Date of publication SEP-30, 2022, date of current version MAY-30, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.3.2685

A Competent Hybrid Digital Image Watermarking Technique Based on Daubechies Wavelet and Block Bitmap Modification

HAYDER G. A. ALTAMEEMI, AHMED A. ALANI, AHMED ABDUL AZEEZ ASMAEL, MUDHAR A. AL-OBAIDI

Middle Technical University, Technical Institute of Baquba, Baquba, Diyala – Iraq

Corresponding author: Mudhar A. Al-Obaidi (e-mail: dr.mudhar.alaubedy@mtu.edu.iq).

ABSTRACT Over many years, in order to provide powerful techniques for protecting digital copyrights, digital watermarking techniques have been developed. This research focuses on proposing an efficient blind hybrid digital image watermarking technique based on the transformation of Daubechies wavelet (DW) and Block Bitmap modification (BBM). DW represents an effective multi-determination frequency domain for including the watermarks. The BBM is used to afford an enhanced capability of embedding and minimize distortion. Two layers of security have been added to the proposed technique for protecting digital images from theft by using the logistic chaotic mapping to select the position of the blocks for the embedding process and Lorenz chaotic mapping for scrambling the watermark image. In the experiments, high values of peak signal to noise ratio (PSNR) and structural similarity index (SSIM) are obtained, and all the obtained results illustrate that the presented technique is highly imperceptible, secure, and robust.

KEYWORDS Hybrid Digital Image Watermarking; Daubechies Wavelet (DW); Block Bitmap Modification (BBM); Logistic Mapping; Lorenz Mapping.

I. INTRODUCTION

Nowadays, as the Internet is being everywhere and digitizing devices like digital cameras and scanners are further obtainable, people can simply share their own resources [1]. In other words, the rapid growing in the utilization of the Internet, PCs, and the technology of digital media has led to sharing digital media with ease. Although the individuals enjoy these conveniences, several critical problems in digital media like unlawful editing, copying, authentication, and distribution are emerged. This occurrence has produced a significant necessity to develop typical solutions for preventing these problems. Moreover, the existence of many image processing tools facilitates the illegal utilization of such media. The illegal users are capable of easily copying, deleting or modifying digital media. This illegal statement has already caused the appearance of intellectual property rights techniques for protecting digital media [2]. Recently, digital watermarking technique has been specified as the main tool to attain copyright authentication/protection in which the digital watermarks can be included in the original cover image in the spatial domain or frequency domain [3]. In the spatial domain, the watermarks are included in the original image via directly adjusting the pixels. However, the watermarks are included via adjusting the coefficients of the transformed image in the frequency domain [4]. It is important to mention that the spatial domain technique has less complexity of computation and less robustness compared to the frequency domain technique [5]. There are various kinds of frequency transformation techniques that are commonly used: Discrete wavelet transform (DWT), Singular Value Decomposition (SVD), and Discrete Cosine transform (DCT) [6]. DWT has a lower computation of many-sided quality. This domain decomposes the image into sub-bands in which the sub-bands provide segregated low and high frequency wavelet coefficients. It possesses a highly convenient position to break down images with characteristics of multiple determination [7]. Furthermore, DWT superiorly detects isotropic merit of the system of human vision more than other transformation techniques [8]. This merit helps to include watermarks in less sensitive positions in accordance with the system of human vision. Thus, the robustness of the watermarking is increased, with no additional degradation in the image quality [9].

This research is arranged as follows: Section 2 reviews the recently existing associated studies. The relevant methodologies are explained in section 3, which involves DWT, Logistic Mapping, and Lorenz Mapping. Section 4 shows the procedures of watermark embedding and extracting.

Section 5 illustrates the results of simulation. Finally, the conclusions are specified.

II. RELATED WORKS

In the field of digital images watermarking, many hybrid techniques were proposed. The foremost concern that encounters these schemes is to attain most significant factors of digital image watermarking including the capacity, security, superiority, and imperceptibility.

Jane and Elbaşi [10] presented a hybrid and non-blind technique of digital image watermarking dependent on DWT and SVD. In this technique, the host gray image was converted into four sub-bands of DWT, and the SVD was performed to the LL sub-band, after that, for embedding the watermark bits, the coefficients of diagonal singular value were modified withe watermark via utilizing a powerful element. Most findings illustrated that this technique has relatively decent robustness and reliability. In spite of the fact that the watermark was included in LL sub-band, this technique provided reasonable results against several types of attacks like filtering, scaling, and cropping. This technique needs to provide the security and capacity factors required for watermarking.

