
EPNN Based High Secure Intensive Hidden Digital Watermark Application in Telemedicine

Rayi Sailaja^{*}, Chiramdasu Rupa², Ardhani Satyanarayana Chakravarthy³

¹ Dept. of CSE, Aditya College of Engg & Tech, Surampalem 533437, India

² Dept. of CSE, VR Siddhartha Engg College, Vijayawada 520007, India

³ Dept. CSE, JNTUK-UCEV, Vizianagaram 535003, India

Corresponding Author Email: sailajarai@gmail.com

https://doi.org/10.18280/ama_a.560104

ABSTRACT

Received: 22 December 2018

Accepted: 6 March 2019

Keywords:

encryption, watermarking, LWT, extended euclid's approach, probabilistic neural networks

This paper presents a novel and secure hybrid approach to securely transmit multimedia medical content over the web to help diagnosis from distance. This approach is a combination of a novel encryption algorithm and Extended Euclid's based watermarking algorithm. This approach provides authentication, confidentiality, and integrity. The user's authentication data is converted into ciphertext and then inserted into the watermark image, a 2-level LWT based decomposition of a host image is performed to retrieve (LL, LH, HL & HH) coefficients. The watermark and cover image one-level LL coefficients are divided into 16*16 blocks and watermark image blocks are embedded into a cover image using Extended Euclid's algorithm. Then the watermarked image and cover image is given as input to PNN to obtain the optimized image matrix. The experimental results show better Peak Signal to Noise Ratio, Mean Square Error and Normalized Correlation with respect to existing methodology. Also, the watermarked image quality is analyzed with different image quality metrics.

1. INTRODUCTION

In modern health environment, many clinicians or health care providers share medical multimedia content like images and electronic patient data as a part of applications of telemedicine such as teleradiology, telesurgery, teleconsulting, etc. With the increased use of teleradiology, the need for security and privacy concern issues in telemedicine is also growing. Another issue is that the transmitted multimedia content is very much tamper prone. So there is a desperate need for implementation of secure medical transfer schemes like medical image watermarking to achieve the security services of cryptography like authentication, integrity, and confidentiality. Authentication verifies that whether the received image arrives from the correct source and belongs to the intended patient or not, confidentiality ensures that only legitimate users have access to the transmitted image and whereas integrity checks that whether the received image has not been transformed by the unauthorized users [1].

Medical Image watermarking can be used to serve the purpose of transferring the medical history of a patient through the web. Patient details can be embedded in the medical images in an encrypted form. At the receiver's end, it can be extracted and decrypted to verify the patient details. Through medical image watermarking patient information is maintained confidentially. The proposed approach also provides authenticity and integrity for the content of the medical image.

The proposed methodology relies on Lifting Wavelet Transform. LWT coefficients are represented by a finite precision number which helps for lossless coding. So LWT provides lossless compression. LWT can reconstruct the

image without any loss as LWT coefficients are integers values that can be accumulated without any round-off errors. LWT implements the lifting scheme. Lifting the wavelet scheme is treated as the best solution than DWT as it is more advantageous for different applications [2]. It is the second generation of the fast wavelet transform. As lifting wavelet increases smoothness and reduces aliasing effect it is considered as better for the reconstruction of the image when compared with general wavelet transform [3]. Applying LWT improves the robustness of the watermark as it enhances the integrality of an embedded watermark in the host image, which results in reduced information loss.

The performance of traditional watermarking methods can be enhanced by artificial neural networks [4]. The relation of watermarked image and watermark image can be memorized by artificial neural networks. One of the artificial neural network methods used is the Probabilistic Neural Network (PNN). This consists of nodes of 4 layers [4]. They are input, pattern, summation and output layers [4]. PNN identifies a learning category and finds out the possibility of similar input sample with the help of the radial bias function.

The proposed approach uses extended Euclid's algorithm to get modular multiplicative inverses so that they can be replaced by cover image pixel values. Modular multiplicative inverse exists only if two integers are coprime i.e. when their gcd is 1. In this algorithm, every divisor and remainder is represented as a linear combination of the two numbers. This algorithm finds x such that $ax \equiv 1 \pmod{m}$ [5]. PNN is also used in this approach to improve the robustness of the watermarked image.

The proposed work is organized as follows; Related Work is analyzed in Section II Section III analyzes the proposed work in detail. Experimental results were shown in section

2. RELATED WORK

One of the major issues in medical image watermarking is to see that patient medical image quality is not affected by the embedded patient data in the medical image. The most important security concern when the patient data is exchanged through the web is authentication, confidentiality, availability, and integrity [6, 7]

Ali Al-Haj et al. [1] proposed a crypto-watermark algorithm which claims that authentication is provided by embedding the watermark image in cover image's regions of non-interest using SVD and DWT [8]. Its performance is evaluated using different images with respect to robustness, imperceptibility, tamper localization.

