Blind image watermarking scheme based on lowest energy contourlet transform coefficient and modified arnold cat/ikeda maps

Jinan N. Shehab, Hussein A. Abdulkadhim, Yousif Allbadi
Department of Communication Engineering, College of Engineering, University of Diyala, Diyala, Iraq

Article Info

ABSTRACT

The widespread of global internet has led to the need for developing new methods of protecting multimedia information from exploitation, alteration or forgery, illegal distribution, and manipulation. An attacker is quickly and illegally distributing or changing multimedia information by using various means of computer technology. For detecting this manipulation, this paper suggests blind watermark image inside a host image for observing in the receiver. If the watermark image was retrieved, then the host image was not attacked or manipulated. While if not retrieved, in this case, the image was attacked. The proposed method is depending on a decomposition of the host image using lowest energy sub-bands of contourlet transform (4-levels), with scrambling by ikeda map of the watermark image, and selecting new positions by modified arnold cat map. This will produce more security and safety, as well as provide more difficulty or prevent hacking. The obtained results confirm the robustness against attacks and more effectiveness of the presented scheme compared with the other similar works. Also, using lowest energy sub-bands will expand area of embedding and this part will be considered in the future works with the color images.

Corresponding Author:

Hussein A. Abdulkadhim
Department of Communication Engineering
University of Diyala, College of Engineering
Ba'qubah 32001, Diyala, Iraq
Email: hussein73@mail.ru

1. INTRODUCTION

Embedding information in multimedia is a popular task when it is necessary to reliably transmit, especially with the rapid development of technology. The huge amount of mutual data via internet represents an environment of risks or attacks by hackers and this leads to decrease in the security level of network [1-5]. Almost everyone can easily access to multimedia such as photos, documents, audios and videos due to the extensive use of internet facilities. This accessibility can lead to some copyright protection issues. Such images, documents, etc can be easily forgery and manipulated which consider a major threat to owners due to changing their work and reducing the owner's earnings. Consequently, the digital watermark appears to solve problems such as copyright and intellectual property protection [5-12]. Therefore, for more security and protection of copyright, authentication and safety of the watermark from detection and change, this paper proposes security method to embed a blind watermark in image. The idea of this work is to exploit unimportant areas in the host image to embed a watermark scrambled depending on contourlet transform (CT) coefficients. Moreover, using of modified arnold cat and ikeda maps will support encryption targets. The word "blind" mean that the extraction watermark process basically will be implemented without

referring to the original host image in the receiver [5, 12]. Typical host samples used in this work are images (512×512). The aim of this work is to keep the submitted image from manipulation and change by embedding a watermark using present method. If the watermark is not retrieved in the receiver, this means that the image has been hacked and manipulated with its contents. Of course, when the embedded watermark is retrieved, this mean that no change in the host or saved images. By other words, the aim is to detect via watermark observation if the host image is hacked or not. Basically, the frequency domain will provide more capacity with minimum deformation, in addition, using of contourlet transform to decompose the host image and select lowest energy sub-band will expand area of embedding [12]. Moreover, this will reduce distortion because of information and details of the host image usually stored in the high energy sub-band. Ikeda and modify cat maps are improving security and robustness of the proposed method and playing an important role as shown in other section later.

Researchers presents different basic terminology submitted to some improvements and modifications over time as well as algorithms and methods to enhance security using watermarking. Despite of the many and different methods exist which have high complexity in some cases, all of them have the main goal of protecting property from exploitation, hacking or forgery. For example, a robust and transparent watermarking scheme using contourlet transform with quantization index modulation is proposed in [13]. The coefficients are divided into 3-quadrants using symmetric property of the contourlet transform. The angle of coefficients is modulated for each of three points. As a result, more effective imperceptibility with higher robustness in the proposed scheme are achieved according to quantization index modulation properties. A technique of semi-blind gray image watermarking by redundant wavelet domain proposed in [14]. The focus of this work primarily is to highlight on the redundant wavelet transforms usefulness in the image watermarking. The authors applied the nonsubsampled contourlet transform to provides rich directional information and redundant discrete wavelet transform (RDWT) as a shift invariant. Thus, the shortcomings overcome of DWT is achieved with more useful in image watermarking. The authors in [15] for medical imaging are propose a CT and discrete cosine transform (DCT) based on multiple robust watermarking algorithms. The proposed scheme uses CT to extract multi-directional and multi-scale texture information. The DCT was used to get the feature vector in the low-frequency directional sub-bands. The authors of [16] are proposes an adaptive quantization contourlet domain blind digital watermarking algorithm. This algorithm combines the decomposition of singular value to embed the watermark in the low-frequency sub-band of CT by mean-adaptive quantization. While in the [17], a new image watermarking method based on visual saliency and CT is proposed. In this algorithm, the detection function of salient object and CT are separately operated on the host image. After splitting the low-pass transformed sub-band into nonoverlapping blocks, the saliency values and energy distribution of the block determine the quantization step-size for each block together. According to [12], an optimized blind image watermarking approach based on principal component analysis (PCA) in redundant discrete wavelet (R-DW) domain is proposed. PCA-R-DW scheme was tested by several attacks to show the robustness. Furthermore, an improved grey-wolf optimizer (IGWO) algorithm which has emerged as an efficient metaheuristic optimization technique is utilized to optimize the performance of PCA-R-DW blind watermarking (BW) approach. In another works, for example, the authors in [18] are proposes an image watermarking algorithm with high-level security and robustness by using matrix decomposition and Gyrator transform. This algorithm is properly developed in the invariant integer-Wavelet domain. But in [19], two modules suggested for embedding and extracting a watermark. In embedding procedure, the secret image bit is inserted into an original image. Similarly, in extracting procedure, the inserted bit is extracted from the watermarked image without losing any information. Here, sanitization approach was applied on the secret image to acquire the secret bit. In the present work, the difference with the previous works is employing of Contourlet decomposition technique with ikeda and modified arnold cat maps. This will produce more security and safety, as well as provide more difficulty or detect hacking.

