Al-Khwarizmi Engineering Journal,Vol. 12, No. 2, P.P. 124- 133 (2016)

Al-Khwarizmi Engineering Journal

Digital Image Watermarking Using Arnold Scrambling and Berkeley Wavelet Transform

Iman M.G. Alwan* **Enas Muzaffer Jamel****

, Department of Computer Science /College of Education for Women / University of Baghdad*

*Email:ainms_66@yahoo.com

**Email: enasm.altai@gmail.com

(Received 26 April 2015; accepted 26 November 2015)

Abstract

Embedding an identifying data into digital media such as video, audio or image is known as digital watermarking. In this paper, a non-blind watermarking algorithm based on Berkeley Wavelet Transform is proposed. Firstly, the embedded image is scrambled by using Arnold transform for higher security, and then the embedding process is applied in transform domain of the host image. The experimental results show that this algorithm is invisible and has good robustness for some common image processing operations.

Keywords: *Berkeley Wavelet Transform, image watermarking, Arnold Transform, watermark attack.*

1. Introduction

Due to rapid distribution of digital files such as text, audio, still images or video over fast communication systems, the plans for verification of digital contents originality and copyright ownership are usually demanded. Digital watermarking is a new solution for content protection. It draws significant interests and becomes an active research field [1]. Generally digital watermark is the technology of adding verification message or hidden copyright information called a watermark or label or signature to the digital media so that it can be extracted or detected later to make a confirmation about the object [2].

Several eligible characteristics should be available in watermarking system. They are Imperceptibility, which means perceptual parity between the original and the watermarked images, Robustness, which means the immovability of the watermark data against changes and alteration to the watermarked file, and finally capacity, which indicates the amount of information that can be saved in the cover media . To reveal the watermark information, two techniques are followed. They are blind and non-blind techniques. In the first one the cover media is not required while in the second one, the original media is required for extraction.

Mainly, two alternative watermarking methods exist; spatial and frequency (transform) domains. The spatial domain techniques are not powerful even to the insignificant of altering or removal attempts (attacks), hence these techniques have become less common. On the other hand, the transform domain techniques have taken the most interests by the researchers and almost all of the known transforms have been used [3]. The transforms used are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) [4,5]. In [3] slantlet transform is adapted in watermarking process, while in [6] the contourlet transform is used as a frequency domain watermarking system. The curvelet transform based logo watermarking is proposed in [7].

In [8] a two-dimensional triadic wavelet transform is proposed, it's called Berkeley Wavelet transform. It participates many characteristics like oriented, spatial localization, and frequency bandpass. It is formed by 4-complete, orthogonal bases which the transform and inverse transform computations are fast. Its good computation and fine primary simulation visually makes it a robust tool in watermarking process. In [9], the authors proposed a watermarking scheme based on Berkeley Wavelet Transform. The embedding process is carried out in the DC band of the transformed host image only by sub-dividing it into non-overlapping blocks, and replacing the binary watermarked coefficient with only one designated coefficient of middle frequency diagonally, and then an inverse Berkeley Wavelet Transform isperformed to get the watermarked image. This algorithm embeds a limited amount of information since it is embedded in one band which is (1/9) of the total host image size. They used a host image of size (243x243) and the binary watermark image of size (27x27).

In this paper, Berkeley wavelet transform is used for grey scale image watermarking process, the grey scale watermark image is first scrambled by using Arnold transform to boost the security side, and then it is embedded in the whole frequency bands of the transformed grey scale host image. So the amount of embedded information is greater. From simulation results, the proposed method shows good performance in terms of Peak Signal to Noise Ratio (PSNR) of the watermarked image and normalized correlation (NC) between the watermark image and the extracted one. The performance of the system is also tested under various attacks including noise, JPEG compression, and cropping. The results exhibit a good response of the proposed system. Rest of this paper is organized as follows: The concepts of Berkeley Wavelet Transfrom are introduced in Section 2. In Section 3, the proposed embedding algorithm will be presented. Finally, the Simulation Results and Discussion will be given in Section 4, followed by the conclusions in Section 5.

