A Wavelet-Based Blind Digital Image Watermarking using Dynamic LSB Replacement (DLSBR) and Symmetric Key Cryptography

Ananya Ghosh, Subhadeep Koley and Sagnik Acharyya

Abstract With advancement of technology and ease of access of digital information and its creation and transference, protection of copyrights for information security is of the prime concern. Digital watermarking gives copyright protection of digital images by impregnating additional information in the original cover image. Thus, watermarking prevents illegal copying by providing a method of enacting the ownership of a redistributed copy. In this paper, we have proposed a wavelet-based dynamic LSB replacement method, which serves the purpose by providing excellent robustness and imperceptibility. Moreover, the watermark is encrypted by a symmetric key cryptographic algorithm to make it secure from further eavesdropping.

Keywords Digital watermarking · LWT · LSB replacement · Symmetric Key Cryptography

1 Introduction

Enormous usage of cloud computing-based systems and transmission of massive multimedia information over the Internet have created a prominent need for state-of-the-art information security frameworks [1]. Steganography, cryptography, and digital watermarking are the methods developed over the years to ensure secure and seamless transmission of data from transmitter to receiver. With the aid of digital watermarking, it is feasible to protect the ownership of any multimedia content and to defend intruders against any sort of attack [2–4]. Digital watermarking can be

A. Ghosh
National Institute of Technology, Durgapur, India
e-mail: ananyag81196@gmail.com

S. Koley (✉) · S. Acharyya
RCC Institute of Information Technology, Kolkata, India
e-mail: subhadeepkoley@gmail.com

S. Acharyya
e-mail: sagnik.acharyya@gmail.com

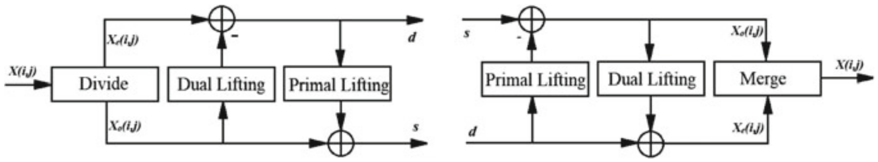
S. Bhattacharyya et al. (eds.), *Recent Trends in Signal and Image Processing*,
Advances in Intelligent Systems and Computing 922,
https://doi.org/10.1007/978-981-13-6783-0_10

mostly classified into three domains, namely frequency domain, spatial domain, and hybrid domain. Hybrid and frequency domain watermarkings are robust and have high computational complexity, whereas watermarking in the spatial domain has added advantages of simplicity and low computational complexity [2]. However, nowadays techniques in wavelet domain are becoming more popular because of the accurate human visual system (HVS) modelling [5]. Recently, outstanding progress has been made in the area of digital image watermarking. Nayak et al. proposed a visual saliency-based LSB replacement method, which has the advantage of increased imperceptibility but at the cost of less robustness [3]. Basu et al. proposed another visual attention model-based pixel adaptive LSB replacement method, which is good in terms of robustness but has a minimal peak signal-to-noise ratio (PSNR) [2]. Verma et al. proposed a novel watermarking scheme based on dynamic stochastic resonance (DSR) and lifting wavelet transform (LWT). In this technique, the attacked image is subjected to DSR to enhance the watermark coefficients to achieve maximum correlation [6]. Tian et al. gave another HVS-based approach of the unique dual watermarking for simultaneous copyright protection and tamper detection [4]. This technique is very robust for all kinds of single and combined attacks but has higher computational complexity. We have incorporated the integer-to-integer LWT instead of conventional discrete wavelet transform (DWT) to segregate the low-frequency component of the image, and then the binary watermark is infused inside the cover image via dynamic LSB replacement (DLSBR). However, only watermarking is not enough to protect the ownership information inside an image. The watermark logo must be encrypted with some sort of encryption in order to attain added security [7]. Therefore, the original watermark logo is transformed into a random chaotic image using symmetric key cryptography (SKC) based on a private key. The same private key is needed at the time of decryption as used for encryption. The rest of the paper contains some other sections like proposed methodology followed by result analysis and conclusion.