2. PRELIMINARIES

Digital watermarking technique is used for embedding symbol such as letter or text…etc. in different types of multimedia data for various purposes. Moreover, a watermark, in general, defined as some small and special data embedded in a media signal without affecting its functionality [9-12, 20]. Components of the digital watermarking model are the formation with encryption method and their implementation in the multimedia with retrieval ability after transmission over networks [10, 11]. Therefore, in this section, components of the proposed method will explain briefly to know the role of each of them. These components are: (Contourlet Transform, Ikeda Map, Modefied Arnold CAT map). Understanding the work mechanism between these components will give a clear idea about the goal of method.

2.1. The contourlet tansform

A new expansion of wavelet transform is called contourlet transform (CT) and proposed by Do and Vetterli [21] in 2002. CT, which also called pyramidal directional filter bank (PDFB), is an image representation method with multi-resolution and directional properties. This method has been used to represent two-dimensional signals which can truly capture geometric structure [21]. The term "Laplacian Pyramid (LP)" is used for multi-scale image decomposition to capture point singularly. Singular points which are distributed in the same direction are yielded to synthesize into a coefficient by directional filter bank (DFB) to capture high frequency components. From original image, LP can produce a low pass sampling approximation image and, as a result, produce a difference image between them. Moreover, to produce directional sub-band image with the number of a multiple of two on any scale, Directional Filter Bank is applied in laplacian pyramid decomposed different image. In this case, to avoid "leaking" of low frequency component, DFB itself is not suitable for processing the low frequency part of image. Therefore, combination of DFB and LP will be bound to realize the image reconstruction with the perfect characteristics [22, 23]. However, Figure 1 show the illustration of contourlet transform.
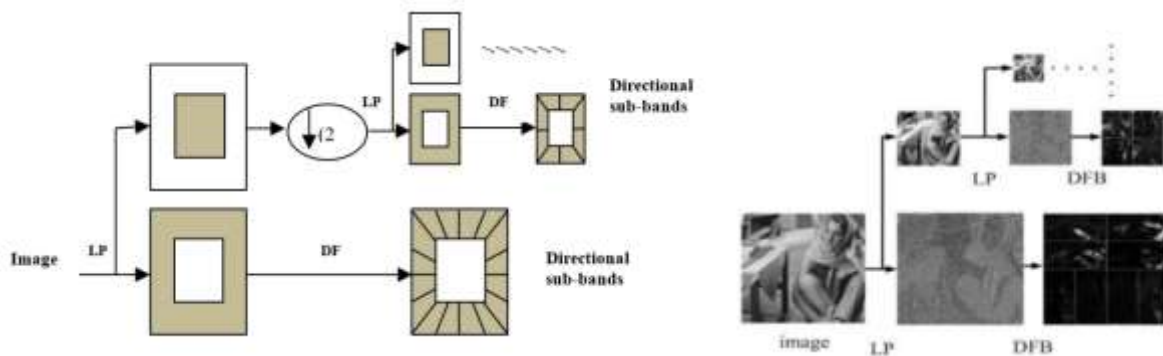
Figure 1. An illustration of contourlet transform

Clearly note from Figure 1. a sequence of image is obtained by repeating the steps several times. In case of these images are stacked one above other, a tapering pyramid data structure will produce as shown in Figure 2 and called Laplacian pyramid. To achieve perfect image reconstruction, two-dimension DFB can be maximally decimated and efficiently implemented via a L-level tree-structured decomposition. This leads to 3-levels sub-bands with wedge-shaped frequency partition as shown in Figure 3 [12, 16].
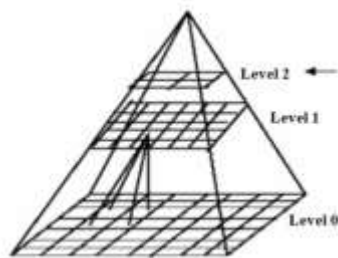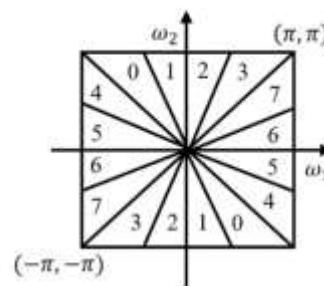

Figure 2. Laplacian pyramid

Figure 3. DFB frequency partitioning with 3-levels and 8 reals wedge-shaped frequency bands

2.2. Ikeda map

Kensuke Ikeda [24] work on the complex map, which is called "Ikeda map", in 1987. This map, described in [24], show that under the suitable conditions, dynamics of the transmitted light inside a specific cavity can be expressed by a set of difference-differential equations. These equations do not involve the spatial coordinate [24] and expressed as:

$$x_{n+1} = 1 + u(x_n \cos t_n - y_n \sin t_n))$$
$$y_{n+1} = u(x_n \sin t_n + y_n \cos t_n)$$

(1)

$$t_n = 0 \cdot 4 - \frac{6}{1+x_n^2+y_n^2}$$

where $u \geq 0 \cdot 6$, $n = 0,1,2 \dots$, $x_0 = 0.1$ and $y_0 = 0.1$.

