ALGEBRAIC FACTORIZATION METHOD (LDL^T) AND BIOMETRIC SAMPLES FOR BLIND DIGITAL IMAGE WATERMARKING

[1]Areej M. Abduldaim, [2]Mohammed Qasim Hamid
[1,2]University of Technology, Applied Sciences Department, Mathematics and Computer Applications, Baghdad, Iraq
E-mail: [1]areejmussab@gmail.com

ABSTRACT: *Personal information needs to be safely transmitted over the internet and address effectively. Blind digital watermarking of biometric samples is a convenient technique used to increase security and data authentication, which is decisive due to the uniqueness of some types of watermark images. Biometrics like fingerprints, voice, retina, iris, and blood vessel tree are being increasingly utilized for affirmative identification since they cannot be mislaid or forgotten and represent perceptible components. Furthermore, in the viewpoint of linear algebra, any digital image can be expressed by a matrix consists of a non-negative number of scalars. Consequently, in this paper, a blind watermarking algorithm using a matrix decomposition method named LDL^T (another version of the classical Cholesky decomposition) is introduced. The algebraic method LDL^T is applied and analyzed to illustrate its impact on each 4×4 block of the LH band in the frequency domain that represents the output of LWT (Lifting Wavelet Transform). According to this analysis of the mathematical advantage of LDL^T, the algorithm is given in which binary biometric watermark bits are embedded into the lowest value in the matrix D and take the position (1,1) of each 4×4 block. The experimental results show that the algebraic proposed algorithm is worked successfully on medical images.*

Keywords: Cholesky Decomposition (LDL^T), lifting Wavelet Transform (LWT), biometrics, fingerprint, medical Images keyword

1. INTRODUCTION

Digital image watermarking is information (the watermark) hiding into the digital data. In other words, to affirm the originality of the data; the embedded secret image can be specified or extracted later. Digital watermarking is the first kind of mechanism to better the impartiality and reliability of digital data. Lately, authentication is one of the major watermarking requirements in image processing applications [1].

On the other hand, linear algebra is a subfield of mathematics interested in matrices, vectors, and linear transforms. It is a fundamental key to the field of image processing, from symbols used to describe the approach of algorithms to the enforcement of algorithms in code. In addition, linear algebra plays an important role particularly in watermarking.

Medical image watermarking is a newcomer area for the preservation of medical images. A numeral of medical image watermarking techniques generally outputs deformations in the medical image in accordance with watermarking this leads to Wrong diagnosis[2-5]. A watermarking technique that segmented the medical image into 8 × 8 blocks is proposed in [6] by Zain and Fauzi and then the mapping is established between the blocks in order to embed the recovery data of each block into its corresponding mapped block. Another algorithm segments the medical image into three parts of pixels: RONI (a region of noninterest), ROI pixels and border pixels. Therefore, ROI data and information of the authentication are embedded in border pixels while the recovery information of ROI is logically embedded into RONI region [7]. Thankia et al. [8], proposed a blind medical image watermarking technique depending on DCT (Discrete Cosine Transform) and FDCuT (Fast Discrete Curvelet Transform). Discrete Wavelet Transform (DWT) is considered a worthy tool in mathematics and computer science. It is used to fulfill security, robustness, and imperceptibility of watermarking exigencies [9].

Three algorithms employed Singular Value Decomposition (SVD) to ensure the robustness versus different types of distortions added to images accidentally or deliberately [10, 11, 12]. In linear algebra, LU factorization writes a matrix as the product of two matrices, a lower triangular matrix with the main diagonal equal 1 and an upper triangular matrix. In the lower triangular matrix, there is a specific correspondence between any two factors in the first column of the lower triangular matrix L after implementing LU decomposition on 4 × 4 sub-image [13]. LU factorization has perfect energy divisions, so it supplies a more frank reference for selecting the position of the watermark embedding [14].