2 Proposed Methodology

2.1 Lifting Wavelet Transform

The LWT proposed by W. Sweldens is the second-generation wavelet transform, an advancement of DWT [8]. It is faster and requires lesser memory space as compared to the traditional wavelet [9]. It generates integer coefficients for all sub-bands unlike the conventional first-generation scheme, which generates floating point coefficients, which may be truncated at any point of time during further processing [9]. LWT transforms the original image to four sub-bands, namely LL, containing low-frequency components, and most of the image energy and LH, HL, *and* HH comprising of high-frequency detailed information. Therefore, we use LL sub-band to embed the watermark data. Lifting scheme in general consists of three steps, namely divide, dual lifting, and primal lifting (Fig. 1).



(a) Forward lifting scheme **(b)** Reverse lifting scheme

Fig. 1 Lifting wavelet transform

1. Divide Operation: The sample image $X\,(i,\ j)$ is divided into two subsets, i.e. even sample set $X_e\ (i,\ j)$ and odd sample set $X_o\ (i,\ j)$ as described in Eqs. 1, and 2.

$$X_e(i,j) = X\,(i,2j) \tag{1}$$

$$X_o(i,j) = X\,(i,2j+1) \tag{2}$$

2. Dual Lifting: The odd sample set $X_o(i,\ j)$ is estimated from the local neighbourhood even coefficients with a prediction operator P. The error in odd sample prediction is used to generate the high-frequency coefficients $h(i,j)$ as described in Eq. 3.

$$h(i,j) = X_o(i,j) - P[X_e(i,j)] \tag{3}$$

From Eq. 4, we can recover the odd sample set as shown below

$$X_o(i,j) = h(i,j) + P[X_e(i,j)] \tag{4}$$

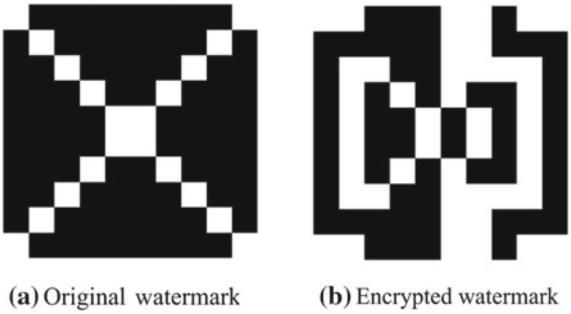
3. Primal Lifting: The low-frequency coefficients $l(i,\ j)$ are generated by revising the even sample with the updating value $U_h(i,j)$ as shown in Eq. 5.

$$l(i,j) = X_e(i,j) + U_h(i,j) \tag{5}$$

2.2 Symmetric Key Cryptography

The robustness of the proposed scheme is further enhanced by addition encryption to the watermark through symmetric key cryptography, which covers the inner information from eavesdroppers. The encryption process includes the following steps

Fig. 2 Watermark before and after encryption



(a) Original watermark **(b)** Encrypted watermark

1. Segregate all rows of the binary watermark in separate arrays.
2. Convert the user-given key to 16-bit binary sequence.
3. Perform bit-wise XOR between the 16-bit binary sequence and the segregated rows of the watermark.
4. Perform Step 3 until all the rows are processed.
5. Concatenate all the processed rows to get the encrypted watermark.

The decryption process is exactly the same as the encryption process, as performing *XOR* again between the segregated rows and the binary version of the user-given decryption key will yield the original unprocessed rows. Figure 2 depicts the original as well as the encrypted watermark.

