A Novel Robust Blind Digital Watermarking Scheme Based on Blocking Probability

Md. Abul Kayum Hawlader, Md. Moniruzzaman and Md. Foisal Hossain
Department of Electronics and Communication Engineering
Khulna University of Engineering and Technology, (KUET)
Khulna, Bangladesh
kayumkuet09@gmail.com, mdzamankuet@gmail.com and foisalkuet@yahoo.com

***Abstract*— Now a days, image watermarking is becoming a very important issue for image authentication and copyright protection due to explosive growth of multimedia applications. In this paper, an innovative robust digital watermarking scheme is proposed for image authentication and copyright protection which is based on the probability of existing total number of one's and zero's in a single block. The proposed scheme uses scrambled binary watermark to embed four times into different locations of host image in order to ensure high security and to be robust. The extraction of watermark is done by comparing between total amount of detecting 'one' and 'zero' bit from each block of size eight by eight. The experimental results show that the proposed method provides perceptually invisible watermark, high security and robustness against various image processing and geometrical attacks such as filtering, cropping as well as salt and pepper noise attacks.**

Keywords- watermarking; watermark; robustness; logistic map

I. INTRODUCTION

Watermarking is the technique of embedding information called watermark into the digital content in order to establish security. Watermark contains useful information for ownership authentication or copyright protection such as company logo, company name and product's name etc. With the development of digital technologies, digital data or information can be easily altered or destroyed. As a result, there is the need for authentication techniques to secure digital images.

Digital image watermarking techniques are classified into two categories. They are digital visible watermarking and digital invisible watermarking. Furthermore, digital invisible watermarking techniques are divided into fragile watermarking and robust watermarking. Fragile watermarking techniques are designed to detect slight changes of watermarked image. On the other hand, robust watermarking techniques are designed to resist all kinds of attacks such as filtering, cropping, rotating, scaling, resizing and image compression. In other words, the robust watermarking techniques ensure high robustness for watermark which means that the watermark is difficult for an attacker to remove or destroy the certifiable information.

Digital watermarking algorithms are also categorized by spatial domain techniques and frequency domain techniques based on working domain. In spatial domain techniques [1], [2], [3], [4], the watermark is embedded by directly modifying the intensities of some selected pixels of the host image. Least significant bit (LSB) is the simplest and most commonly used technique in the spatial domain techniques. In [1], a secret message is embedded by modifying the LSB of each pixel of the host image. The methods [5], [6], are quit robust against filtering, scaling, rotation but they are less robust against cropping attack because the watermark is embedded into the whole image. In [7], the watermark is embedded by dividing the original image into different block size. In [7], [8], [9], initially the host image is converted into a set of frequency domain coefficients by using discrete Fourier transforms (DFT), discrete wavelet transforms (DWT), discrete cosine transforms (DCT) etc. Then the watermark is embedded in the transformed coefficients of the host image to make an invisible watermark. Finally, the watermarked image is obtained by applying inverse transformations of the coefficients. In [8], the watermark is embedded three times in different frequency bands that are low, medium and high. As a result the watermark can not be totally destroyed by either low pass, medium or high pass filter. In [9], the watermark is embedded into the DCT coefficients of subsampling part of original image. In [10], a detail analysis on wavelet based watermarking techniques can be found.

This paper proposed a new blind spatial domain digital watermarking scheme for gray scale images. The original host image is divided into a number of non-overlapping blocks. The watermark is binary logo image which is scrambled by using logistic map in order to provide high security. Then the scrambled watermark is embedded four different positions into the host image. The extraction of watermark is performed by making decision on the presence of total binary bits '1' and '0' in a single block. The main attraction of the proposed scheme is that the scheme is more secured and highly robust against cropping, filtering as well as salt and pepper noise attack. This scheme also provides high level of signal to noise ratio (SNR) and minimum number of bit error rate (BER).

The rest of the paper is designed as follows: Section II gives an overview of logistic map. The details of watermark generation, watermark embedding and watermark extraction schemes are explained in section III. Section IV provides experimental results and comparison with other methods. And finally, some conclusions are drawn in section V.