2.3. Modified arnold cat map

Russian mathematician Vladimir I. Arnold [25] is discovering the particular instance of chaos map and named arnold cat map (ACM) by using an image of a cat. This map is a simple demonstration and elegant illustration of some chaos principles underlying order of an apparently random evolution of a system. In general, any image is performed with a transformation which apparently randomizes the original pixels organization; and new image reappear when this operation iterated enough times [25, 26]. Let us an image represented as a matrix X and can examine selected entries in X (ACM) is a clipping transform and used in the embedding process to improve the image hiding safety and visual quality of the extracted message (secret message). A shuffling operation is done on this process of the original message via successive mixing of the initial information which is "spread" all over the available state space. Due to discrete nature of the image and ACM with the same dimensions, ACM is used to shuffle the hidden message overall proper sub-band of the cover image. As a result, the initial message will be exponentially hard to recover if the secret key or transformation not available. However, the mathematical formula of ACM is [25, 26]:

$$\begin{pmatrix} \hat{x} \\ \hat{y} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N$$

(2)

The original 2D Arnold transformations can be modified to produce a sequence of Arnold transformations by setting new coefficients (a1, b1, c1) to increase and ensure high security implementation [25, 26]. Assume an image with $N \times N$, then Arnold cat map is given as follows:

$$\begin{pmatrix} \hat{x} \\ \hat{y} \end{pmatrix} = \begin{bmatrix} 1 & b+c^2 \\ a & 1+ab+ac^2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N$$

(3)

Where a1, b1 and c1 are positive control coefficients $\epsilon\ R$, $(\hat{x}, \hat{y})$ are the shuffled pixel coordinates [26].

3. THE PROPOSED PROCEDURES

This section presents main procedures: embedding and reconstructing a watermark image. In the embedding procedure, there are two threads simultaneously are performed as shown in Figure 4. The first thread includes scrambling process for the watermark image selected using a key provided by Ikeda map (eq. (1)) to produce a new watermark image scrambled. In this case, as a rule, x_{n+1} to scramble rows and y_{n+1} to scramble columns of the watermark image. The produced image will convert to a vector (SW) with one dimension. To reduce the watermark effect on the host image contents, the vector SW will multiply by a float coefficient $\alpha : 0.1 \leq \alpha < 1$, thus $SW' = SW \times \alpha$. The second thread includes analyzing the host gray image into many levels using Contourlet Transform. As a rule, selecting number of levels is relating with the size of image in order not to distort the image details. However, this host image will be selected with low details and edges to allow replacing the values from watermark image without effecting on the original host image. In this case, CT decomposition process will apply on the gray image and then calculate energy levels of the directional sub-bands. In this work, the idea of using CT is to select of lowest energy which contains low significant information and details. This area will used for the watermark image embedding, and consequently, does not cause a distortion or deformation as well as obtain high value of PSNR. Decompose the host image (512×512) with 4-levels will produce: $32 \times 32 + (2 \times 32 \times 64) + (4 \times 64 \times 64) + (8 \times 64 \times 128) + (16 \times 64 \times 256) = 349,184$ coefficients as show in Figure 5. To calculate energy of the Contourlet coefficients $s(i.j)$, the following expression is used [16]:

$$E = \sum_{i=1}^{N} \sum_{j=1}^{M} |s(i.j)^2|$$

Where $s(i.j)$ - value of the contourlet coefficient. Consequently, the suitable sub-band energy value, as a result, for example will be around 0.2348 and if full then select another sub-band about 0.5263 and so on. According to the watermark image size (see Figure 5.). Results of the two threads will be ready to set to the next stage of embedding operation: Modified CAT map stage. This stage starts from generating CAT map

and creating new coordinates $(\hat{x}, \hat{y})$ for replacing the coefficients values of directional lowest energy area in the host gray image by the values of SW'. This mean, shuffling pixels of SW' in the host image completely and the new locations submitted to CAT map. At the end, by using inverse contourlet transform (ICT), reconstruct watermarked image, then to transmitter.