Arya et al. [11] proposed a non-blind technique of digital image watermarking dependent on DCT and DWT. In this technique, DWT was executed on the gray original cover image. Then, DCT was performed on each 8x8 block of LL sub-band, after that, the watermark bits were included in the final pixel at each block. Results explained that the presented technique is robust against particular kinds of attack with a reasonable imperceptibility. However, this technique ignored the security and capacity factors required for watermarking.

Saravanan et al. [12] suggested a technique of digital image watermarking dependent on DWT, discrete Fourier transform (DFT), and SVD. The family of the DW was utilized for performing DWT, wherein this step, the coefficients of the horizontal detail of the image was used. In the second step, the problem of DWT translation variance was compensated by using the DFT, where the image frequency characteristics were exploited. After that, DCT was utilized for compression. In the Final step, SVD has utilized for emerging the watermark image into the cover image. The obtained results show a good increase in the values of PSNR, but this presented technique needs to make the watermark more secure.

Al-Shayea et al. [13] presented a technique of digital image watermarking dependent on DW. This family of wavelet domain was very robust against different kinds of attacks. The obtained results show that this technique provides high protection for digital images. However, this technique needs to provide the security and capacity factors required for watermarking.

Waqas et al. [14] utilized a watermarking technique dependent on DW. To provide the security and the initial conditions for the logistic mapping, the hash algorithm was applied to the original cover image. Furthermore, a unique dynamic substitution box was implemented for substituting the watermark. In the embedding process, the DW was applied to the original cover image, and the least significant bits of the vertical coefficient of HL and the diagonal coefficient of HH were replaced with the most significant bits of the watermark. The proposed technique provided two levels of security with a good result of imperceptibility and robustness, despite it ignored the capacity factor required for watermarking.

Up to the authors' knowledge, the utilization of DW with BBM has not yet been used to maximise the efficiency of digital image watermarking. This paper intends to present a new technique of hybrid digital images watermarking based on DW and BBM that is characterized by its high level of security and convenience as well as imperceptibility, capacity, and robustness.

III. THE MAIN METHODOLOGIES

A. DWT

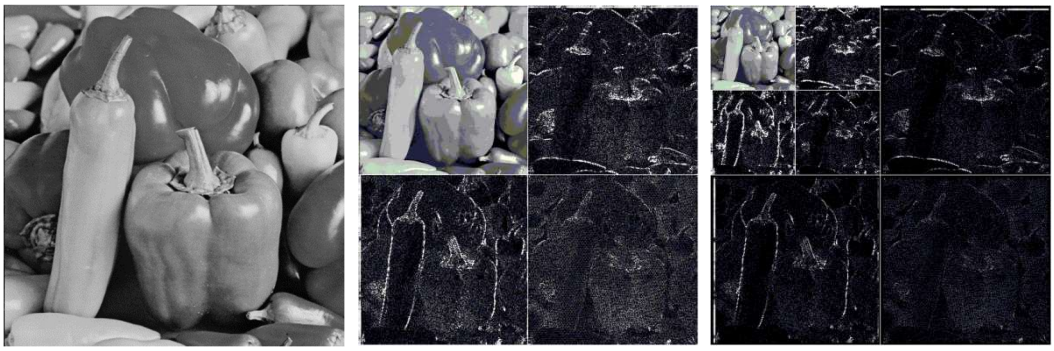
The main principle of applying DWT to the 2D images is implemented via utilizing sub-component filters. Firstly, the image is broken down into four sub-components "LL, HL, LH, HH". LL sub-component can further be decomposed and subsampled. For obtaining the next coarser scaled wavelet components, this process should be performed repeatedly depending on the required application [15].

In the applications of digital watermarking, DWT has minimal complexity of computation when the watermark is included hierarchically via utilizing the technology of DWT [16]. Watermarking techniques based on DWT provides considerable robustness against different kinds of attacks. DWT is capable of selecting various filter banks to the needed broadband. The widely utilized filters are Daubechies, Haar, Biorthogonal, and Coiflets [17, 18].

DW transformation has been used in this paper since it provides a set of robust tools to perform fundamental operations of digital image processing. These operations involve enhancement, removing noise, and etc. Also, it is an effective multi-determination transformation domain for including the watermarks. An instance of 2D DW decomposition is shown in Figs. 1 and 2.

(a) (b) (c)

Figure 1. (a) Lena image, (b) Lena image of 1-level DW, (c) Lena image of 2-levels DW



(a) (b) (c)

Figure 2. (a) Peppers image, (b) Peppers image of 1-level DW, (c) Peppers image of 2-levels DW

B. LOGISTIC MAPPING

The logistic map is a polynomial mapping of degree two, chaotic conduct can expand from candid non-linear dynamical correlations [19]. One of the most notable one-dimensional chaotic maps is the Logistic map. Also, an increase of the sequence length would enhance the randomness of the chaos sequence [20]. The chaotic logistic map is mathematically expressed in Equation 1 within two initial values r and $Logi_0$.