II. LOGISTIC MAP

The proposed scheme used Logistic map to generate a chaotic sequence for increasing the security which is very sensitive to its initial conditions. All the orbits of logistic map are dense by the value of range [0,1]. The two chaotic sequences generated by logistic map with different initial conditions are statistically uncorrelated with each other. 1-dimensional logistic map is one of the simplest chaotic maps which is described by

$$x(n+1)=\mu \times x(n) \times (1-x(n)), \quad n=1,2,\ldots \qquad (1)$$

Where μ is a constant of value $0<\mu\leq 4$ and x(1) is the initial value.

III. PROPOSED METHOD

The proposed scheme used a binary logo image as the original watermark W of size m×n. The original watermark is scrambled by performing bit wise exclusive OR operation between the original watermark bits and random bits or a chaotic binary sequence in order to make a strong watermark. This chaotic binary sequence is generated by using logistic map and then the output sequence is modified by reshaping into original watermark size. Finally, the elements of chaotic sequence is scaled and rounded into the range [0, 1]. "Fig.1(a)" shows the original watermark and "Fig.1(b)" shows the corresponding scrambled watermark.

The proposed watermark embedding scheme is shown in "Fig.3". The watermark is embedded four times in different locations into the original host image of size M×N, where M>m and N>n as shown in "Fig.2" in order to be robust against cropping attack. The original host image is divided into a non-overlapping blocks of size p×q, where p<m and q<n. Each encoded bit of scrambled watermark image is embedded into a single block, therefore one watermark of size m×n is required (m×n) blocks.

"Fig.4" shows the proposed watermark extraction scheme which does not depend on the original host image and the original watermark, therefore it is a blind watermarking scheme. The proposed watermark extraction is based on the presence of total binary bits '1' and '0' in each single block of size p×q.

A. Watermark Generation

In the proposed scheme, the scrambling process of the original watermark W includes the following steps:

1. Consider a binary watermark W of size m×n.

2. Apply 1-dimensional logistic map to generate a chaotic sequence.

3. Reshape the generated chaotic sequence into size of m×n.

4. Scale and rounde the reshaped chaotic sequence into range [0,1]. The result is denoted by K, which is secret key.

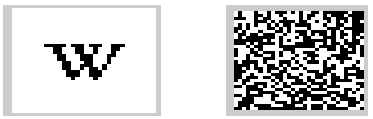

Fig.1 (a) Original watermark, (b) Scrambled watermark

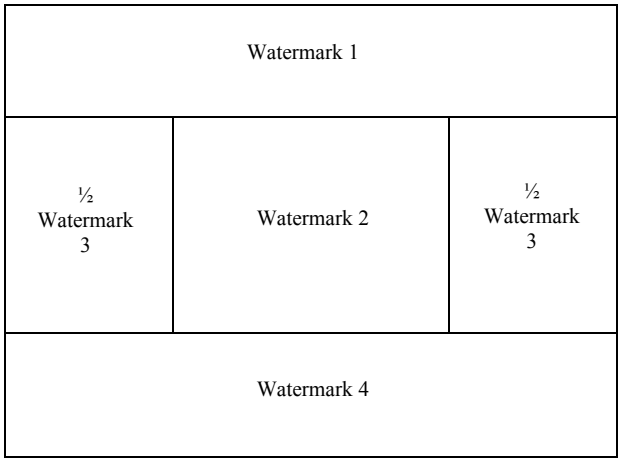

Fig.2 Block diagram of proposed watermark embedding positions

5. Obtain a scrambled binary watermark W_s using exclusive-or (X-OR) operation denoted the mark $\oplus$ between the binary watermark W and secret chaotic binary sequence K as follows:

$$W_s = W \oplus K \qquad (2)$$

B. Watermark Embedding

The proposed watermark embedding process includes the following steps:

1. Produce a scrambled binary watermark W_s from original binary watermark W as described in section III(A).

2. Consider a original host image H of size M×N.

3. Divide the original host image H into 8-bit planes.

4. Divide the original host image H into non-overlapping blocks of size p×q pixels.

5. Make all the odd pixels of each block of H to even number by setting zero to least significant bit (LSB) i.e, $b_0=0$.

6. Each encoded bit of scrambled binary watermark W_s is embedded into a block of size p×q pixels as follows:

If $W_s=1$

Then $b_0'=1$; for all the pixels of p×q blocks

If $W_s=0$

Then $b_0'=b_0=0$; for all pixels of p×q blocks.

Where b_0' is the modified LSB.

7. Step 6 is repeated until all encoded bits of scrambled binary watermark W_s are embedded to obtain the watermarked image $\hat{I}$.