2.3 Watermark Encoder and Decoder

Let I be the original host image of size $m \times n$. The image is represented as

$$I = X(i,j) \mid 0 \le I < m,\ 0 \le I < n,\ X(i,j) \in \{0,\ 1,\ 2,\ \ldots,\ 255\} \tag{6}$$

Also, W is the original binary logo of size $p \times q$ and characterized as

$$W = V(i,j) \mid 0 \le I < p,\ 0 \le I < q,\ V(i,j) \in \{0,\ 1\} \tag{7}$$

After encryption, the original logo W is changed to W_k and represented as

$$W_k = A_{\text{enc}}(W, k) \tag{8}$$

where A_{enc} is the encryption operator and k is the private encryption key. The decrypted watermark W_d is represented as

$$W_d = A_{\text{dec}}(W_d, k) \tag{9}$$

where A_{dec} is the decryption operator.

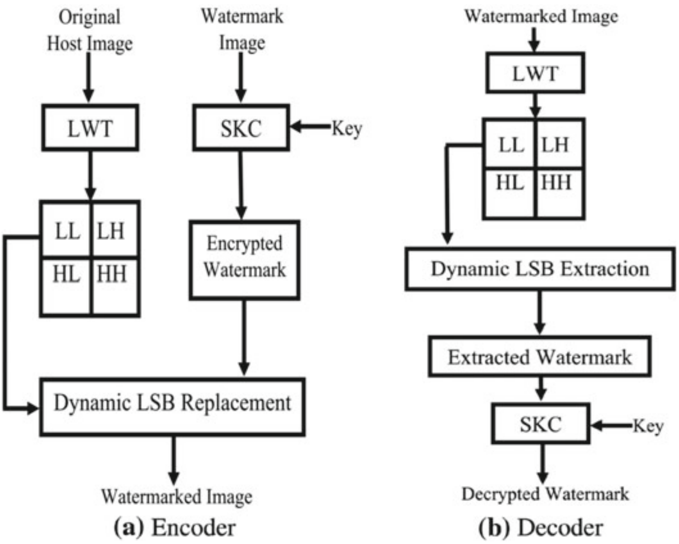


Fig. 3 Watermark encoder and decoder block diagram

Figure 3 represents the watermark encoding and decoding procedures. Here, the '*approximation*' or the '*LL*' component is isolated from the image via LWT. After the watermark encryption process, based on the *LL* coefficient value each watermark bit is infused inside the *LL* block of the cover image via a novel method called the *dynamic least significant bit replacement (DLSBR)*. In DLSBR, the LSBs of the *LL* block coefficients are replaced dynamically with the watermark bits depending upon the *LL* coefficient values. If the *LL* coefficient value is less than 100 then last 3 bits, if coefficient value is less than 200 and greater than 100 then last 2 bits, otherwise last 1 bit of the *LL* coefficient is replaced with the watermark bit. This dynamic substitution has proven to be more robust than conventional single-bit replacement. Being a *blind* watermarking process, the decoder does not need the original host image in the time of decoding. The decoding process is depicted in Fig. 3b. In the decoding process, each watermark bit is extracted from the *LL* coefficients using dynamic LSB extraction. To decrypt the extracted watermark, one should provide the same private key as used in the time of encryption. However, the robustness against attacks and the visual imperceptibility of the proposed algorithm must be evaluated using some well-established quality metrics, which is the topic of discussion in the next subsection.

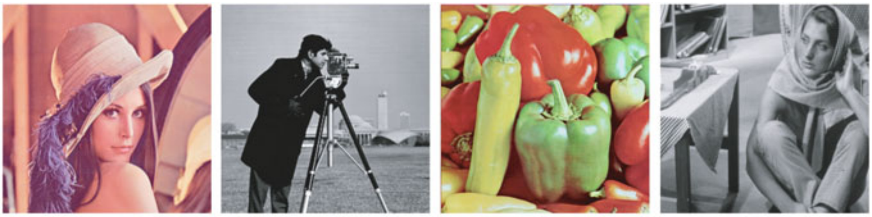
3 Result Analysis and Discussion

To test the imperceptibility and the robustness of the scheme proposed, we have taken several standard 512 × 512 grayscale and colour images and one binary watermark of dimension 10 × 10. Figure 4 depicts four out of the various cover images we have used. Figure 5 shows the corresponding watermarked image along with corresponding *PSNR* and *structural similarity index (SSIM)*.