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

where, x_i takes values in the interval (0,1), x_0 is the initial value of the sequence. Also, the chaotic parameter r∈[3,4] is a positive constant that usually acknowledged as the biotic potential. The chaotic logistic map is applied to fabricate the chaotic sequence [21]. Furthermore, it is highly sensitive for initial values, and even when the initial conditions are very close, the uncorrelated chaotic sequences are quite large, and the results of the iteration are not similar. Therefore, it is very complicated for an attacker to find the initial condition of the chaotic map from a sequence with finite-length [17]. In this paper, the logistic mapping is used to control the embedding process (i.e., the selection of blocks for the watermark embedding process).

C. LORENZ MAPPING

Around 1960, the Lorenz system was found by Edward Lorenz. This dynamical system is defined as a nonlinear system of ordinary differential equations, as presented in the following equation:

$$\dot{x} = i(y - x), \dot{y} = (\sigma - z)x - y, \dot{z} = xy - jz, \tag{2}$$

where i, σ, and j are real numbers that represent the control parameters, and x, y, and z indicate state variables. The dots indicate the time derivatives of x, y, and z. With the specified control parameters and the initial values of the state variables, this system is generally solved numerically by utilizing the methods of Runge–Kutta like RK45. Lorenz mapping possesses many characteristics like confusion and diffusion properties, unpredictability, and sensitivity for the initial parameters and conditions [22]. In this paper, the Lorenz chaotic mapping is used to increase the security of the watermark.

IV. THE PROPOSED TECHNIQUE OF HYBRID WATERMARKING

The proposed watermarking technique includes two procedures, such as embedding and extraction. In the procedure of watermark embedding, *1*-level of DW is performed on the original cover image. Since doing any simple change to LL sub-band makes it easy to be perceptible to the human eye, so, HH sub-band and Middle sub-bands are selected as an appropriate position for embedding the watermark. Then, these sub-bands are separated into non-overlapped blocks. The essential processes in this technique are that the watermark is scrambled via Lorenz chaotic mapping, and the selection of blocks for embedding the watermark bits is based on the key generated via logistic chaotic mapping. The scrambled watermark bits are included in the selected blocks based on BBM method. Finally, the watermarked image is constructed by utilizing the modified HH sub-band and Middle sub-bands after applying the inverse of the DW transformation process.

A. THE PROCEDURE OF WATERMARK EMBEDDING

The watermark embedding procedure requires an input cover color image and a watermark binary image to gain the watermarked image [23-25]. Fig. 3 depicts a schematic diagram of the watermark bits embedding procedure. It includes the following steps:

Step 1: Split the input color image into three channels: red, green, and blue (RGB), and use 1-level of 2D DW to transform each channel of image IM into the Daubechies Wavelet Domain.

$$[LL, HL, LH, HH]=DW(IM). \tag{3}$$

Step 2: Segregate the HH sub-band and Middle sub-bands (HL and LH) from the transformed image, and partition them to non-overlapping blocks (each of 4×4 pixels) to be ready for watermark embedding.

Step 3: Scramble the binary watermark bits W by using the Lorenz mapping, and select the blocks for embedding these scrambled watermark bits W^s by using the key generated via logistic mapping (i.e., the number of selected blocks is equal to the number of watermark image bits).

Step 4: Apply the BBM method to embed one bits of W^s in each (4×4) selected block. This method is applied to each block B as follows:

- Firstly, calculate the mean M of the block coefficients, then, calculate xi that indicates the average of pixels' value that are minimum of M, and y^i that indicates the average of pixels' value that are maximum or equal of M.
- Secondly, replace the coefficients of B with the values of x_i and y_i to obtain a new block $\bar{B}$ as follows:

$$\bar{B}_i = \begin{bmatrix} x_i & if \;\; B_i < M \\ y_i & otherwise \end{bmatrix} . \quad (4)$$

Thirdly, obtain the block bitmap $\bar{\bar{B}}$ as follows:

$$\bar{\bar{B}}_i = \begin{bmatrix} 1 & if \;\; \bar{B}_i = y_i \\ 0 & otherwise \end{bmatrix} . \quad (5)$$