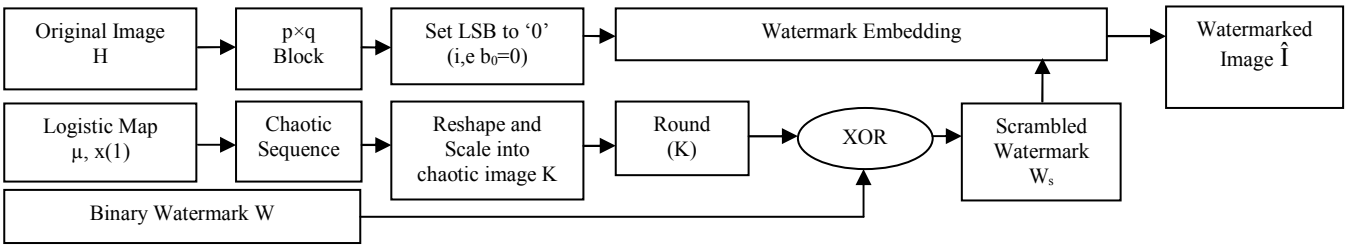

Fig.3 Block diagram of proposed watermark embedding process

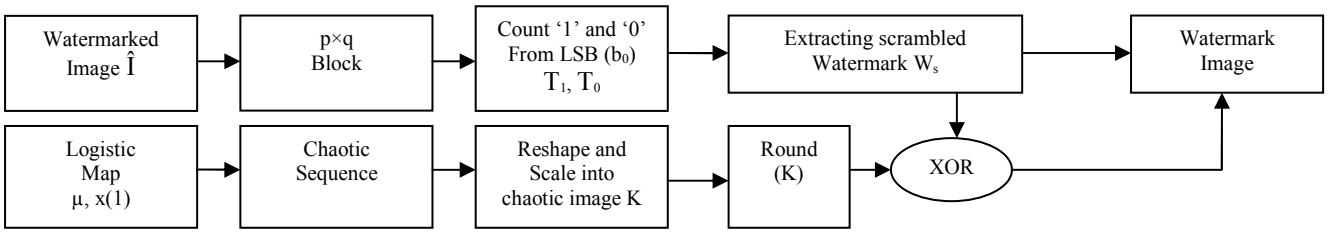

Fig.4 Block diagram of proposed watermark extraction process

C. Watermak Extraction

The proposed watermark extraction process includes the following steps:

1. Divide the watermarked image Î into 8-bit planes.

2. Divide the watermarked image Î into non-overlapping blocks of size p×q pixels.

3. The extraction of scrambled binary watermark bit depends on the total number of '1' and '0' bit denoted by T_1 and T_0 respectively from each block of size 8×8 pixels as follows:

$$\text{If } T_1 \geq T_0$$
$$\text{Then } W_s=1$$
$$\text{If } T_1 < T_0$$
$$\text{Then } W_s=0$$

4. Repeat step 3 until all encoded bits of scrambled watermark W_s are extracted to get the scrambled binary watermark W_s.

5. Apply X-OR operation between the scrambled binary watermark W_s and secret chaotic binary sequence K to obtain the original binary watermark as follows:

$$W = W_s \oplus K \qquad (3)$$

6. Apply the same process to obtain the four watermarks from different locations of watermarked image.

IV. Experimental Results And Comparison

To test the efficiency of the proposed algorithm, various experiments are carried out in this part. For all the experiments, a binary logo image of size 32×32 pixels is used as watermark which is scrambled by using logistic map with parameters μ=3.999 and x(1)=0.4567. Here the value of μ and x(1) are the initial conditions which are also secret. On the other hand, original gray scale images of 'Cameraman', 'Lena', 'Baboon' and 'House' of size 512×512 pixels are used as test images. In the proposed scheme the watermark of size 32×32 is embedded four times in different locations of host image. Each location is divided into 1024 blocks of size 8×8 pixels. One bit out of 1024 bits of watermark is required to embed each block of size 8×8 out of 1024 blocks. Hence, one watermark is required to embed 1024 block of size 8×8 pixels. The proposed scheme used the peak signal to noise ratio (PSNR), mean square error (MSE) and bit error rate (BER) as shown in equations (4), (5) and (6) respectively, as the performance tools. To test the robustness of the proposed scheme, some common image processing attacks such as filtering, cropping and salt and pepper noise also applied.