Motivated by the above, this paper focus on a digital watermarking algorithm depends primarily on LDL^T factorization which is taken into consideration for the first time in the watermarking techniques. Common with the Lifting Wavelet Transform (LWT), this work investigates the robustness and imperceptibility in the frequency domain. Moreover, in this paper, the medical images are adopted to demonstrate the importance of digital image watermarking.

The remainder of this paper is organized as follows. In Section 2, the basic important information of LDL, LET and chaotic logistic map are described concisely. Section 3 devoted to present the proposed algorithm. Experimental results and discussion are illustrated in Section 4. Finally, the conclusions are documented in Section 5.

2. PRELIMINARIES

In this section, we will provide the reader by known and basic important information which will be used in the rest of this paper.

2.1 Cholesky Decomposition (LDL^T Version)

In linear algebra, the Cholesky decomposition or Cholesky decomposition is a factorization of a positive-definite Hermitian matrix into the product of a lower triangular matrix and it plays an important role in image processing to explain the efficient numerical solutions. One of the related variants of the classical Cholesky decomposition is the LDL factorization,

$A=LDL^*$

where **L** is a lower unit triangular matrix, **L*** denotes the conjugate transpose of **L** and **D** is a diagonal matrix. In case matrix A has real entries, then $L^*=L^T$ [15]. There are several types of Cholesky decomposition depending on the final form of the original matrix after disassembly, some of them are the following [16-18]:

i- $A = LL^T$ (The Cholesky decomposition L^T version)

ii- $A = LDL^T = LD^{1/2}D^{1/2}L^T = (LD^{1/2})(LD^{1/2})^T = \acute{L}\acute{L}^T$ (The Cholesky decomposition LDL^T version)

iii- $A = LDL^T = L(DL^T) = LU$ (The Cholesky decomposition LU version)

2.2 Lifting Wavelet Transform

Sweldens in [19] introduced the Lifting Wavelet Transform (LWT) depending on the classical wavelet. The LWT has a number of advantages compared with the classical wavelet (DWT) because 1-LWT has the ability to compute more efficiently, 2-LWT doesn't need big memory space, 3-LWT has integer coefficients, 4-DWT capable to address the impairment of quantization errors from the classical wavelet transform. Lifting wavelet Transform facilitates the case by immediately analyzing the case in the special domain. The major precept of the LWT is to establish a new wavelet with improved characteristics depend on a simple wavelet that represents the basic key of lifting. LWT turn into a robust scheme for different applications used in image processing: image compression [20], watermarking [21] and pattern recognition [22]. The lifting wavelet transform (LWT) and its inverse transform (ILWT) are of one dimensional (ID) signals. An obvious method to use LWT for two-dimensional signals like images is to use row-column (horizontal-vertical) or column-row (vertical-horizontal) passes of the corresponding one dimensional LWT. In general, this strategy contains three essential phases:

Splitting: The cover image Im is dismantled into even and odd nonoverlapping elements of $Im_e(x)$ and $Im_o(x)$.

$Im_e(x) = Im(2x), \quad Im_o(x) = Im(2x+1)$

Prediction: In this phase, the value of an odd element is predicted using even elements:

$$E(x) = Im_o(x) - P(Im_e(x))$$

Where $P(.)$ denotes the prediction operator. The prediction phase represents the highpass filtering operation and $E(x)$ regards the high-frequency synthesis which is the error between the original element and its predicted value.

Updating: This phase considered as the lowpass filtering operation and $L(x)$ regards the low-frequency synthesis which shows the coarse approximation to the original image:

$$L(x) = Im_o(x) + U(E(x))$$

2.3 Logistic Map (Chaotic Case)

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, chaotic behavior can grow from very straightforward nonlinear dynamical equations [23]. The Logistic map is one of the distinguished one-dimensional chaotic maps. Furthermore, for the randomness of the chaos sequence, the randomness will be better if the sequence length is greater. The mathematical definition of the chaotic logistic map with two initial values r and $Logi_0$ can be expressed as follows:

$$x_{i+1} = rx_i(1 - x_i)$$

where x_i take values in the interval (0,1), x_0 is the initial value for the sequence and the chaotic parameter $r \in [3.5699456, 4]$ is a positive constant sometimes known as the biotic potential. The chaotic map is used to fabricate the chaotic sequence and used to control the encoding process [24].