Sriti Thakur et al. [8] presented a robust watermarking approach which is based on chaotic encryption and image watermarking based on DWT-DCT-SVD. The proposed method performance is analyzed with existing methods and claims that extracted watermark is highly robust with respect to various image processing attacks.

Nambakhsh et al. [9] presented a digital watermarking approach in which the zero-tree wavelet algorithm is implemented. Evaluation of the proposed approach is done using a CT scan and MRI images and also claimed that it uses only 15% of the host image to insert a watermark image.

Mohammed M. et al. [10] has presented an approach in which the SHA 256 hash algorithm is applied whose hash code is encrypted along with compressed R-S vector and patient identity using RSA. The encrypted data is watermarked into the original image. Its experimental results show that its embedding capacity is 0.525bpp.

Anand et al. [11] has presented an algorithm in which encrypted patient data is watermarked into medical images by exchanging the LSB of gray pixel values of the original reference image with a watermark image.

Titan J. [12] proposed an algorithm for medical images based on difference expansion, it modifies the relationships between the adjacent pixels by adjusting the luminance values. This algorithm claims more embedding capacity.

Cheh Huang et al. [13] proposed a reversible watermarking scheme for the medical image, in which histogram of images is modified to hide data but includes little overhead.

Manideep Kaur et al. [14] proposed a reversible medical image watermarking in which additive expansion is applied on interpolation error for embedding data. Author claims that the method achieves good image quality and high embedding capacity but results were not shown.

A.K Singh et al. [15] has proposed an algorithm which embeds patient information into chosen sub-band of Discrete wavelet transform coefficients of the reference medical image using the spread spectrum technique. It is observed that watermark is extracted with high robustness and shown better results against different attacks.

3. PROPOSED METHODOLOGY

3.1 Encryption approach

Input: Patient Identification Data, the Patient Fingerprint

image

Output: Ciphertext

1. Read Plaintext P.
2. Read key matrix $K = \{K | K(i, j) \text{ is a printable character on the keyboard}\}$ according to ULDS where $U = \{u | u \text{ is a uppercase letter}\}$, $L = \{l | l \text{ is a lower case letter}\}$, $D = \{d | d \text{ is a digit}\}$, $S = \{s | s \text{ is a special symbol}\}$
3. Encode each plaintext character to get Ciphertext T using a random variable from $R_i, i \in \{1, 2, \dots, N\}$, where N is the length of K.
4. Embed the ciphertext into watermark I_w using the LSB and penultimate LSB. The encryption and embedding approach is shown in Figure 1.

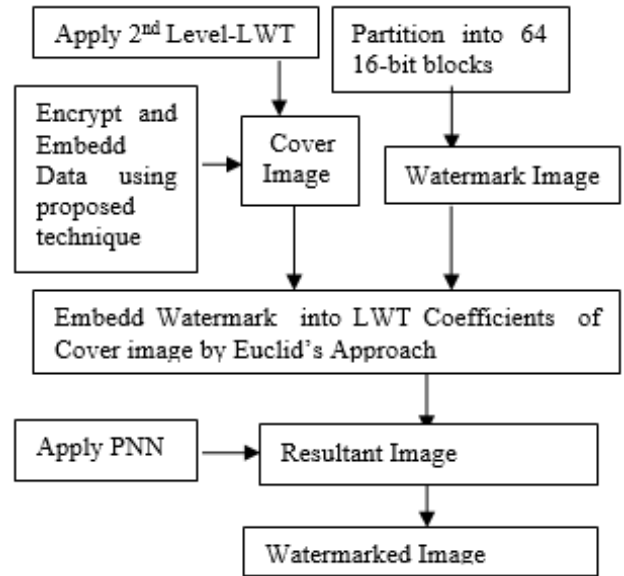


Figure 1. Encryption and embedding

3.2 Watermark embedding approach

Watermark image: Patient fingerprint image in which ciphertext is embedded

Cover Image: Patient Medical Image

Output: Patient Watermarked medical Image.