2. Berkeley Wavelet Transform

The Berkeley wavelet transform is a wavelet basis, triadic, 2- dimensional transform. It presents an effective image representation. Its computational prosperities are useful; it is complete, orthonormal, and a sparse code for images of natural type. BWT includes 4- pairs of mother wavelets at 4- orientations.

At every pair, one of the wavelet is odd symmetric, and the other is even symmetric. Orthonormal, complete basis in 2- dimensions are resulted from the translation and scaling of the total set plus a single constant term of wavelet. The mother wavelets are piecewise constant functions, so each wavelet, $\beta_{\theta,\phi}$, can be totally represented as a matrix $b_{\theta,\phi}$ of 3x3 dimensions [8]:

$$b_{|,0} = \frac{1}{\sqrt{6}}\begin{bmatrix}-1 & 0 & 1\\ -1 & 0 & 1\\ -1 & 0 & 1\end{bmatrix} \quad \ldots(1)$$

$$b_{|,e} = \frac{1}{\sqrt{18}}\begin{bmatrix}-1 & 2 & -1\\ -1 & 2 & -1\\ -1 & 2 & -1\end{bmatrix} \quad \ldots(2)$$

$$b_{/,0} = \frac{1}{\sqrt{6}}\begin{bmatrix}-1 & 1 & 0\\ 1 & 0 & -1\\ 0 & -1 & 1\end{bmatrix} \quad \ldots(3)$$

$$b_{/,e} = \frac{1}{\sqrt{18}}\begin{bmatrix}-1 & -1 & 2\\ -1 & 2 & -1\\ 2 & -1 & -1\end{bmatrix} \quad \ldots(4)$$

$$b_{-,0} = \frac{1}{\sqrt{6}}\begin{bmatrix}-1 & -1 & -1\\ 0 & 0 & 0\\ 1 & 1 & 1\end{bmatrix} \quad \ldots(5)$$

$$b_{-,e} = \frac{1}{\sqrt{18}}\begin{bmatrix}-1 & -1 & -1\\ 2 & 2 & 2\\ -1 & -1 & -1\end{bmatrix} \quad \ldots(6)$$

$$b_{\backslash,0} = \frac{1}{\sqrt{6}}\begin{bmatrix}0 & -1 & 1\\ 1 & 0 & -1\\ -1 & 1 & 0\end{bmatrix} \quad \ldots(7)$$

$$b_{\backslash,e} = \frac{1}{\sqrt{18}}\begin{bmatrix}2 & -1 & -1\\ -1 & 2 & -1\\ -1 & -1 & 2\end{bmatrix} \quad \ldots(8)$$

Daughter wavelets $\beta_{\theta,\phi}^{m,n,s}$ can be produced at various positions *(i, j)* in the x-y plane, and various scales, (s) through scaling and translation of the mother wavelets $\beta_{\theta,\phi}$ by using the dilation equation:

$$\beta_{\theta,\phi}^{m,n,s} = \frac{1}{s^2}\beta_{\theta,\phi}(3^s(x-i), 3^s(y-j)) \quad \ldots(9)$$

The BWT uses triadic scaling, i.e. the sizes of the daughter wavelets are scaled by powers of 3. To form an orthogonal set, the possible translations in the x-y plane are locked to integer multiples of the wavelet size, 3s. All of the BWT wavelets have zero mean, and so a single DC term is required to represent the mean value of an image:

$$\beta_0 = [u(x/3, y/3)]/\sqrt{9} \quad \ldots(10)$$

Note that this DC term is not subject to the dilation equation; instead, it is applied only once, at the largest spatial scale. Since the BWT is a complete, orthonormal set, it is self-inverting. An image can be reconstructed from its BWT coefficients using [8]:

$I(x,y) = \sum_{\theta\in\Theta,\phi\in\Phi} \sum_{m,n,s=0}^{\infty} w_{m,n,s}\beta_{\theta,\emptyset}(3^s(x - m), 3^s(y-n)$ …(11)

where $w_{m,n,s}^{\theta,\phi}$ are the BWT coefficients representing the image.

Figure (1) shows the output of the Berkeley Wavelet Transform of the image Boat as it is obtained by the Berkeley Wavelet Transformation program.

(a) (b)

Fig. 1. The original image (a), the transformed image (b).