3. PROPOSED ALGORITHM

The watermark embedding phase and the watermark extraction phase represent the main two execution phases of the proposed algorithm can be complemented. The proposed watermark embedding scheme based on Cholesky decomposition, LDL^T version, and LWT is illustrated in Fig. 1. In order to improve the security of the watermarking algorithm, the logistic map is applied to mix the blocks obtained after divided the image randomly. The watermark can be mixed randomly by utilizing a certain chaotic parameter, and the extracted watermark can get back similarly to the certain chaotic parameter in the extraction phase. The Watermark embedding and extraction algorithms are given below.

3.1 Embedding algorithm

The detailed embedding phase using LDL^T factorization and DWT are explained and given as follows:

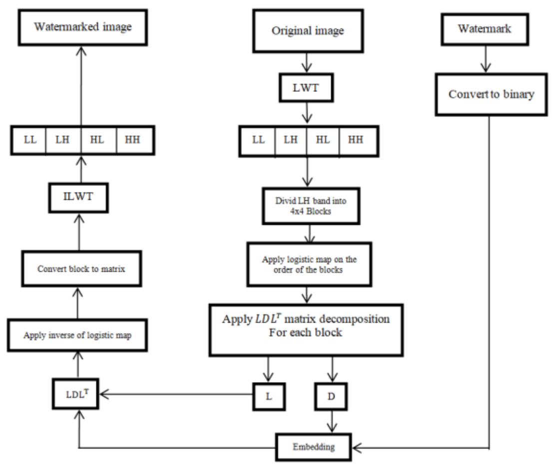


Figure 1: Embedding phase

Step1: Input the original image that has size $N \times N$ and convert this image to a grayscale image.

Step2: The original image is decomposed by a one-level (LWT) to the subbands {LL, LH, HL, LL}, each band of size $\frac{N}{2} \times \frac{N}{2}$.

Step3: Divide the band {LH} into 4×4 non-over lapping blocks, the number of blocks is $M \times M$.

Step4: Input the watermark image with size $M \times M$ and convert this image to binary image.

Step5: The chaotic logistic map in eq.1 is applied to switch locations of the blocks

$$x_{(i+1)} = rx_i(1 - x_i) \qquad (1)$$

Step6: Apply LDL^T factorization to each block.

Step7: Embedding binary watermark bits in D sub-matrix produced from step 6.

$$D\,(1,1) = D\,(1,1) - D\,(1,1)\,(\mathrm{mod}\,S) + T1 \qquad if\ w = 1$$

$$D\,(1,1) = D\,(1,1) - D\,(1,1)\,(\mathrm{mod}\,S) + T2 \qquad if\ w = 0$$

Where S=2 is the quantization step, T1 = 0.75*S, T2 = 0.25*S.

Step8: Apply reverse operations for LDL^T, logistic map, collect all blocks to one matrix and finally ILWT to get the watermarked image.

3.2 Extracting Algorithm

The detailed extraction phase is illustrated and given as follows:

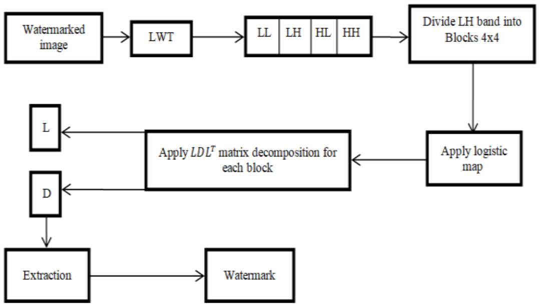


Figure 2: Extraction phase

Step1: Input the watermarked image with size $N \times N$ and convert this image to a grayscale image.
Step2: The watermarked image is decomposed by a one-level (LWT) to the subbands {LL, LH, HL, LL}, each band of size $\frac{N}{2} \times \frac{N}{2}$.
Step3: Divide the band {LH} band into 4×4 non-over lapping blocks, the number of blocks is $M \times M$.
Step4: The chaotic function (logistic map) is applied on all blocks to restore the blocks to their original locations.
Step5: Apply LDL^T factorization to each block.
Step6: Extraction binary watermark bits from the sub-matrix D.