1. Apply the second level LWT on Cover Image(I_c).
 $[A1, H1, D1, V1] = \text{lwt2}(I_c)$.
2. Let Part (I_w) be the set of partitions of I_w .
3. $(X_p), I_w \in \text{Part}(I_w), 1 < p \leq 64$ and each $|X_p|$ is 16-bit partition.
4. $A1_w = \text{Embed}(X_p, A1), 1 < p < 16$ using Extended Euclid's Approach
 Loop Begin:
 Let $M = X_p(i, j), N = A1(i, j)$, where $1 < i \leq 16, 1 < j \leq 16$
 if $\text{gcd}(M, N) = 1$
 Find T such that $M * T \equiv 1 \pmod{255}$ then
 $N = T$
 else
 $N = M$
 End
 $A1_w(i, j) = N$
 Loop End
5. Repeat the step4 for H1 to get $H1_w$, where $17 < p \leq 32$.

6. Repeat the step4 for D1 to get D1_w, where 33 < p ≤ 48.
7. Repeat the step4 for V1 to get V1_w, where 49 < p ≤ 64.
8. I_{wk} = ilwt2 (A1_w, H1_w, D1_w, V1_w).
9. I_{wk} = PNN(I_{wk}, I_c).

3.3 Extraction approach

1. Read Watermarked Image
 2. [A1_w, H1_w, D1_w, V1_w] = ilwt2 (I_{wk})
 3. X_{pA} = Extract (X_{pw}, A1_w), 1 < pw < 16 using Extended Euclid's Approach
 - i. Let Part (A1_w) be the set of partitions of A1_w
 - ii. (X_{pw}) ∈ A1_w ∈ Part (A1_w), 1 < pw ≤ 16 and each | X_{pw} | is a 16-bit partition.
 - iii. Loop Begin:
 - Let M = X_{pw} (i , j) where 1 < i ≤ 16, 1 < j ≤ 16
 - if M * T ≡ 1 mod 255, then
 - N = T
 - else
 - N = M
 - End
 - A1'(i, j) = N
 - Loop End
4. Repeat the step3 for H1_w to get X_{pH}, where 17 < p ≤ 32.
5. Repeat the step3 for D1_w to get X_{pD}, where 33 < p ≤ 48.
6. Repeat the step3 for V1_w to get X_{pV}, where 49 < p ≤ 64.
7. Combine the partitions X_{pA}, X_{pH}, X_{pD}, X_{pV} to get extracted watermark I_{Ewk}.
8. Extract the ciphertext T from watermark using the inverse process of encryption approach. The process is shown in Figure 2.

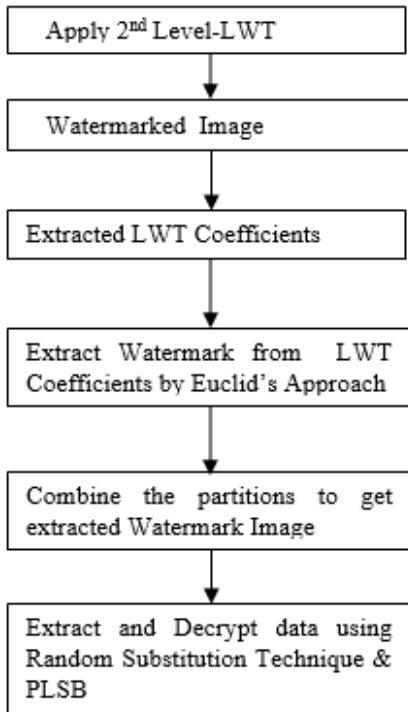


Figure 2. Extraction approach

4. EXPERIMENTAL ANALYSIS

4.1 Performance measures

Different image quality metrics are available to analyze the watermarking results. Among them, the most extensively used and simple image quality metric is the metric mean square error (MSE), which is evaluated by averaging the squared differences of distorted and reference image pixels. MSE value is used to evaluate peak to signal noise ratio (PSNR). A larger PSNR indicates more imperceptibility and is defined as

$$PSNR = 10 \log \frac{(B_{max})^2}{MSE} \quad (1)$$

MSE can be computed as

$$MSE = \frac{1}{P \times Q} \sum_{i=1}^P \sum_{j=1}^Q (Or(i, j) - W(i, j))^2 \quad (2)$$

where Or(i, j) refers to reference image pixel value and W(i, j) refers to the distorted image pixel value. The maximum pixel value of the image is the B_{max}. As per [16] the PSNR value of higher than 27 DB is acceptable for the watermarked image. The resemblance of the extracted watermark with original watermark can be evaluated using Normalized correlation factor and is computed as

$$NC = \frac{\sum_{i=1}^P \sum_{j=1}^Q O(i, j) \times W(i, j)}{\sum_{i=1}^P \sum_{j=1}^Q O(i, j)^2} \quad (3)$$

There are other image metrics using which we can analyze the image quality. They are listed in Table 1. Where O(i, j) refers to the reference image and W(i, j) refers to the distorted image.