From Fig. 5, it is evident that the watermark image has no visible hint of the hidden logo and also all of the images possess high PSNR and SSIM value. To prove the imperceptibility of the proposed scheme, Table 1 has been presented with some renowned quality metrics [2]. Metric values in S. No. 1–2, 5–9, 12–15 depict premier quality as higher metric value denotes better imperceptibility [2]. On the other hand, metric values in S. No. 3–4, 10–11, also illustrate that the hidden logo is completely invisible as lower metric value denotes higher imperceptibility [2]. Hence, the proposed algorithm is proven to be beneficial in every test of imperceptibility. 'Robustness' deals with the proficiency of the watermarking algorithm in correctly detecting the watermark in the cover image after common geometric and signal processing attacks [1]. Figure 6 is presented with some attacked watermarked images along with the corresponding retrieved watermarks. It is evident from Fig. 6 that the watermarked image can sustain the watermark even after strong signal processing and geometric impairments.

(a) Lena **(b)** Cameraman **(c)** Peppers **(d)** Barbara

Fig. 4 Original cover images



(a) Lena PSNR=75.51dB SSIM=1 **(b)** Cameraman PSNR=70.14dB SSIM=1 **(c)** Peppers PSNR=72.30dB SSIM=1 **(d)** Barbara PSNR=70.05dB SSIM=1

Fig. 5 Watermarked images and their PSNR and SSIM values

Table 1 Result of various imperceptibility metrics on *Lena* image

S. No.	Metrics	Value
1	Peak signal-to-noise ratio	75.51 dB
2	Structural similarity index	1.0000
3	Average difference	0
4	Mean square error	0.000182
5	Structural content	1.0000
6	Signal-to-noise ratio	65.6533 dB
7	Image fidelity criterion	7.438
8	Universal image quality index	1.0000
9	Normalized cross-correlation	1.0000
10	Normalized absolute error	0.000002
11	Laplacian mean square error	0.000019
12	Weighted signal-to-noise ratio	92.3797 dB
13	Visual information fidelity	0.9992
14	Pixel-based visual information fidelity	0.9999
15	Multi-scale structural similarity index	1.0000