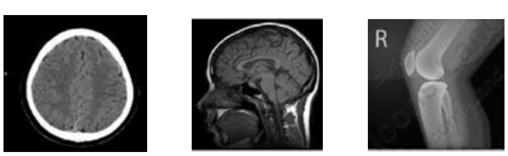
$$W = 0 \quad if\ mod\ (D\ (1,1)) > (T1 + T2)/2$$
$$W = 1 \quad if\ mod\ (D\ (1,1)) <= (T1 + T2)/2$$

4. RESULTS AND DISCUSSION

In general, the performances of image watermarking techniques are measured by the robustness, invisibility, computation complexity, etc. The following figures represent respectively the host images, the watermark image, and the resulted watermarked images.

1- CT Image 2- MRI Image 3- X-RAY Image

W



4 5 6

Figure 3: The original images 1,2 and 3, the watermark image W, the watermarked images 4,5 and 6.

The PSNR represents a good rule for the watermark visibility estimation, its definition is given by the following equation:

$$MES = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

$$PSNR = 10 log_{10} (\frac{MAX^2}{MSE})$$

The similarity between the extracted watermark E and the original watermark W is computed based on a normalized correlation coefficient between W and E.

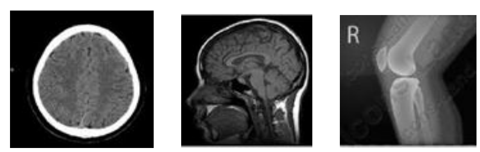
$$NC = \frac{\sum_i \sum_j w(i,j).w'(i,j)}{\sqrt{\sum_i \sum_j w(i,j)}\sqrt{\sum_i \sum_j w'(i,j)}}$$

According to the above measurements, the following Table 1 shows the PSNR and NC of the given images

Table 1: The PSNR and NC values for watermarked images without attacks

Image	1- CT Image	2- MRI Image	3- X-RAY Image
PSNR	37.398	37.009	35.462
NC	1	1	1

The following are the watermarked images and the extracted watermark image from each one respectively:



1 2 3

W W W

Figure 4: The watermarked images 1,2 and 3, the extracted watermark image W.

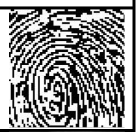
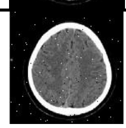
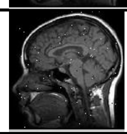
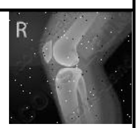
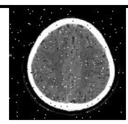
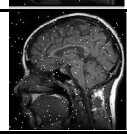
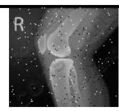
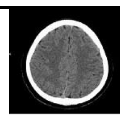
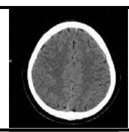
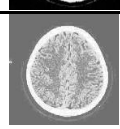
For testing the robustness of the proposed method, various attacks are performed on the watermarked image:

Table 2: The PSNR and NC values for watermarked images with attacks

Attacks	Image 1		Image 2		Image 3	
	PSNR	NC	PSNR	NC	PSNR	NC
Salt and Pepper %1	25.873	0.270	25.878	0.270	25.371	0.324
Salt and Pepper %5	21.681	0.216	21.238	0.362	20.919	0.392
JPEG Compression	60.198	0.259	59.678	0.283	61.267	0.231
Gaussian Noise	37.888	0.391	38.261	0.381	39.031	0.404
Histogram equalization	14.557	0.227	9.1299	0.370	8.3874	0.216

The visual watermarked images and the extracted watermark are given in Table 3 as follows:

Table 3: Three medical original and watermarked images after attacks

Image Type / Attacks	1- CT	2- MRI	3- X-RAY
Original Image			
Watermark			
Watermarked Image			
Salt and Pepper %1			
Salt and Pepper %5			
JPEG compression			
Gaussian Noise			
Histogram Equalization			

For more illustration, convert the original image 1- CT to a 512×512 grayscale image and then apply the LWT to decompose the original image to obtain the four bands LL, LH, HL, and HH. Each band is of size 256×256 and we choose the LH band because it contains mostly the vertical detailed information.