3. The Proposed System

The proposed system is based on embedding grey scale visual watermark image of size (1/9) of the host image into the host grey scale image by using Berkeley Wavelet Transform (BWT). For security confirmation and robustness improvement, the watermark image is scrambled before embedding into the host image. Arnold transform algorithm is adopted as a scrambling scheme to the original watermark image. Arnold transform has periodicity process, so the image can be reclaimed after the permutation concept. It is only appropriate for N×N digital images. It is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad \text{…(12)}$$

where (x, y) represent the pixel coordinates of the original image, while (x', y') represent the pixel coordinates of the encrypted image. Let C indicate the matrix at the left of the right hand side of equation (12), $Im(x, y)$ indicate the original image pixels, and $Im(x', y')^n$ indicate pixels of the encrypted image acquired by n-times Arnold transform application. Thence, Arnold transform's image encryption is [10]:

$Im(x',y') = C\ Im(x,y)^{(r-1)}(mod\ N)$ …(13)

Where r = 1, 2, ….. n, and $Im(x',y')^0 = Im(x,y)$.

To obtain $Im(x,y)^{(r-1)}$, the inverse matrix of C can be multiplied at each side of equation (13). This means, the encryption of the encrypted image can be made by computing the equation (14) n-times iteratively.

$D(x,y)^{(r)} = C^{-1}\ D(x',y')^{r-1}(mod\ N)$ …(14)

where $D(x',y')^{(0)}$ is the encrypted image's pixel, and $D(x,y)^{(r)}$ is a decrypted pixel by executing r iterations. Figure (2) shows an example of Arnold image encryption with n=5 for pepper test image of size (256x256).

(a) (b)

Fig. 2. The original image (a), Arnold transformed image (b).

For embedding process, the host image should be a power of $3^n x 3^n$ where n is an integer number, and the bit stream of the encrypted watermark image is transformed into a sequence *wi(1)….wi(L)*, where L is the bit stream length, and $wi(m) \in \{-1,1\}, (m = 1, …., L\}$. The sequence is used as the watermark.

A: Watermark Embedding Process

Input: Host image, Secret image, α the scaling factor.

Output: Watermarked image.

1. Read the host image I(N,N), the watermark image w(m,m).
2. Apply Berkeley wavelet transform to I(N,N). Triadic pattern image decomposition is applied.
3. Apply Arnold transform to the grey- scale watermark image.
4. Change the 2-D 8-bit scrambled watermark pattern of size m x m into a binary sequence $w = \{w(k)|k = 0, …., m^2\}$, where $w(k) \in \{0,1\}$. Then map the watermark information w into a bipolar vector

$wi^b = \{wi^b(k)|k = 0, ……, m^2\}$ and $wi^b(k)$ is denoted as

$wi^b(k) = (-1)^{wi\,(k)}$ …(15)

where k=0,1,…..,m^2

5. Embed the binary sequence in the all transformed host image's subbands according to the formula

$WtImg = H + \alpha \times wi^b$ …(16)

where, *WtImg* is the watermarked image, H is the host Berkeley Wavelet Transformed image, α is the scaling factor, lower value of it gives better quality for the watermarked image, and wi^b is the watermark information stream.

6. Apply the inverse of the Berkeley Wavelet transform to get the watermarked image.
7. End

B: Watermark Extracting Process

It is assumed that the original image, value of α, and number of iteration for Arnold scrambling technique n, are known for extraction procedure.

Input: Watermarked Image.

Output: Watermark secret image.

1. Apply Berkeley Wavelet transform for the watermarked image, to get the transformed subbands.
2. Extract the embedded sequence from the all subbands of the transformed image according to the equation:
3. $wi^b = (WtImg - H)/\alpha$ … (17)
4. Convert the extracted sequence wi^b into 0, 1 sequence, reconstruct the scrambled *mxm* watermark image.
5. Apply the inverse Arnold transform to get the watermark image.
6. End

4. The Simulation Results and Discussion

In this part, the simulation parameters settings of the proposed algorithm, the simulation results, and discussion of the results are exhibited.