In the receiver, the reconstruction procedure is following to the inverse of embedding procedure in the sender. To extract the watermark image, the receiver does not need the host image because the system is blind. The values (a1, b1, c1) of modified CAT map, the secret key (x_{n+1}, y_{n+1}, u) from Ikeda map and values of (α) must be available to complete the reconstruction process as following steps: Firstly, decomposing the received image (watermarked image) to 4-levels using contourlet transform and going to the sub-band region. After this step, determining the lowest energy sub-bands and detecting the correct locations of the watermark image using coefficients (a1, b1, c1) of modified cat map. Then, the result of the present step is SW' values which will store in the temporary buffer and the watermark image will reconstructed by Inverse Contourlet transform. Of course, these data will divide by (α) to retrieve the real pixels values. Finally, the original watermark image completely retrieved using x_0, y_0 of the Ikeda map. Observation of the watermark image status will explain if the host image hacked or not? Hence, this situation will explain in the next section.
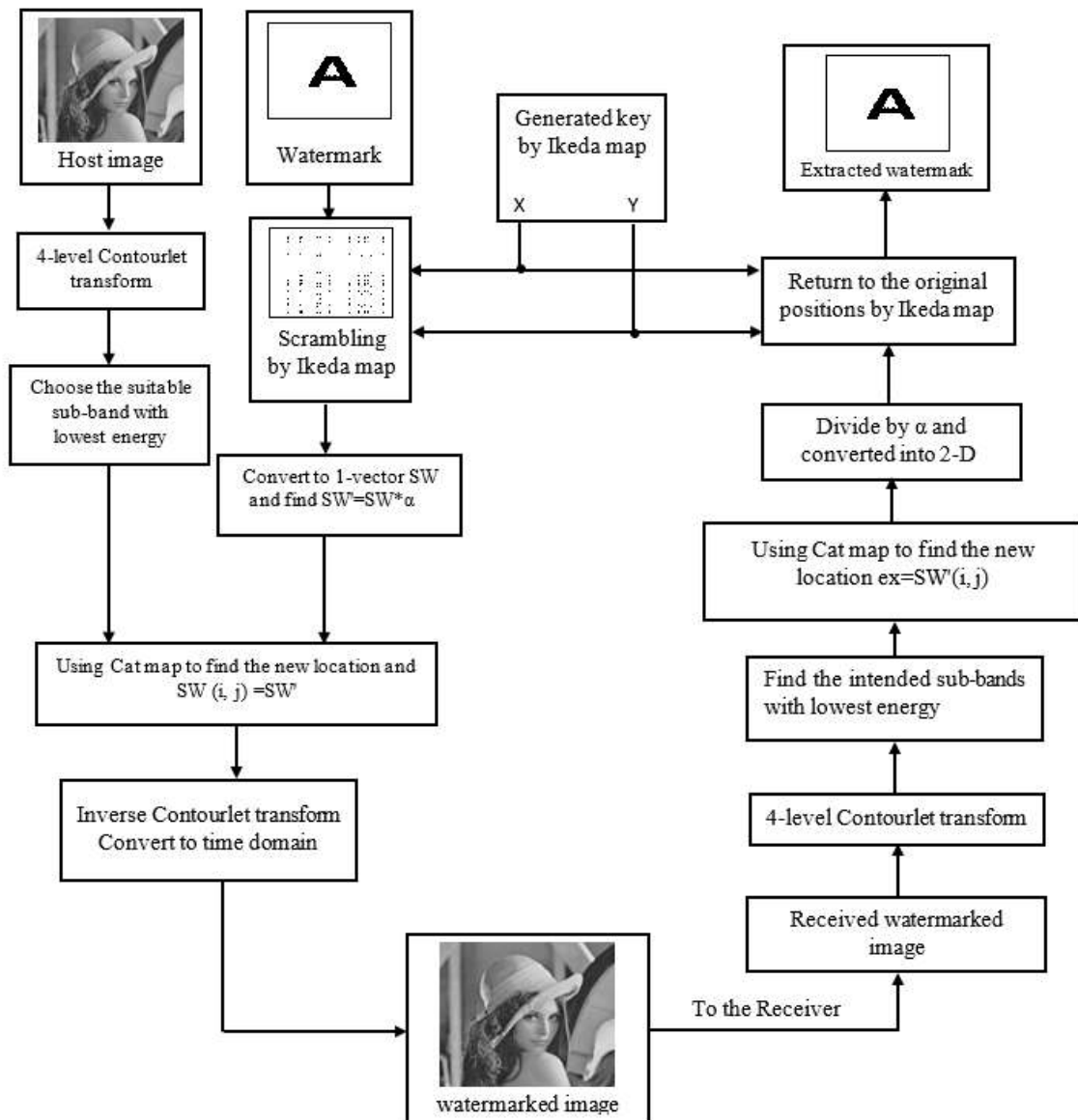
Figure 4. The schematic configuration of the proposed watermarking system
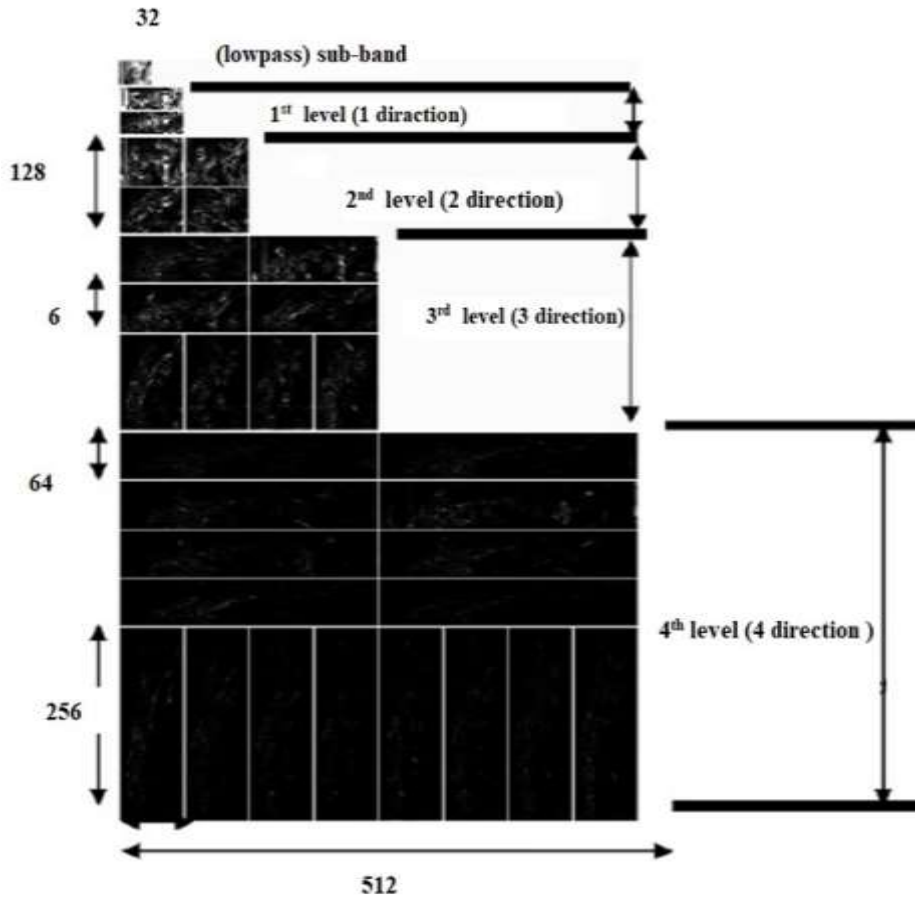
Figure 5. 4-level contourlet decomposition