Next, divide the band LH into 64×64 blocks each of which of size 4×4 and then the chaotic logistic map applied to scramble the locations of the blocks as a security process. By applying the LDL^T factorization, each block will correspond to two matrices L and D; the embedding process of the binary watermark will be in the (4,4) position of each block.

To explain the embedding process above, a 4×4 sub-image S of the LWT band (LH) and its LDL^T factorization process is given as:

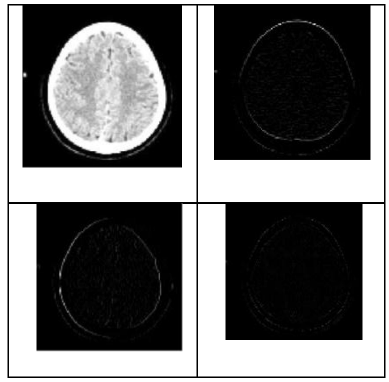


Figure 5: The Original Image 1 Transferred by LWT

$$S = \begin{bmatrix} 162 & 162 & 163 & 164 \\ 162 & 163 & 164 & 166 \\ 162 & 164 & 166 & 168 \\ 164 & 166 & 169 & 169 \end{bmatrix}$$

After S is factored by LDL^T factorization, L and D factors are shown as the following:

So the (4,4) position element is 0.0763 in which the watermark information embedded.

5. CONCLUSION

In this paper, a new algorithm depending on Cholesky decomposition (LDL^T version) is proposed to secure digital medical images using Lifting Wavelet Transform (LWT). The features of the proposed algorithm include: 1- The low-high band of LWT is chosen to modify the imperceptibility and robustness. 2- Based on the mathematical characteristics of LDL^T factorization, the element in the (4,4) position is adapted to embed the information of the watermark image. 3- From the experimental results, it is shown that the proposed method can get better PSNRs and that the proposed algorithm fulfills better watermark invisibility and robustness under Gaussian attacks. Finally, it is hoped that digital watermarking and biometrics technologies can facilitate essential work functions, such as Viewer Tracking, Copyright Control, Forensics, Copy Protection, Telemedicine, and Content Identification.

REFERENCES

1. Guru, J. and Damecha, H., “Digital Watermarking Classification: A Survey,” *International Journal of Computer Science Trends and Technology*, **2**(5): 8–13(2014).
2. Eswaraiah, R. and Reddy, E. S., “Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI,” *International Journal of Telemedicine and Applications*, **2014**: 1-10(2014).
3. Hu, Y.C., Lo, C.C., Wu, C.M., Chen, W.L. and Wen, C.H., “Probability-based Tamper Detection Scheme for BTC-compressed Images Based on Quantization Levels Modification,” *International Journal of Security and Its Applications*, **7**(3): 11-32(2013).
4. Kim, K.S., Lee, M.J., Lee, J.W., Oh, T.W. and Lee., H.Y., “Region-Based Tampering Detection and Recovery Using Homogeneity Analysis in Quality-

Sensitive Imaging," *Computer Vision and Image Understand*, **115**(9): 1308-1323(2011).