- Fourthly, for each watermark bit ${W^s}_i$, if ${W^s}_i$ is 'One' and the number of Ones in the block bitmap $\bar{\bar{B}}$ is odd, then no replacement is done, and when the number of Ones in the block bitmap $\bar{\bar{B}}$ is even, then scan for the first 'Zero' in $\bar{\bar{B}}$ and replace it with 'One'. If ${W^s}_i$ is 'Zero' and the number of Ones in the block bitmap $\bar{\bar{B}}$ is even, then no replacement is done, and when the number of Ones in the block bitmap $\bar{\bar{B}}$ is odd, then find the first 'One' in $\bar{\bar{B}}$ and replace it with 'Zero'.
- Finally, in order to obtain the watermarked block B^w, the coefficient in block B that match the Modified bit in block bitmap $\bar{\bar{B}}$ is replaced with x_i if the Modified bit is equal to 'Zero', else, the coefficient is replaced with y_i.

This step is repeated until all the scrambled watermark bits are embedded.

Step 5: Perform inverse DW transformation on the modified and unmodified sub-bands for getting the final watermarked image.

$$IM_w = Inverse\ DW[LL, HL_w, LH_w, HH_w] . \quad (6)$$

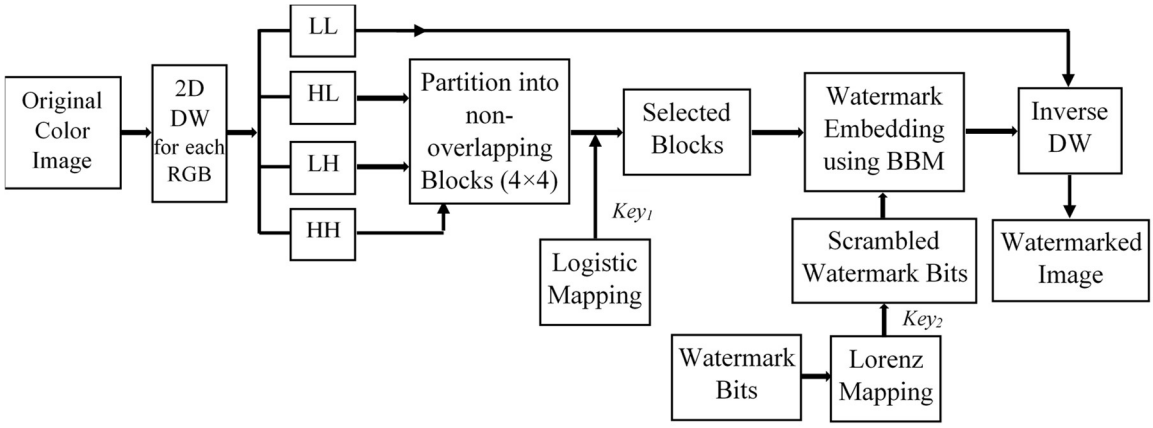


Figure 3. A schematic diagram of the watermark embedding procedure

B. THE PROCEDURE OF WATERMARK EXTRACTION

Fig. 4 provides a schematic diagram of the watermark bits extraction procedure. It includes the following steps:

Step 1: Use 1-level of 2D DW to transform the watermarked image IM_w into the Daubechies Wavelet Domain.

$$[LL, HL_w, LH_w, HH_w] = DW(IM_w) . \quad (7)$$

Step 2: Segregate the HH sub-band and Middle sub-bands (HL and LH) from the transformed watermarked image, and partition them to non-overlapping blocks (each of 4×4 pixels) to be ready for watermark extracting.

Step 3: Select the blocks for extracting scrambled watermark bits by using the key generated via logistic mapping using the same initial values utilized in embedding procedure.

Step 4: Apply the method of BBM to extract one bit from each (4×4) selected block. This method is applied to each block B as follows:

- Firstly, calculate the mean M of the block coefficients, then, calculate xi that indicates the average of pixels' value that are minimum of M, and y_i that indicates the average of pixels' value that are maximum or equal of M.
- Secondly, replace the coefficients of B with the values of x_i and y_i to obtain a new block $\bar{B}$ as in equation (4).
- Thirdly, obtain the block bitmap $\bar{\bar{B}}$ as in equation (5).
- Fourthly, if the number of Ones in the block bitmap $\bar{\bar{B}}$ is odd, then the extracted watermark bit ${\acute{W}^s}_i$ is 'One', else, if the number of Ones in the block bitmap $\bar{\bar{B}}$ is even, then the extracted watermark bit ${\acute{W}^s}_i$is 'Zero'.

$$\acute{W}^s{}_i = \begin{bmatrix} 1 & if\ No.of\ Ones\ in\ \bar{\bar{B}}\ is\ Odd \\ 0 & if\ No.of\ Ones\ in\ \bar{\bar{B}}\ is\ Even \end{bmatrix} . \quad (8)$$

This step is repeated until all the scrambled watermark bits are extracted.