4.   RESULTS AND DISCUSSION

This section includes brief test and analysis of the proposed method using different host images (512×512) and watermark image (256×256). To show accuracy and hardiness of this method, obtained results will be compared with the other results of various recent works. In fact, two main categories for testing:

4.1. Estimating image quality

Estimating image quality is a vital part at any application; therefore, this method utilizes some of quality metrics to prove stability and efficiency over the blind watermarking applications. For this situation, the quality metrices which utilized here are: peak signal-to-noise ratio (PSNR), mean square error (MSE), normalized correlation coefficient (NCC) and structural similarity index (SSIM) [2, 4, 12, 16]. These well-known scales for estimating image quality. However, the mathematical expressions of PSNR value in dB and MSE value are:

$$PSNR = 10 \, log_{10} \frac{255^2}{MSE} \; , \tag{4}$$

$$MSE = \frac{1}{M \times N} \sum_{a=0}^{M-1} \sum_{b=0}^{N-1} [h(a,b) - w(a,b)]^2$$

Where M and N - represents the number of rows and columns of image; $h(a,b)$ – array refer to the host image in pixel; $w(a,b)$ – array refer to the watermarked image in pixel. The following algorithm is used for estimating Normalized Correlation Coefficient [16]:

$$NCC = \sum_{a=0}^{M-1} \sum_{b=0}^{N-1} \frac{h(a,b)*w(a,b)}{h(a,b)^2 * w(a,b)^2}$$

and the SSIM index is calculated as [12,16]:

$$SSIM = \frac{(2\mu_a\mu_b+c_1)(2\sigma_{ab}+c_2)}{(\mu_a^2+\mu_b^2+c_1)(\sigma_a^2+\sigma_b^2+c_2)} \ ,$$

Where μ_a and μ_b are the mean of a and b; σ_a^2 and σ_b^2 are the variances of a and b ; σ_{ab} is the covariance between a and b; $c_1, c_2 -$ are the couple of variables to steady the division with thin denominator. In case of no attack and by using various host gray images for the blind watermarking, the results obtained by estimating PSNR, MSE, SSIM and NCC are shown in Table 1.

Analysis of obtained results shows slight differences between original & extracted watermark images and between original & watermarked images in the receiver. These differences may be affected by details which available in the host image. if the host image has low details, then the capacity of hiding will increase and NCC =1.

Table 1. Results of the quality matrices through embedding and reconstruction operations

Experimental images				Quality matrices values between original and extracted watermark images			Quality matrices values between the host and watermarked images			
Host Image	Watermark image	Watermarked image	Extracted watermark	PSNR	NCC	SSIM	PSNR	MSE	NCC	SSIM
	A		A	54.9329	1	0.9903	46.9331	0.000061	1	0.9896
	A		A	55.0560	1	0.9911	44.008	0.0171	0.9995	0.9768
	A		A	54.8726	1	0.9908	42.4191	0.0001258	1	0.9608
	A		A	54.8926	1	0.9914	47.2563	0.0001692	0.9998	0.9782
	A		A	54.6776	1	0.9907	47.2447	0.0002403	1	0.9766

4.2. Robustness experiment

For the purpose of testing the system robustness, some attacks are carried out on the watermarked image. Under these conditions, watermark image will be extracted, objectively observed and evaluated. JPEG compression: Images are usually transmitted via internet channel as JPEG compression which can be controlled by the quality factor (QF) [17, 27]. By selecting different quality factors and samples of watermarked image, this attack test is performed. The results in Table 2 show that NCC value obtained for the watermark image extracted is unity when the quality factor approaches up to 15. In this case, the watermark image may be completely retrieved from the watermarked image.