4.1 The Simulation Parameters Settings

The proposed algorithm was implemented and tested on several standard images using MATLAB Version 7.0.4.365, and was implemented with an Intel core i7, 2.7 GHz processor. The host images are of size 243x243, and the watermark images are of size 80x80. To evaluate the qualityof the watermarked image, PSNR criteria were adopted. Greater values of PSNR indicate preferable quality of the watermarked image. Values of PSNR more than 30 dBs denote acceptable image quality, where no significant change is made by watermarking process [10]. The algorithm was also tested under different kinds of signal attack. Figure (3a) and (3b) displays the test host, and watermark images. Equation (18) represents the peak signal to noise ratio [10].

$PSNR = 10log_{10}(\frac{255^2}{MSE})$ …(18)

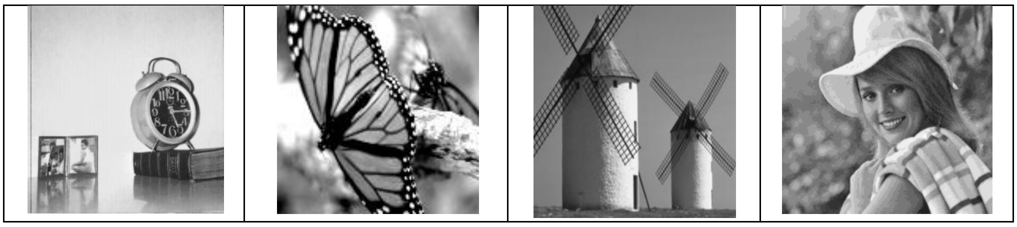
$MSE = (\frac{1}{N})^2 \sum\sum(p_{ij} - p_{ij}^{'})^2$ …(19)

where p_{ij}'s stand for the values of the original pixel, $p_{ij}^{'}$'s stand for the values of the modified pixel, and N is the image dimension. The efficiency of the watermark extraction result is evaluated by using normalized correlation coefficient (NC), for the extracted watermark W' and the original watermark W as:

$NC(W, W^{'}) = \frac{\sum_{i=1}^{n} w(i)w^{'}(i)}{\sqrt{\sum_{i=1}^{n} w(i)^2}\sqrt{\sum_{i=1}^{n} w^{'}(i)^2}}$ …(20)

where (n×n) are the watermark dimensions. The unity value given exact matching between the extracted watermark and the original watermark images, NC of about 0.7 or above is counted passable [11].

a. Test Host Images.



b. Test watermark Images.

Fig. 3. Test host and watermark images.

4.2. The Simulation Results

The simulation results of the proposed algorithm are shown in Figure (4). It shows the watermarked images and the reconstructed watermark images. PSNR values of the watermarked images are also included. The Normalized Correlation (NC) is listed to indicate the similarities between the original watermarks and the extracted ones.

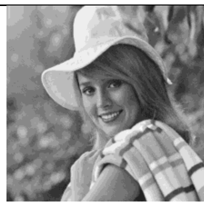
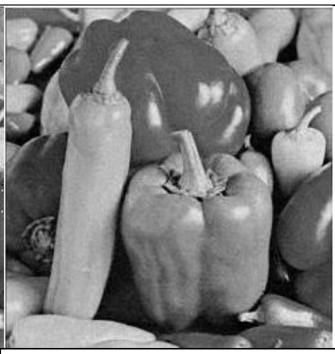
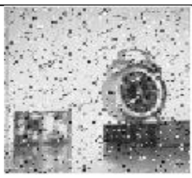
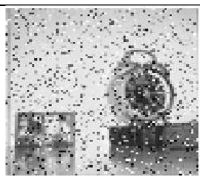
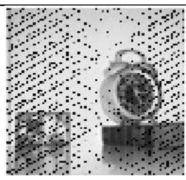
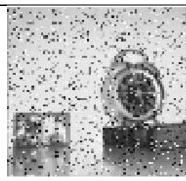
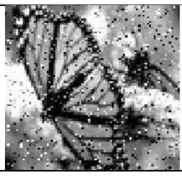
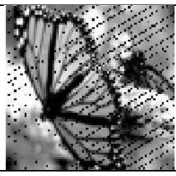
			
PSNR= 40.88 dB	**PSNR=40.66 dB**	**PSNR=40.87 dB**	**PSNR=40.7 dB**
			
NC=1	**NC=1**	**NC=1**	**NC=1**

Fig. 4. The watermarked images and the reconstructed watermark images.