Step 5: Descramble the watermark image by using the watermark scrambling key generated via Lorenz mapping using the same initial values utilized in embedding procedure.

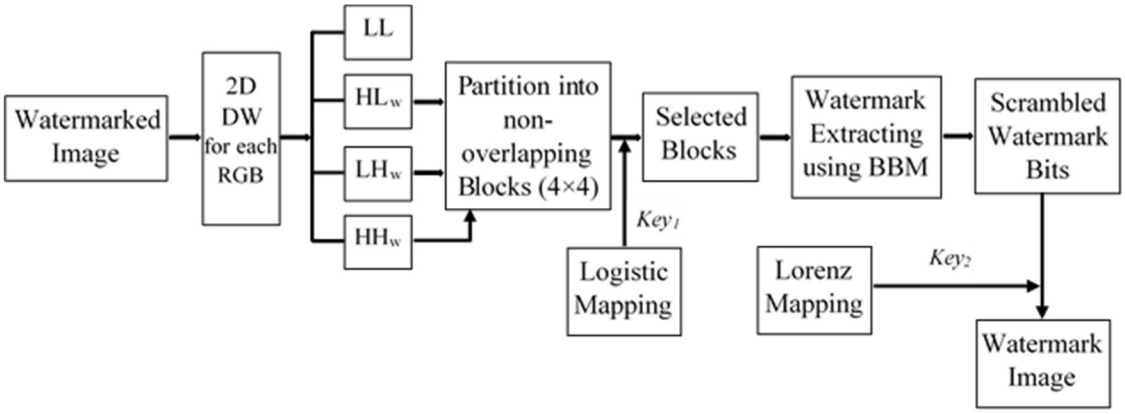


Figure 4. A schematic diagram of the watermark extracting procedure

V. RESULTS AND DISCUSSION

This section utilizes the simulation to clarify the efficiency of the proposed watermarking technique by analyzing the four factors; capacity, security, robustness, and imperceptibility. Here, the computer is run on Windows 10 with Intel-core i7, CPU of 3.20GHz and memory of 16G with version R2018b of Matlab language. The proposed technique is performed on several color images; Women, Car, Lena, Peppers, House, and all of the size 512×512. The utilized watermark images size is 64×64. The utilized watermark images and the original color images are shown in Fig. 5.

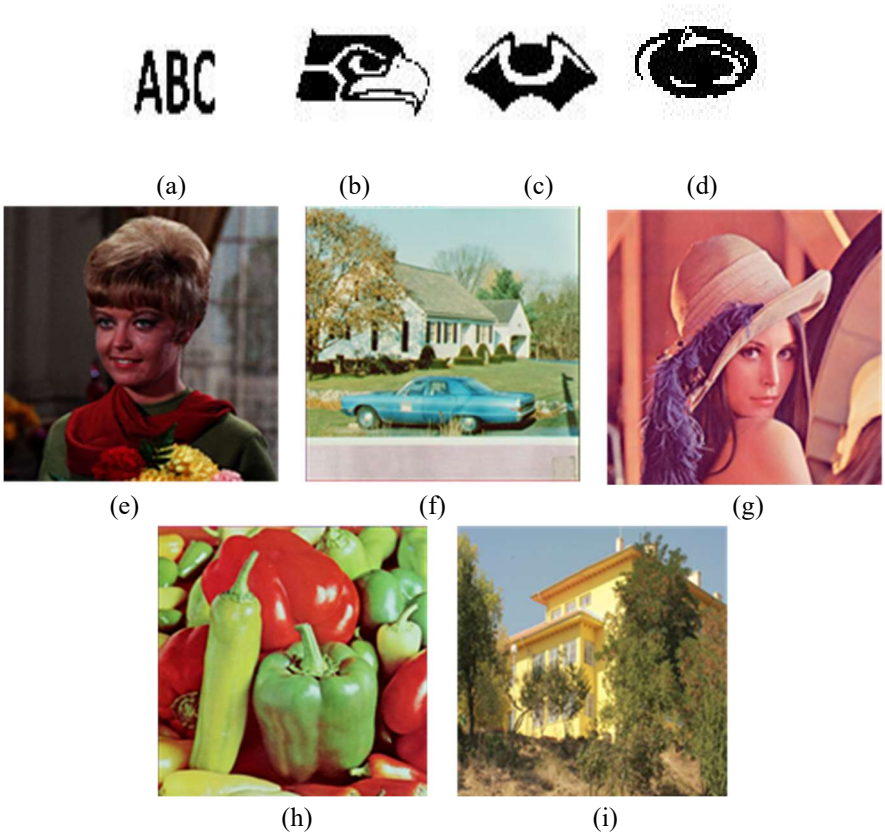


Figure 5. (a-d): The utilized watermark binary images, and (e-i) the original color images

In this research, the structural similarity index (SSIM) and the peak signal-to-noise ratio (PSNR) are deployed to measure the watermarking. The extracted watermarks are equal to the embedded watermarks.