Table 2. NCC values obtained for the blind watermark image extracted under JPEG compression attacks

QF of JPEG compression	Baboon	Barbara	Boat	Peppers
QF=5	0.9916	0.9856	0.9848	0.9842
QF=15	1	1	1	1
QF=25	1	1	1	1

4.2.1. Noise attack

This is employed with uniform scale for simulating the random interference when the watermarked image transmits through channel [27]. Firstly, the watermarked image is normalized, then Gaussian noise, Salt & Pepper noise and Speckle noise with different intensities are applied respectively. Quality of the extracted watermark image will be reduced obviously when the noise intensity increasing, However, Table 3 show the NCC values which are greater than 0.95 with better resistance to these types of attacks.

Table 3. NCC values of the watermark image extracted under gaussian noise attacks

Type of attack	Baboon	Barbara	Boat	Peppers
Gaussian noise (intensity = 0.001)	1	0.9998	0.9997	1
Gaussian noise (intensity = 0.05)	0.9883	0.9890	0.9705	0.9686
Gaussian noise (intensity = 0.1)	0.9592	0.9589	0.9553	0.9585
Salt & pepper noise (intensity = 0.005)	0.9975	0.9977	0.9975	0.9974
Salt & pepper noise (intensity = 0.01)	0.9824	0.9827	0.9825	0.9826
Speckle noise (intensity = 0.005)	0.9722	0.9789	0.9726	0.9741

4.2.2. Filtering attacks

Table 4 contains results of use the gaussian, median, and mean filters with (3×3). NCC values obtained show that the watermark image is retrieved with slight error.

Table 4. NCC values of the watermark image extracted under filter attacks

Type of attack	Baboon	Barbara	Boat	Peppers
Gaussian filter (3×3)	1	1	1	1
Median filter (3×3)	0.9776	0.9789	0.9781	0.9786
Mean filter (3×3)	0.9956	00.9987	0.9986	0.9991

4.2.3. Geometric attack

Scaling, various types of cropping and angles of rotation attacks are applied in this test. Table 5 contains results which prove that the algorithm can resist these attacks, especially scaling and cropping.

Table 5. NCC values of watermark image extracted under geometric attacks

Geometric attack	Baboon	Barbara	Boat	Peppers
Rotation (-30)	0.6372	0.6929	0.6396	0.6459
Scaling (factor 2)	0.9868	0.9898	0.9912	0.9888
Cropping	0.8154	0.8564	0.8762	0.8812
Motion Blur	0.9761	0.9793	0.9770	0.9791

Visually, to see the effect of attacks with standard conditions on the host, watermarked and watermark images, "Lena.jpg" used as a typical example as a host image with PSNR and NCC values (see Table 6). From the table, the watermark image was extracted clearly in the receiver although the attack conditions, in particular, rotation and cropping. In case of manipulation on the watermarked image, the watermark image will not retrieve.

In order to demonstrate the robustness and improvement, in this section, the obtained results are compared with the results of [16, 19, 27]. The watermark images which used in [19] have the size of (256×256) as in the present work, while in [16,27] have the size of (32×32). From the Table 7 which contains details of comparison, the blind watermarking gets about 10 dB optimization and the values of PSNR, MSE, NCC and SSIM are got better than the values obtained from the references [16, 19, 27]. However, these improvements will support significantly the presents work.

Furthermore, another comparison to prove robustness will be performed with the results of the references [16, 27, 28, 29] by observing NCC. Tables 8 and 9 show the differences between obtained results from the references and the present results of the proposed method under attack conditions. The tables prove that the proposed blind watermarking methodology had superior values over other methodologies.

Table 6. NCC values of watermark images extracted after filter attack

Type of attack	Host image	Watermarked image	PSNR (dB)	Watermark image	Extracted watermark	NCC
JPEG compression (QF = 10)			45.6165			1
Gaussian noise (intensity = 0.05)			36.0551			0.9735
Salt & pepper noise (intensity = 0.01)			44.2367			0.9825
Speckle Noise (intensity = 0.005)			39.4798			0.9720
Gaussian filter (3 × 3)			44.2403			1
Median filter (3 × 3)			40.7819			0.9787
Mean filter (3 × 3)			38.0659			0.9932
Rotation (10°)			26.7190			0.9797
Scaling (factor 2)			53.6910			0.9878
Motion Blur			34.4201			0.9789
Cropping			27.4545			0.7921

Table 7. Values of the quality metrices between the proposed method and references [16, 19, 27]

Host image (512x512) without noise	Quality matrices of reference [19]: watermark image (256x256)			Quality matrices of reference [27]: watermark image (32x32)		Quality matrices of reference [16]: watermark image (32x32)		Quality matrices of the present work: watermark image (256x256)			
	PSNR	MSE	NCC	PSNR	NCC	PSNR	NCC	PSNR	MSE	NCC	SSIM
Baboon	35.50857078	0.009955556	0.988420565	-	-	-	-	46.9331	0.000061	1	0.9896
Barbara	38.81102235	0.021333333	0.97621226	44.3189	1	40.7159	1	44.008	0.0171	0.9995	0.9768
Boat	38.48068826	0.0176	0.990485031	-	-	-	-	42.4191	0.0001258	1	0.9608
Lena	40.37547528	0.013688889	0.988191711	45.6123	1	41.3913	1	47.2563	0.0001692	0.9998	0.9782
Pappers	39.22766092	0.01991111	0.983410138	46.4041	1	41.4851	1	47.2447	0.0002403	1	0.9766