Table 1. Other image quality metrics

S.No	Metric	Description
1	Average Difference	$MD = \frac{1}{P \times Q} \sum_{i=1}^P \sum_{j=1}^Q O(i, j) - W(i, j)$
2	Structure Content	$SC = \frac{\sum_{i=1}^P \sum_{j=1}^Q W(i, j)^2}{\sum_{i=1}^P \sum_{j=1}^Q O(i, j)^2}$
3	Normalized Absolute Error	$NAE = \frac{1}{PQ} \sum_{i=1}^P \sum_{j=1}^Q O(i, j) - W(i, j) $
4	Maximum Difference	$MD = \text{MAX} O(i, j) - W(i, j) $
5	Image Fidelity	$IF = 1 - \frac{\sum_{i=1}^P \sum_{j=1}^Q O(i, j) \times W(i, j)}{\sum_{i=1}^P \sum_{j=1}^Q O(i, j)}$

4.2 Experimental results

The key challenges of multimedia content authentication using watermarking are to achieve the parameters like robustness against different image accidental or incidental distortions and maintaining the good perceptual quality of the extracted watermark and the original image.

By using MATLAB R2014a, the proposed approach has been tested on the text and medical image data. We selected 100 MRI brain, CT scan images around to evaluate the proposed method's performance. We considered 8-bit

grayscale images, the original image of size 256*256 and watermark image size of 64*64. It is observed that the perceptuality of the watermarked image is maintained. The watermarked image resembles the original image so the anonymity of the existence of the watermark is maintained successfully.

The perceptual quality of the extracted watermark image and the watermark image is analyzed with image metrics like Normalized Correlation (NC), Maximum Difference(MD), Peak Signal to Noise Ratio (PSNR), Average Difference(AD), Mean Square Difference(MSE), Normalized Absolute Error(NAE), and Structure Content (SC) which is shown in table2.

Table 2. Proposed approach performance at scaling factor 0.01

S.NO	Image Metric	Baby Scan image	X-Ray image	MRI brain image	MRI Muscle image
1	MSE	0.04	0.06	0.13	0.11
2	PSNR	61.858	60.138	57.021	57.933
3	MD	4.000	4.000	5.000	9.000
4	NC	0.999	0.999	0.998	0.999
5	SC	0.999	0.999	0.996	0.999
6	NAE	0.007	0.004	0.002	0.007

Ideally, NC value should be 1 but value up to 0.7 is acceptable according to [16] This approach provides NC of 0.999. The acceptable value of PSNR due to wireless transmission quality loss is between 20dB and 25dB, but higher is better. This approach exhibits PSNR above 55dB which indicates that image reconstruction is of high quality. It's Mean Square Error and Average Difference is also small.

Table 3. Performance of the proposed approach at scaling factor 0.001 with different input medical images






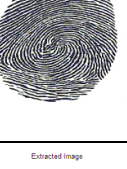


S.No	PSNR	NC	Watermarked Image	Extracted Watermark
1	57.021	0.998		
2	60.138	0.999		
3	57.933	0.999		
4	61.858	0.999		

Table 3 depicts the output images for different input medical images.

Table 4. Comparison of NC values of the existing and proposed approach

S.No	Attacks	A.K.Singh et al.[15]	Proposed Method
1	Gaussian Noise	0.975	0.999
2	Median filtering [1 1]	0.998	0.999
3	JPEG	0.990	0.998
4	Salt and Pepper [0.001]	0.963	0.999
5	Salt and Pepper [0.01]	0.755	0.988

Watermarked image robustness is checked by adding intentionally some noise to the watermarked image, whether it is able to resistant to different image attacks like Gaussian noise, median filtering, salt & pepper, JPEG Compression. The approach's performance is evaluated with respect to NC at scaling factor 0.001, also proposed approach is compared with the existing approach [15] and shown better results as shown in table 4.

Table 5. Proposed approach analysis with different factors against existing[15, 17] approaches

S.No	Factor	A.K.Singh et al. [15]	R.Sailaja et al. [17]	Proposed Approach
1	PSNR	35.84	54.072	57.021
2	NC	0.999	0.985	0.999
3	Embedding Capacity	High	High	High
4	Perceptuality	High	High	High
5	Encryption involved	Yes	Yes	Yes

In table 5 proposed approach is also analyzed with two existing approaches[15, 17] with respect to different implementation factors.