In general, PSNR and SSIM represent the mainly utilized indicators to evaluate imperceptibility. These measurements with higher values indicate the higher quality of the watermarked image. Considering each channel of RGB image (of size m×m), the PSNR measurement is given as follows [7]:

$$\mathrm{PSNR} = \mathrm{L}\frac{(255)^2}{\frac{1}{m\times m}\sum_{k=1}^{m}\sum_{h=1}^{m}[\mathrm{IM}(k,h)\text{-}\mathrm{IM_w}(k,h)]^2}. \quad (9)$$

L indicates 10 logarithm$_{10}$, and IM indicates the input image and IMw indicates the output watermarked image.

The SSIM measurement is given as follows [26]:

$$SSIM(IM, IM_w) = \frac{(2\mu_{IM}\mu_{IM_w}+t_1)(2v_{IMIM_w}+t_2)}{(\mu_{IM}{}^2+\mu_{IM_w}{}^2+t_1)(v_{IM}{}^2+v_{IM_w}{}^2+t_2)}, \quad (10)$$

where, μ_{IM} and μ_{IM_w} indicate the mean values of images IM and *IMw*, respectively. v_{IM} and v_{IM_w} indicate the variance of images *IM* and *IMw*, respectively, and t_1 and t_2 are constants.

The obtained PSNR values were varied between 34 and 38 db, and the obtained SSIM values were extremely close to one. The obtained results showed that the proposed hybrid digital image watermarking technique has good imperceptibility.

Tables 1, 2, 3 and 4 show the obtained results of PSNR, and SSIM when embedding the first, second, third, and fourth watermarks, respectively, in the original five color images.

Table 1 shows that the best value of PSNR is 40.5844 in hiding first watermark inside (first) color image (women image), and the best value of SSIM is 0.9955 inside (third) color image (Lena image).

Table 2 shows the best value of PSNR is 40.590 in hiding second watermark inside (first) color image (women image), and the best value of SSIM is 0.9955 inside (third) color image (Lena image).

Table 3 shows the best value of PSNR is 40.5932 in hiding third watermark inside (first) color image (women image), and the best value of SSIM is 0.9955 inside (third) color image (Lena image).

Table 4 shows the best value of PSNR is 40.5532 in hiding third watermark inside (first) color image (women image), and the best value of SSIM is 0.9955 inside (third) color image (Lena image). Based on the obtained results of Tables 1, 2, 3 and 4, it is easy to notice that the women and Lena images have the highest values of PSNR and SSIM, respectively, and this means the number of replacements in the block bitmap is at a small rate and this leads to watermarked image quality at a higher rate. If the watermark bits satisfied the condition of no replacement in the block bitmap, then the quality of the watermarked image still high values.

In order to test the technique's robustness, several attacks are applied to the watermarked images. The obtained results of SSIM values for the extracted watermarks after implementing the Gaussian noise and salt and pepper noise are acceptable. Furthermore, the obtained results of SSIM values for the extracted watermarks after implementing the Intensity Adjustment, Gamma Correction, and histogram equalization are approximately perfect.

As shown in Table 5, some of the related works have been chosen to provide a comparison for verifying the imperceptibility of the proposed technique utilising the DW transformation and Lena color image (of size 512×512).

Table 1. Results of embedding the first watermark in the original color images

Image	PSNR	SSIM
Women	40.5844	0.9675
Car	37.7553	0.9715
Lena	40.2889	0.9955
Peppers	39.4345	0.9954
House	38.2197	0.9832

Table 2. Results of embedding the second watermark in the original color images

Image	PSNR	SSIM
Women	40.5900	0.9675
Car	37.7300	0.9713
Lena	40.2798	0.9955
Peppers	39.4172	0.9954
House	38.1607	0.9830

Table 3. Results of embedding the third watermark in the original color images

Image	PSNR	SSIM
Women	40.5932	0.9674
Car	37.7294	0.9712
Lena	40.2723	0.9955
Peppers	39.4111	0.9954
House	37.9688	0.9830