Table 8. NCC values between the proposed method and the references [16, 28, 29]

Type of attack	NCC of reference [28]	NCC of reference [29]	NCC of reference [16]	NCC of the present work
JPEG compression (20)	0.8126	0.9712	0.9961	1
Gaussian noise (0.001)	0.8996	0.9762	1	1
Salt and pepper noise (0.005)	0.9712	0.9836	0.9974	0.9974
Gaussian filtering (3×3)	0.9236	0.9587	1	1
Median filtering (3×3)	0.9312	0.9612	0.9961	0.9787
Mean filtering (3×3)	0.9324	0.9592	1	0.9932
Zoom (0.5)	0.9985	0.9826	1	1
Upper left corner cut 1/4	0.9183	0.7952	0.9900	0.9998
Rotation (10°)	0.6531	0.7512	0.9267	0.9797

Table 9. NCC values between the proposed method and the reference [27]

Type of attack	Baboon in [27]	Present work
Gaussian noise (0.1%)	0.9695	1
Gaussian noise (0.3%)	0.8506	0.9898
Gaussian noise (0.5%)	0.7871	0.9883
Salt & Pepper noise (0.5%)	0.9235	0.9975
Salt & Pepper noise (1%)	0.8505	0.9825
Salt & Pepper noise (2%)	0.7875	0.9791
Speckle noise (0.5%)	0.9284	0.9720
Speckle noise (1%)	0.8341	0.9090
Speckle noise (2%)	0.7396	0.8556

5. CONCLUSIONS

This paper present methodology for detecting manipulation on gray images sent via internet channel to protect copyright and intellectual properties from attackers by embedding a blind image watermark. This methodology will provide more improvements in robustness, security and safety for these images. Employing Ikeda map for scrambling watermark image and contourlet transform decomposition (4-levels) to select lowest energy sub-band for embedding watermark image will support security. Moreover, using modified Arnold Cat map to select new positions of the scrambled pixels in CT coefficient will, in particular, produce more safety and sensitivity to detect hacking. Various quality matrices show more improvement about 10% in imperceptibility and 2% in robustness compared with the values of other works. These reliable results are obtained by merge operations of maps with CT coefficients to achieve the purpose of this work. Employ present maps with redundancy wavelet coefficients and color images for more protection are our future works.

REFERENCES

[1] Prajanto Wahyu Adi, Yani Parti Astuti, Egia Rosi Subhiyakto, "Imperceptible Image Watermarking based on Chinese Remainder Theorem over the Edges", *Proc. EECSI 2017, Yogyakarta, Indonesi*a, 2017.

[2] Jinan N. Shehab, Hussein A. Abdulkadhim, "Image Steganography Based on Least Significant Bit (LSB) and 4-Dimensional Lu and Liu Chaotic System," *2018 IEEE, International Conference on Advanced Science and Engineering (ICOASE), Kurdistan Region, Iraq*, 2018.

[3] Anton Yudhana, Sunardi, Shoffan Saifullah, "Segmentation Comparing Eggs Watermarking Image and Original Image", *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 47-53, 2017.

[4] Hussein A. Abdulkadhim, Jinan N. Shehab, Ali N. Albu-rghaif, "Audio Security Based on LSB Steganography and 4-D Lü System," *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, 2018.

[5] Milad Yousefi Valandar, Milad Jafari Barani, Peyman Ayubi, "A blind and robust color images watermarking method based on block transform and secured bymodified 3-dimensional Hénon map," *Springer-Verlag GmbH Germany, part of Springer Nature*, 2019.

[6] Pan-pan Niu, Li Wang, Xin Shen, Si-yu Zhang, Xiang-yang Wang, "A novel robust image watermarking in quaternion wavelet domain based on superpixel segmentation," *Multidimensional Systems and Signal Processing*, 2020.

[7] Media Anugerah Ayu, Teddy Mantoro, I Made Alan Priyatna, "Advanced watermarking technique to improve medical images' security," *TELKOMNIKA*, vol. 17, no. 5, pp. 2684-2696, 2019.

[8] Yu-Guang Yang, Lu Zou, Yi-Hua Zhou, Wei-Min Shi, "Visually meaningful encryption for color images by using Qi hyper-chaotic system and singular value decomposition in YCbCr color space", *Optik*, 2020.

[9] Zihan Yuan, Decheng Liu, Xueting Zhang, Qingtang Su, "New image blind watermarking method based on two-dimensional Discrete Cosine Transform", *Optik*, 2019.

[10] Ling-Yuan Hsua and Hwai-Tsu Hu, "Blind watermarking for color images using EMMQ based on QDFT," *Expert Systems with Applications*. 2020.

[11] Anoop Kumar Chaturvedi & Piyush Kumar Shukla, "Effective watermarking technique using optimal discrete wavelet transform and sanitization technique," *Multimedia Tools and Applications*, 2020.