Various attacks are used to test the robustness of the watermark algorithm, such as noise (Gaussian, Salt & Pepper), geometrical distortion (cropping), and JPEG compression. Figure (5) shows results of applying various attacks to the watermarked test image.

			
PSNR= 25.22 dB Salt & Pepper noise	**Gaussian Noise mean=0, variance=0.00005, PSNR= 32.37 dB**	**Crop 1/9 of image PSNR=15.12 dB**	**JPEG compression 30% PSNR= 32.94 dB**
			
NC= 0.8404	**NC=0.8071**	**NC=0.6241**	**NC=0.8043**
			
PSNR= 25.01 dB Salt & Pepper noise	**Gaussian Noise mean=0, variance=0.0005 PSNR= 34.84 dB**	**Crop 1/9 of image PSNR= 16.48 dB**	**JPEG compression 30% PSNR= 30.99 dB**
			
NC=0.8950	**NC=0.8071**	**NC= 0.8293**	**NC= 0.7491**
			
PSNR = 24.90 dB Salt & Pepper noise(0.01)	**Gaussian Noise mean=0, variance=0.00005 PSNR= 35.58 dB**	**Crop 2/9 of image PSNR= 12.93 dB**	**JPEG compression 30% PSNR = 36.44 dB**

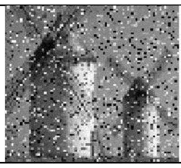
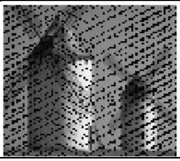
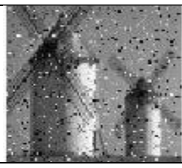
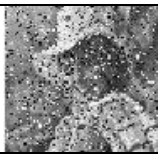
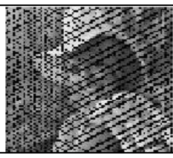
			
NC= 0.7631	**NC=0.6527**	**NC= 0.5391**	**NC= 0.7635**
			
PSNR= 27.68 dB Salt & Pepper noise(0.004)	**Gaussian Noise mean=0, variance=0.0005 PSNR= 31.85 dB**	**Crop 3/9 of image PSNR= 8.14 dB**	**JPEG compression 30% PSNR= 30.99 dB**
			
NC=0.8950	**NC=0.6642**	**NC= 0.4417**	**NC= 0.7930**

Fig. 5. Results of applying various attacks to the watermarked images.

The results of the proposed algorithm were compared with [10] in which non blind digital image watermarking based on discrete wavelet transform has been proposed. The watermark image was encrypted by Arnold transform and Cross chaotic sequence, the encrypted watermark image is transformed into wavelet transform domain, and the medium frequency coefficients are extracted and embedded into the wavelet transformed host image. Figure (6), shows the PSNR and NC of both algorithm in [10] and the proposed one respectively.

Results of algorithm in [10]	Results of the proposed algorithm
	
PSNR=33.243dB.	**PSNR=40.66 dB**
	

Fig. 6. PSNR and NC of both algorithms in [10] and the proposed.

4.3. The Discussion

The simulation results show that the proposed algorithm offers good response in terms of quantitative parameters (Peak-Signal-to-Noise-Ratio and normalized correlation) and in terms of visual quality. From Figure (4), the values of PSNR of the watermarked images are between (40.66- 40.88) dB for the test images which is perfectly convenient for the human eyes since values of PSNR greater than 30 dBs indicate convenient image quality. Also the extracted watermark test images have normalized correlation values of one which means exact similarity between the original and the watermarked images. The inviolability of the watermark versus remove or degradation attempts by attacks of different digital signal processing operations like noise (Gaussian, Salt & Pepper), different rates of geometrical distortion (cropping), and JPEG compression is measured by NC criteria. From the results of Figure (5), it is seen that watermark can be still extracted despite the degradation of image quality due to different types of attacks. Also from Figure (6), it can be noticed that the proposed algorithm offers better imperceptible results. The improvement in the PSNR value for Boat image is 7.417 dB.

5. Conclusion

In this paper, a non-blind digital image watermarking scheme is proposed. It depends on using Berkeley Wavelet Transform (BWT), which is a complete orthonormal basis functions. The watermark image is firstly scrambled by Arnold transform to achieve higher embedding security. The embedding process is done in the whole frequency subbands of the transformed host image. The evaluation of the proposed method in terms of PSNR and normalized correlation shows very good performance as far as invisibility. Also the proposed method offers good response under various image attacks.