Table 4. Results of embedding the fourth watermark in the original color images

Image	PSNR	SSIM
Women	40.5532	0.9673
Car	37.7244	0.9713
Lena	39.9670	0.9955
Peppers	39.1329	0.9954
House	38.1604	0.9830

Table 5. Comparison with some related works

Authors Name, Year	Logistic Mapping	Average PSNR	Average SSIM
Saravanan et al. (2016)	No	36.3922	-
Waqas et al. (2019)	Yes	37.1237	0.9417
Proposed Technique	Yes	37.2770	0.9955

VI. CONCLUSIONS

In this research, an efficient and secure digital image watermarking technique based on DW and BBM is developed to shield the copyright of the digital images. The new technique of digital image watermarking possesses strong robustness, high imperceptibility, and large embedding capacity. A high level of security could be provided when using the Logistic mapping for selecting the blocks identified for embedding watermark bits, via benefiting from the aperiodic features, irrelevant and non-convergent. Also, another level of security has been added by using the Lorenz chaotic mapping for scrambling the watermark bits.

References

[1] D. Rayburn, *Streaming and Digital Media: Understanding the Business and Technology*, CRC Press, London, 2012. https://doi.org/10.4324/9780080476339.

[2] S. M. Arora, "A DWT-SVD based robust digital watermarking for digital images," *Procedia Computer Science*, no. 132, pp. 1441-1448, 2018. https://doi.org/10.1016/j.procs.2018.05.076.

[3] M. Begum, M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, issue 2, 110, 2020. https://doi.org/10.3390/info11020110.

[4] E. H. M. El-Shazly, *Digital Image Watermarking in Transform Domains*, Egypt, 2004.

[5] H.-J. Ko, C.-T. Huang, G. Horng, S.-J. Wang, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation," *Information Sciences*, vol. 517, pp. 128-147, 2020. https://doi.org/10.1016/j.ins.2019.11.005.

[6] M. I. Khan, M. Rahman, M. Sarker, I. Hasan, "Digital watermarking for image authentication based on combined DCT, DWT and SVD transformation," arXiv preprint arXiv:1307 6328, 2013.

[7] J. Waleed, D. Huang, S. Hameed, "An optimized digital image watermarking technique based on cuckoo search (CS)," *ICIC Express Letters. Part B, Applications: An International Journal of Research and Surveys*, vol. 6, issue 10, pp. 2629-2634, 2015.

[8] N. Al Bassam, V. Ramachandran, S. E. Parameswaran, Wavelet Theory and Application in Communication and Signal Processing, *Open Access Peer-Reviewed Chapter*, IntechOpen, 2021. https://doi.org/10.5772/intechopen.95047.

[9] T. K. Araghi, A. A. Manaf, "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*, vol. 101, pp. 1223-1246, 2019. https://doi.org/10.1016/j.future.2019.07.064.

[10] O. Jane, E. Elbaşi, "Hybrid non-blind watermarking based on DWT and SVD," *Journal of Applied Research and Technology*, vol. 12, issue 4, pp. 750-761, 2014. https://doi.org/10.1016/S1665-6423(14)70091-4.

[11] R. K. Arya, S. Singh, R. Saharan, "A secure non-blind block based digital image watermarking technique using DWT and DCT," *Proceedings of the 2015 IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2015, pp. 2042-2048. https://doi.org/10.1109/ICACCI.2015.7275917.

[12] P. Saravanan, M. Sreekara, K. Manikantan, "Digital image watermarking using Daubechies wavelets," *Proceedings of the 2016 3rd IEEE International Conference on Signal Processing and Integrated Networks (SPIN)*, 2016, pp. 57-62. https://doi.org/10.1109/SPIN.2016.7566662.

[13] T. K. Al-Shayea, C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla, E. K. Markakis, E. Pallis, "On the efficiency evaluation of a novel scheme based on Daubechies wavelet for watermarking in 5G," *Proceedings of the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1-6. https://doi.org/10.1109/CAMAD.2018.8514968.

[14] U. A. Waqas, M. Khan, S.I. Batool, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," *Multimedia Tools and Applications*, vol. 79, pp. 6891-6914, 2019. https://doi.org/10.1007/s11042-019-08570-5.

[15] J. Wang, Z. Du, "A method of processing color image watermarking based on the Haar wavelet," *Journal of Visual Communication and Image Representation*, vol. 64, article 102627, 2019. https://doi.org/10.1016/j.jvcir.2019.102627.

[16] A. Mohanarathinam, S. Kamalraj, G. P. Venkatesan, R. V. Ravi, C. S. Manikandababu, "Digital watermarking techniques for image security: a review," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-9, 2019. https://doi.org/10.1007/s12652-019-01500-1.