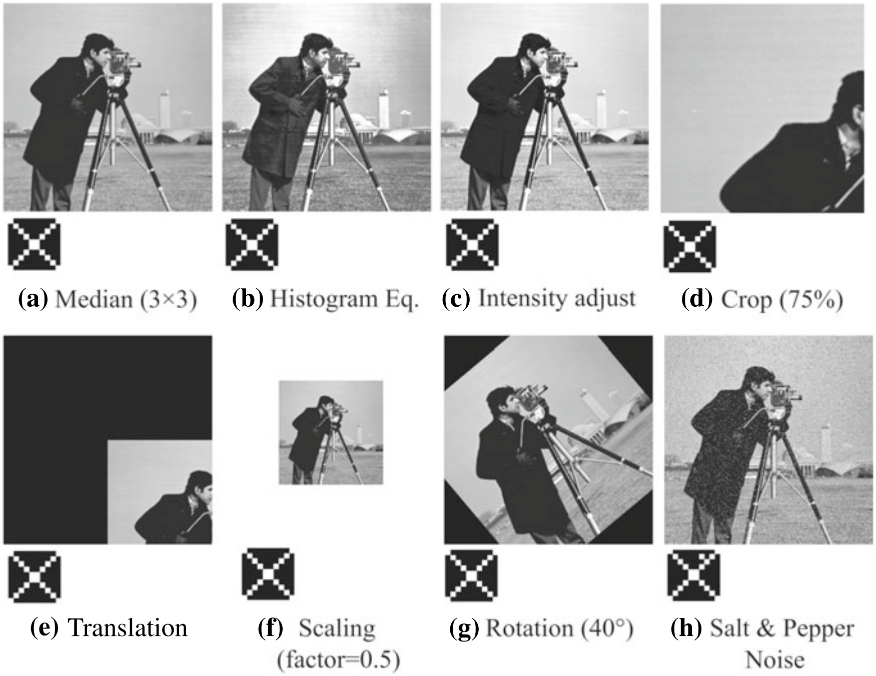


Fig. 6 Attacked watermarked images and corresponding extracted watermarks

Table 2 Imperceptibility comparison with various state-of-the-art methods

S. No.	Method	PSNR (dB)	SSIM
1	**Proposed scheme**	**75.51**	**1.0000**
2	Visual attention model-based LSB replacement [2]	42.27	0.9490
3	Visual saliency-based watermarking approach [3]	54.00	0.9670
4	DCT-based compression sensing watermarking [10]	47.19	0.9958
5	Bit pairs matching and cryptographic watermarking [11]	52.99	0.9854
6	Image region detector-based spatial watermarking [12]	53.35	0.9930

Bold signifies the highest metric value among all the competing method and also the result of the proposed method

Normalized cross-correlation (NCC) has been taken as the primary metric to test our approach. In most of the cases, we got the NCC value of 1 or almost 1. Other metric values like *SSIM, MSE, PSNR* are also in support of the superior ruggedness of the algorithm. To establish the superiority of the proposed framework, a competitive analogy with various state-of-the-art schemes has been drawn in Table 2. It can be observed that, among all models, the projected approach gives highest PSNR as well as SSIM.

4 Conclusion

A wavelet domain, blind watermarking, and secure watermarking framework have been presented in this paper. This scheme impregnates the watermark by substituting the LSBs of the *LL* block coefficients with the watermark bits. Furthermore, the original watermark logo is encrypted with SKC for added security. Experimental results establish the fact that the projected approach has excellent imperceptibility and is robust against most forms of signal processing impairments. In near future, we aim to make the algorithm faster for effective hardware implementation.

References

1. Cox IJ, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
2. Basu A, Sarkar SK (2013) On the implementation of robust copyright protection scheme using visual attention model. Inf Secur J Glob Perspect 22(1):10–20

3. Nayak MR, Tudu B, Basu A, Sarkar SK (2015) On the implementation of a secured digital watermarking frame work. Inf Secur J Glob Perspect 24(1):1–9
4. Tian L, Zheng N, Xue J, Li C, Wang X (2011) An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection. Signal Process Image Commun 26(8–9):427–437
5. Reddy AA, Chatterjii BN (2005) A new wavelet based logo watermarking scheme. Pattern RecognLett 26(7):1019–1027
6. Verma VS, Jha RK (2017) LWT-DSR based new robust framework for watermark extraction under intentional attack conditions. J Franklin Inst, Elsevier 354(14):6422–6449
7. Menezes AJ, van Oorschot PC, Vanstone SA (1996) Handbook of applied cryptography. CRC Press, Boca Raton, FL
8. Sweldens W (1998) The lifting scheme: a construction of second generation wavelets. Soc Ind Appl Math 29(2):511–546
9. Lee S, Yoo CD, Kalker T (2007) Reversible image watermarking based on integer-to-integer wavelet transform. IEEE Trans Inf Forensics Secur 2(3):321–330
10. Thanki R, Dwivedi V, Borisagar K (2017) A hybrid watermarking scheme with CS theory for security of multimedia data. J King Saud Univ Comput Inf Sci 1–10
11. Bal SN, Nayak MR, Sarkar SK (2018) On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. J King Saud Univ Comput Inf Sci 1–10
12. Abraham J, Paul V (2017) An imperceptible spatial domain color image watermarking scheme. J King Saud Univ Comput Inf Sci 1–10