5. CONCLUSION

A robust and secure digital watermarking algorithm based on extended Euclid's and PNN approach in the wavelet domain is proposed in this paper. This study exhibits significantly anonymity and robustness of the watermark. LWT based 2-level decomposition is performed on the original image to get LL2, LH2, HL2, HH2 wavelets. Watermark image of size 64*64 and 2-level LWT wavelets are divided into 16*16 blocks. Using the extended Euclid's approach watermark image is embedded into the original image. The watermarked image is optimized using PNN approach. The proposed algorithm shows better invisibility of the watermark and also provides extraction of the watermark from the watermarked image. The strength of the proposed algorithmic approach is analyzed against various image attacks like JPEG compression, Gaussian noise, salt and pepper noise, and median filtering, Also the approach has shown better Normalized Correlation when compared with the existing approach with respect to mentioned attacks.

REFERENCES

- [1] Al-Haj, A., Mohammad, A., Amer, A. (2017). Crypto-watermarking of transmitted medical images. *Journal of Digital Imaging*, 30(1): 26-38. <https://doi.org/10.1007/s10278-016-9901-1>
- [2] Preet, K., Geetu, L. (2012). Comparative analysis of DCT, DWT & LWT for image compression. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 1(3): 90-93.
- [3] Daubechies, I., Swedens, W. (1998). Factoring wavelet transform into lifting scheme. *The Journal of Fourier Analysis and Applications*, 4(1): 247-269. <https://doi.org/10.1007/BF02476026>
- [4] AL-Nabhani, Y., Jalab, H.A., Wahid, A., Md Noor, R., (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University-Computer and Information Sciences*, 27: 393-401. <https://doi.org/10.1016/j.jksuci.2015.02.002>
- [5] Extended Euclidean algorithm - <https://shashwat001.wordpress.com/2012/08/17/extended-euclidean-algorithm>
- [6] Kumar, B., Singh, H.V., Singh, S.P., Mohan, A. (2011). High capacity spread spectrum watermarking for telemedicine applications. *World Academy of Sciences Engineering Technology*, 5(7): 62-66.
- [7] Mohanty, S.P. (1999). Watermarking of digital image. M.S.Thesis, Indian Institute of Sciences, India.
- [8] Sriti, T., Singh, A.K., Ghrrera, S.P., Mohamed, E. (2019). Multi-layer security of medical data through watermarking and chaotic encryption for telehealth applications. *Multimedia Tools and Applications*, 78(3): 3457-3470. <https://doi.org/10.1007/s11042-018-6263-3>
- [9] Nambahsh, M.S., Ahmadian, A., Ghavami, M., Dilmaghani, R.S. (2006). A novel blind watermarking of ECG signal on medical images using EZW algorithm. *Proc. of 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3274-3277. <https://doi.org/10.1109/IEMBS.2006.259603>
- [10] Ada-Elyadem, M.M. (2014). Medical image authentication based on reversible watermarking. *Proceedings of the International Conference on Informatics and Systems*, pp. 15-24.
- [11] Anand, D., Natarajan, U.C. (1998). Watermarking medical images with patient information. *Proc.of IEEE/EMBS Conference HongKong, China*, pp. 703-706. <https://doi.org/10.1109/iembs.1998.745518>
- [12] Titan, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits Systems, and Video Technology*, 13(8): 890-896. <https://doi.org/10.1109/TCSVT.2003.815962>
- [13] Huang, H.C., Fang, W.C. (2009). Integrity preservation and privacy protection for medical images with histogram-based reversible data hiding. *IEEE Life Science Systems and Applications Workshop*. <https://doi.org/10.1109/LISSA.2011.5754168>
- [14] Kaur, M., Kaur, R. (2012). Reversible watermarking of medical images authentication and recover-a survey. *Journal of Information and Operation Management*, 3(1): 241-244.
- [15] Singh, A.K., Dave, M., Mohan, A. (2016). Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*, 75(14): 8381-8401. <https://doi.org/10.1007/s11042-015-2754-7>
- [16] Singh, A.K., Dave, M., Mohan, A. (2013). Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain. *National Academy of Sciences, Lett*, 37(4): 351-358. <https://doi.org/10.1007/s40009-014-0241-8>
- [17] Sailaja, R., Rupa, Ch., Chakravarthy, A.S.N. (2017). Robust and indiscernible multimedia watermarking using light weight mutational methodology. *Traitement Du Signal*, 34(1-2): 45-55. <http://dx.doi.org/10.3166/ts.34.45-55>

SUBSCRIPTS

I_c	Cover Image
I_w	Watermark Image
X_p	Partition or Block
$[A_1, H_1, D_1, V_1]$	Coefficients of Cover Image
I_{wk}	Watermarked Image
$[A_{1w}, H_{1w}, D_{1w}, V_{1w}]$	Coefficient of Watermarked Image
X_{pH}, X_{pD}, X_{pV}	Coefficients of extracted watermark