[17] Y. Liu, S. Tang, R. Liu, L. Zhang, Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95-105, 2018. https://doi.org/10.1016/j.eswa.2017.12.003.

[18] V. S. Verma, and R. K. Jha, "An overview of robust digital image watermarking," *IETE Technical review*, vol. 32, issue 6, pp. 479-496, 2015. https://doi.org/10.1080/02564602.2015.1042927.

[19] R. M. May, "Simple mathematical models with very complicated dynamics," In: Hunt, B.R., Li, TY., Kennedy, J.A., Nusse, H.E. (eds) The Theory of Chaotic Attractors. Springer, New York, NY, 2004, pp. 85–93. https://doi.org/10.1007/978-0-387-21830-4_7.

[20] M. Alawida, A. Samsudin, W. H. Alshoura, "Enhancing one-dimensional chaotic map based on bitstream dividing model," *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 2019, pp. 130-134. https://doi.org/10.1145/3316615.3316657.

[21] J. Zheng, R. Lu, L. Sun, S. Zhuang, "Low-noise multiple watermarks technology based on complex double random phase encoding method," *Proceedings of the Information Optics and Optical Data Storage*, SPIE. Digital library, 2010, vol. 7851, paper 78511E. https://doi.org/10.1117/12.881230.

[22] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, pp. 2395-2405, 2017. https://doi.org/10.1007/s00521-017-3195-1.

[23] J. Abraham, V. Paul, "An imperceptible spatial domain color image watermarking scheme," *Journal of King Saud University – Computer and Information Sciences*, vol. 31, issue 1, pp. 125-133, 2019. https://doi.org/10.1016/j.jksuci.2016.12.004.

[24] J. S. Teh, and A. Samsudin, "A chaos-based authenticated cipher with associated data," Security and Communication Networks, 2017. https://doi.org/10.1155/2017/9040518.

[25] J. S. Teh, A. Samsudin, and A. Akhavan, "Parallel chaotic hash function based on the shuffle-exchange network," *Nonlinear Dynamics*, vol. 81, issue 3, pp. 1067-1079, 2015. https://doi.org/10.1007/s11071-015-2049-6.

[26] H. Zhang, Z. Li, X. Liu, C. Wang, X. Wang, "Robust image watermarking algorithm based on QWT and QSVD using 2D Chebyshev-Logistic map," *Journal of the Franklin Institute*, vol. 359, issue 2, pp. 1755-1781, 2022. https://doi.org/10.1016/j.jfranklin.2021.11.027.

HAYDER G. A. ALTAMEEMI, ***graduated Middle Technical University, Technical Institute of Baqubah. Received Master degree of Technology and Information Systems, 2018, Tambov Technical University, Russia. Specialist in information technology and systems, expert in many programming languages HTML, PHP, JavaScript, C ++, Visual Basic. Experience in project management and client relations. He has a good experience in designing programs and databases for people and institutions, correcting their mistakes, and making modification operations. E-mail: hayderaltamimee@mtu.edu.iq.***

AHMED A. ALANI, ***graduated Middle Technical University, Technical Institute of Baqubah. Received Master degree of Computer Science, information systems technology from University of Dayala, 2006. E-mail: Ahmed.abdulrahman@mtu.edu.iq.***

***AHMED ABDUL AZEEZ ASMAEL**, graduated Middle Technical University, Technical Institute of Baqubah. A. A. Ismael worked and still in technical universities in Iraq since 2016 as a lecturer, The universities he worked for are Diyala University 2015, Al-Bayan Technical University 1016, Northern Technical University 2017, middle Technical University from 2019 to now. The author completed his MSC at Bangalore University, India 2014. He has experiences in the field of computer networks, the Internet and communications, where he worked at the Earth link company for the Internet and Communications for the years 2010 to 2012 as a maintenance engineer and programmer for communications devices. He has participated in international conferences, seminars and workshops in several technical fields. E-mail: Ahmed.abdulazeez@mtu.edu.iq.*

***DR. MUDHAR A. AL-OBAIDI**, graduated Middle Technical University, Technical Institute of Baqubah. Mudhar Al-Obaidi is a Lecturer in Computing at the Middle Technical University, Iraq. He obtained his BSc and MSc degrees in chemical engineering from the University of Baghdad and University of Technology in Iraq in 1993 and 1997, respectively. He obtained his PhD in chemical engineering in 2018 from the University of Bradford, UK. He has contributed to more than 65 peer-reviewed journal papers, conference presentations, and chapters. Recently, he has published his first book related to wastewater treatment. E-mail: dr.mudhar.alaubedy@mtu.edu.iq.*