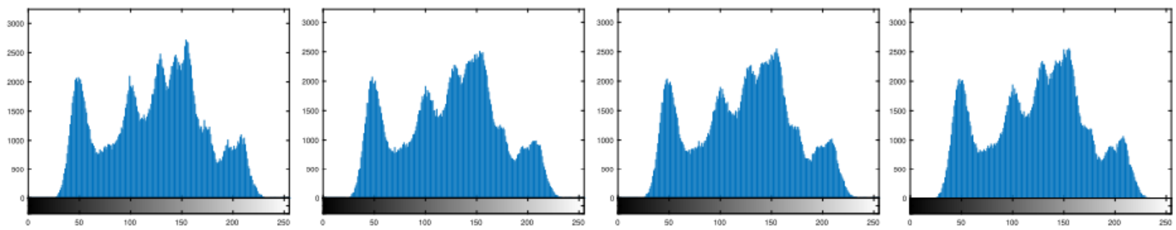
Watermarked Image	**PSNR & SSIM**	**Watermark**	**Normal**		**Zero**	
			NC	**BER %**	**NC**	**BER %**
	PSNR = 40.26 dB SSIM = 0.9638		**1.0000**	**0**	0.9873	**1.26**
	PSNR = 40.17 dB SSIM = 0.9784		**1.0000**	**0**	0.9829	**1.66**
	SNR = 41.29 dB SSIM = 0.9715		**1.0000**	**0**	0.9792	**2.05**

In table 2 presented the medical MRI image with different watermark scheme are presented for different MRI images.

Table 2: Comparison of different watermark

Watermarked Image	PSNR & SSIM	Extracted Watermark	Normal Watermark		Zero - watermark	
			NC	**BER %**	**NC**	**BER %**
	PSNR = 40.16 dB SSIM = 0.9658		**1.0000**	**0**	**0.9873**	**1.26**
	PSNR = 42.37 dB SSIM = 0.9684		**1.0000**	**0**	**0.9829**	**1.66**
	SNR = 41.29 dB SSIM = 0.9915		**1.0000**	**0**	**0.9792**	**2.05**

The evaluation of the different watermark schemes over the medical MRI images expressed that the minimal influence is observed for the medical data. With binary watermark scheme the encryption is performed with the cover images for estimation. However, in the watermark scenario the watermarks are extracted with minimal data loss. As a result, the proposed SVDUWT may be inferred to be effective for a variety of images and watermark formats. Additionally, histogram of the input dicom MRI images data is illustrated in figure 2.



(a) (b) (c) (d)

Fig. 2: (a) histogram for watermark 1 (b) histogram for watermark 2 (c) histogram for watermark 3 (d) histogram for watermark 4

In the figure 2 presented the sub-band estimation of the watermarked images for different watermark is presented. The evaluation of LL-sub band is based on consideration of SVD – DWT transformation process with frequency domain analysis.In table 3 Evaluation of the suggested SVDUWT system in comparison to the watermark scheme are presented.

Table 3: Comparative analysis

Attacks	Others		Normal Watermark		Zero - watermark	
	Ref [11]	Ref [12]	NC	BER %	NC	BER %
Salt&Peppers (0.005)	0.9516	0.9516	0.9350	10.06	0.9835	**1.66**
Gaussian (0.001)	-	-	0.9676	**5.08**	0.9795	**2.05**
Speckle (0.005)	0.9678	4.59	0.8571	17.97	0.9855	**1.46**
PSNR	40.40		41.17		-	
SSIM	0.9820		0.985		-	

The performance of proposed SVDUWT scheme with conventional scheme for watermarking is as depicted in table 3. The analysis expressed that the suggested plan demonstrates superior functionality compared with conventional technique.

5. Conclusion

This research described an SVDUWT watermarking system for medical image security. The developed SVDUWT scheme is incorporated the encryption scheme for watermark images. Watermark image embedded with the SVD-DWT is involved in computation of LL1 sub – band for computation. In watermarking process, a effective sequence is generated with the watermarked positions with respect to position of images. The entropy computes the values of the each pixel and calculate the effectiveness. The proposed SVDUWT method is tested under a various attack types scenarios, incorporating scale and noise attacks. Comparative investigation revealed that the proposed method performs superior than conventional technique. For many scenarios, the performance of the suggested SVDUWT framework is effective.

References

[1] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., & Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, *6*, 10269-10278.

[2] Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, *97*, 95-105.

[3] Zainol, Z., Teh, J. S., &Alawida, M. (2020). A new chaotic image watermarking scheme based on SVD and IWT. *IEEE Access*, *8*, 43391-43406.

[4] Thanki, R., Kothari, A., & Trivedi, D. (2019). Hybrid and blind watermarking scheme in DCuT–RDWT domain. *Journal of Information Security and Applications*, *46*, 231-249.

[5] Liu, X., Lou, J., Fang, H., Chen, Y., Ouyang, P., Wang, Y., ... & Wang, L. (2019). A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. *IEEE Access*, *7*, 76580-76598.

[6] Araghi, T. K., & Abd Manaf, A. (2019). An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Generation Computer Systems*, *101*, 1223-1246.

[7] Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W., &Xiong, N. N. (2019). A robust watermarking scheme in YCbCrcolor space based on channel coding. *IEEE Access*, *7*, 25026-25036.

[8] Molina-Garcia, J., Garcia-Salgado, B. P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., & Cruz-Ramos, C. (2020). An effective fragile watermarking scheme for color image tampering detection and self-recovery. *Signal Processing: Image Communication*, *81*, 115725.

[9] Yuan, Z., Su, Q., Liu, D., & Zhang, X. (2021). A blind image watermarking scheme combining spatial domain and frequency domain. *The Visual Computer*, *37*(7), 1867-1881.

[10] Araghi, T. K., Abd Manaf, A., &Araghi, S. K. (2018). A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Systems with Applications*, *112*, 208-228.

[11] Najafi, E., &Loukhaoukha, K. (2019). Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform.

Journal of information security and applications, *44*, 144-156.

[12] Zhou, N. R., Hou, W. M. X., Wen, R. H., & Zou, W. P. (2018). Imperceptible digital watermarking scheme in multiple transform domains. *Multimedia Tools and Applications*, *77*(23), 30251-30267.

[13] Hou, J., Li, Q., Tan, R., Meng, S., Zhang, H., & Zhang, S. (2019). An intrusion tracking watermarking scheme. *IEEE Access*, *7*, 141438-141455.

[14] Zeebaree, D. Q. (2021). Robust watermarking scheme based LWT and SVD using artificial bee colony optimization. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 1218-1229.

[15] Sadreazami, H., &Amini, M. (2018). A robust image watermarking scheme using local statistical distribution in the contourlet domain. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *66*(1), 151-155.

[16] 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.

[17] Liu, D., Yuan, Z., &Su, Q. (2020). A blind color image watermarking scheme with variable steps based on Schur decomposition. *Multimedia Tools and Applications*, *79*(11), 7491-7513.