Notation

BWT	Berkeley Wavelet Transform
H	host image in BWT domain
Im(x,y)	original image pixel
$Im(x',y')^n$	pixels of encrypted image acquired by n- times Arnold transform.
MSE	Mean Square Error
NC	Normalized Correlation
PSNR	Peak Signal to Noise Ratio
WtImg	watermarked image
w(m,m)	watermark image

Greek letters

α	scaling factor
β_0	DC term of BWT
$\beta_{\theta,\phi}^{m,n,s}$	daughter wavelet of BWT
$w_{m,n,s}^{\theta,\phi}$	BWT coefficients

6. References

[1] Ramani K., Prasad E.V., Naidu V.L., and Ganesh D.,"Color Image Watermarking Bi-Orthogonal Wavelet Transform", International Journal of Computer Application, vol.11, no.9, pp. 25-29, December, 2010.

[2] Ram B., "Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Vol. 2, No.4, pp.19-27,April-2013.

[3] Lafta M.M. and Alwan I.M.," Watermarking in Image Using Slantlet Transform", Iraqi Journal of Science, Vol.52, No.2, pp. 225-230, 2011.

[4] Bailey K., Curran K.," An Evaluation of Image Based Steganography Methods", Multimedia Tools & Applications, vol. 30, no. 1,pp. 55-88,July 2006.

[5] Gutub A., Fattani M.," A Novel Arabic Text Steganography Method Using Letter Points and Extensions", WASET International Conference on Computer, Information and System Science and Engineering, Vienna Austria, May 25-27, 2005.

[6] Taiyue W., Hongwei LI.," A Novel Scrambling Digital Image Watermarking Algorithm Based on Counterlet Transform", Journal of Natural Science, vol. 19, no. 4, pp.315-322, 2014.

[7] Hien T.D., Miyara K., Nagata Y.,Nakao Z., and Chen Y.W.," Curvelet Transform Based Logo Watermarking", Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, pp 305-309, Springer 2007.

[8] Willmore B., Prenger R.J., Wu M. C-K, and Gallant J.L.,” The Berkeley Wavelet Transform: A biologically-inspired orthogonal wavelet transform”, MIT Press Journals, Neural Computation, vol. 20, no.6, pp. 1537-1564, June 2008.

[9] Ravindran R. P., Soman K.P.,” Berkeley Wavelet Transform Based Image Watermarking”, International Conference on Advances in Recent Technologies in Communication and Computing, India, pp. 357-359, 2009.

[10] Pradhan C., RathS. and Kumar Bisoi A. , ” Non Blind Digital Watermarking Technique Using DWT and Cross Chaos”, 2nd International conference on communication, computing, and security, India, Procedia Technology, Elsevier Ltd., no.6, pp. 897-904, 2012.

[11] Pan J.S., Huang H.C., and Jain L.C., ”Intelligent Watermarking Techniques”, World Scientific Publishing Co. Pte. Ltd., 2004.

العلامة المائية الرقمية بإستعمال تحويلة Arnold و تحويلة Berkeley Wavelet

ايمان محمد جعفر علوان*   ايناس مظفر جميل**

، قسم الحاسبات/ كلية التربية للبنات/ جامعة بغداد*

*البريد الألكتروني: ainms_66@yahoo.com

**البريدالألكتروني:enasm.altai@gmail.com

الخلاصة

تعرف عملية تضمين البيانات في وسط رقمي كملف الفديو، أو الملف الصوتي ، أو الصورة بالعلامة المائية الرقمية ويقدم هذا البحث خوارزمية العلامة المائية التي تعتمد على تحويلة Berkeley Wavelet. في هذه الخوارزمية المقترحة يتم اولا تشفير الصورة السرية باستعمال تحويلة Arnold لتحقيق مستوى أمان أعلى، ومن ثم تنفذ عملية الاخفاء في مجال التحويلة للصورة المضيفة. أظهرت النتائج العملية جودة هذه الخوارزمية المقترحة ومتانتها لبعض عمليات المعالجة الصورية.