[12] D. Rajani, P. Rajesh Kumar, "An Optimized Blind Watermarking Scheme Based on Principal Component Analysis in Redundant Discrete Wavelet Domain," *Signal Processing, Elsevier B.V.*, 2020.

[13] Abdulmawla Najih, S.A.R. Al-Haddad, Abd Rahman Ramli, S.J. Hashim, Mohammad Ali Nematollahi, "Digital image watermarking based on angle quantization in discrete contourlet transform," *Journal of King Saud University–Computer and Information Sciences*, 2016.

[14] Siddharth Singh1, Vivek Singh Rathore, Rajiv Singh and Manoj Kumar Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain," *Springer Science+Business Media, New York*, 2017.

[15] Xiaoqi Wu, Jingbing Li1, Rong Tu, Jieren Cheng, Uzair Aslam Bhatti and Jixin Ma, "Contourlet-DCT based multiple robust watermarkings for medical images," *Springer Science+Business Media, LLC, part of Springer Nature, Multimedia Tools and Applications*, 2018.

[16] Di Fan, Ying Wang, Chunwei Zhu1, "A blind watermarking algorithm based on adaptive quantization in Contourlet domain," *Springer Science+Business Media, LLC, part of Springer Nature, Multimedia Tools and Applications*, 2019.

[17] Yifeng Zhanga, Yibo Suna, "An image watermarking method based on visual saliency and contourlet transform," *Optik - International Journal for Light and Electron Optics*, 2019.

[18] Lina Zhang, "Image Watermarking Based on Matrix Decomposition and Gyrator Transform in Invariant Integer Wavelet Domain," *Signal Processing, Elsevier B.V.*, 2019.

[19] Anoop Kumar Chaturvedi, Piyush Kumar Shukla, "Effective watermarking technique using optimal discrete wavelet transform and sanitization technique," *Springer Science+Business Media, LLC, part of Springer Nature*, 2020.

[20] Ferda Ernawan, Dhani Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 2185-2195, 2019.

[21] Minh N. Do, Martin Vetterli, "Contourlets: A Directional Multiresolution Image Representation," *International Conference on Image Processing*, 2002.

[22] Minh N. Do, and Martin Vetterli, "The Contourlet Transform: An Efficient Directional Multiresolution Image Representation", *IEEE transactions on image processing*, 2005.

[23] Taiyue Wanga and Xinxiang Zhang, "A novel anti-geometrical attack digital watermark algorithm based on Contourlet transform and human visual system," *Journal of Computational Methods in Sciences and Engineering*, vol. 18, pp. 269–281, 2018.

[24] V. Aboites, D. Liceaga, A. Kir'yanov and M. Wilson, "Ikeda Map and Phase Conjugated Ring Resonator Chaotic Dynamics," *International Journal of Applied Mathematics & Information Sciences*, 2016.

[25] Ahmed M. Elshamy, Fathi E. Abd El-Samie, Osama S. Faragallah and others, "Optical image cryptosystem using double random phase encoding and Arnold's Cat map," *Springer Science+Business Media, New York*, 2016.

[26] Yue Wu, Zhongyun Hua, and Yicong Zhou, "n-Dimensional Discrete Cat Map Generation Using Laplace Expansions," *IEEE transactions on cybernetics*, vol. 46, no. 11, 2016.

[27] An-Wei Luo, Li-Hua Gong, Nan-Run Zhou, Wei-Ping Zou, "Adaptive and blind watermarking scheme based on optimal SVD blocks selection," *Springer Science+Business Media, LLC, part of Springer Nature*, 2019.

[28] Bi H, Li X, Zhang Y et al, "A blind robust watermarking scheme based on CT and SVD," *IEEE, international conference on signal processing, IEEE*, pp. 881-884, 2010.

[29] Hosseini SA, Ghofrani S, "Digital Watermarking based on Contourlet-SVD," *Majlesi. J Electr Eng*, pp. 63-68, 2014.

BIOGRAPHIES OF AUTHORS

Jinan N. Shehab is a faculty member in the department of communication engineering\college of the engineering\University of Diyala-Iraq. She received her bachelor's degree in the field of electronic engineering from the University of Diyala/Iraq in 2005 and the master's degree at the field of electronic and communications from the department of electrical engineering/University of Al-Mustanseriya-Iraq in 2014. Her research interests include image processing, digital watermarking and steganography

Hussein A. Abdulkadhim received the B.Sc. and M.Sc. degrees in Electrical and Electronic Eng./Communication Engineering; certified by AL-Rasheed College/University of Technology-Baghdad, Iraq, 1999 and 2004 respectively. He received Ph.D. Degree in Communication Engineering- certified by Ulyanovsk State Technical University/Ulyanovsk /Russian Federation, 2017. He is a faculty member in the department of communication engineering/College of Engineering\University of Diyala. His interested scientific fields mainly focus on Navigation Systems, Image processing and obiect detection

Yousif Allbadi received M.Sc. degree in Telecommunications Engineering from Warsaw University of Technology-Poland in 2017. He is Assistant Manager and a faculty member in the department of communication engineering/College of Engineering/University of Diyala. His interested scientific fields mainly focus on Robotics, Image processing and Automation.