5. Liew, S.C. and Zain, J.M., "Reversible medical image watermarking for tamper detection and recovery," *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology*, 9-11(2010).
6. Zain, J.M. and Fauzi, A.R.M., "Medical image watermarking with tamper detection and recovery," *Proceedings of the 28th IEEE EMBS Annual International Conference Engineering in Medicine and Biology Society, New York City, USA*, 3270- 3273(2006).
7. Eswaraiah, R. and Reddy, E.S., "Medical Image Watermarking Technique for Accurate Tamper Detection in ROI and Exact Recovery of ROI," *International Journal of Telemedicine and Applications*, **2014**: 1-10(2014).
8. Thankia, R., Borrab, S., Dwivedia, V. and Borisagar, K., "An efficient medical image watermarking scheme based on FDCuT–DCT," *Engineering Science and Technology, an International Journal*, **20**(4): 1366-1379(2017).
9. Mohammed, F.G. and Al-Dabbas, H.M., "The Effect of Wavelet Coefficient Reduction on Image Compression Using DWT and Daubechies Wavelet Transform", Science International (Lahore), **30** (5): 757-762(2018).
10. Rani, A. and Raman, B., "An Image Copyright Protection System Using Chaotic Maps," *Multimedia Tools and Applications*, **76**(2): 3121–3138(2017).
11. Jane, O. and Elbaşi, E., "A New Approach of Nonblind Watermarking Methods Based on DWT and SVD Via LU Decomposition," *Turkish Journal of Electrical Engineering and Computer Sciences*, **22**(5): 1354-1366(2014).
12. Zhang, H., Wang, C. and Zhou, X., "A Robust Image Watermarking Scheme Based on SVD in The Spatial Domain," *Future Internet*, **9**(3): 1-16(2017).
13. Su, Q., Wang, G., Zhang, X., Lv, G. and Chen, B., "A New Algorithm of Blind Color Image Watermarking Based on LU Decomposition," *Multidimensional Systems and Signal Processing*, 29(3): 1055–1074(2018).
14. Wang, S., Zhao, W. and Wang, Z., "A Gray Scale Watermarking Algorithm Based on LU Factorization," 2008 *International Symposiums on Information Processing IEEE*. 598-602(2008).
15. Golub, G.H. and Loan, C.F.V., "*Matrix Computations*," *John Hopkins University Press, Baltimore, MD*, 1983.
16. Gentle, J.E., "Cholesky Factorization. §3.2.2 in Numerical Linear Algebra for Applications in Statistics" *Berlin: Springer-Verlag*, 93-95(1998).
17. Nash, J.C., "The Choleski Decomposition. Ch. 7 in Compact Numerical Methods for Computers: Linear Algebra and Function Minimisation," *2nd ed. Bristol, England: Adam Hilger*, 84-93(1990).
18. Press, W. H., Flannery, B. P., Teukolsky, S. A. and Vetterling, W. T., "Cholesky Decomposition. §2.9 in Compact Numerical Methods for Computers: Linear Algebra and Function Minimisation," *2nd ed. Cambridge, England: Cambridge University Press*, 89-91(1992).
19. Phadikar, A., Maity, S. P. and Kundu, M. K., "Quantization Based Data Hiding Scheme for Efficient Quality Access Control Of Images Using DWT Via Lifting," *Proc. Sixth Indian Conference on Computer Vision, Graphics and Image Processing, Bhubaneswar, India*, 265- 272(2008).
20. Fan, W., Chen, J. and Zhen, J., "SPIHT Algorithm Based on Fast Lifting Wavelet Transform in Image Compression," *International Conference on Computational and Information Science*, 838–844(2005).
21. Lei, B ., Soon, IY., Zhou, F., Li, Z. and Lei., H., "A Robust Audio Watermarking Scheme Based on Lifting Wavelet Transform and Singular Value Decomposition," *Signal Processing*, **92**(9): 1985–2001(2011).
22. Zhang, S.Q., He, N. and Zang, H.Y., "Research of The Lifting Wavelet Arithmetic and Applied in Rotary Mechanic Fault Diagnosis," *Journal of Physics: Conference Series*, **48**: 696–700(2006).
23. Jihong, Z., Rongwen, L., Liujie, S. and Songlin, Z., "Low-Noise Multiple Watermarks Technology Based on Complex Double Random Phase Encoding Method," *Proceedings of SPIE - The International Society for Optical Engineering 7851*, 1-10(2010).
24. Marek, M. and Schreiber, I., "Chaotic Behaviour of Deterministic Dissipative," *Cambridge University Press, Cambridge*, 1991.