$$PSNR=10\times\log_{10}(L^2/MSE)\ \text{dB} \qquad (4)$$

Where L is the maximum gray level and MSE is the mean square error between the original image and attacked image Î, given by

$$MSE=(1/M\times N)\sum_i\sum_j [I(i,j)-\hat{I}(i,j)]^2 \qquad (5)$$

Where $1\leq i \leq M$ and $1\leq i \leq N$

$$BER=(1/m\times n)\sum_i\sum_j [W(i,j) \oplus W^*(i,j)] \qquad (6)$$

Where $1\leq i \leq m$ and $1\leq i \leq n$

Fig.5 Examples of applying image-processing operations on the watermarked image.(a) the original Baboon image, (b) the original House image, (c) the Lena image, (d) the original Cameraman image, (e-h) their corresponding watermarked image, (i-h) extracted watermarks from (e-h) respectively, (m- J) the results of cropping, salt and pepper noise and filtering attack on (e-h).

"Fig.5(e-h)", show the watermarked images of original images in "Fig.5(a-d)" with PSNR 15.14dB, 15.13dB, 51.14dB and 51.14dB respectively. "Fig.5(i-l)", show the extracted watermarks from "Fig.5(e-h)" with 0% BER.

"Fig.5(m-p)", show the attacked watermarked images by cropping 25% from bottom, 50% from left and right side, 75% from surrounding and 75% from bottom and left and right side respectively. "Fig.5(q-t)" show their corresponding extracted watermarks with 0% BER.

"Fig.5(u-x)", show the attacked watermarked images by salt and pepper noise with intensity 0.6, 0.7, 0.8 and 0.8 respectively. "Fig.5(y-B)", show the extracted watermarks from "Fig.5(u-x)" with 0%, 0.78%, 5.66% and 23.44% BER respectively.

"Fig.5(C-F)", show the attacked watermarked images by Median filter 3×3, Median filter 5×5, Median filter 7×7 and Median filter 7×7 with 36.34dB, 29.61dB, 32.97dB and 34.62dB PSNR respectively. "Fig.5(G-J)" show their corresponding extracted watermarks with 0%, 0.097%, 0.20% and 0.68% BER respectively.

"Fig.6", shows the relationship between noise intensity and BER of our proposed scheme. The bit error rate is zero up to the level of intensity equal to 0.6. Above this value, the bit error rate is increased with the intensity of noise.

"Table I", shows the performance of robustness of the proposed scheme against salt and pepper noise attack for original Cameraman, Baboon and House images by evaluating BER as a performance tool. For the value of noise intensity 0.6 or less than 0.6, the bit error rate is zero. Hence, the proposed scheme provides better performance. The bit error rate increases with intensity of noise above this limiting value.

"Table II", also shows the performance of robustness of the proposed scheme in case of filtering attack for original Baboon, House and Lena images by calculating BER and PSNR values. Here, the proposed scheme used Median filter 3×3, Median filter 5×5 and Median filter 7×7 to test the robustness. The bit error rate for every case is almost zero and the values of PSNR are maintained a satisfactory level which shown the robustness of the proposed scheme.

"Table III", shows the comparison results of PSNR and BER of proposed method with other two existing methods in case of Lena image. It indicates that the proposed method has better value of PSNR than method in [12]. The proposed method gives 0% BER when the watermarked image is attacked by salt and pepper noise with intensity 0.1 to 0.6 while the method in [13] the BER is more than 0%. At the same time, in case of filtering attacks the proposed method also gives 0% BER where some BER rates are obtained from the method in [13]. Therefore the proposed watermarking scheme shows robustness against some attacks.

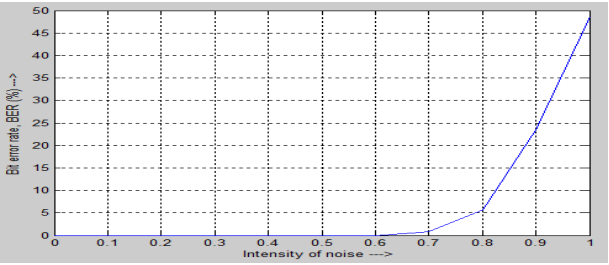

Fig.6 The relationship between intensity of noise and BER

TABLE I. EXPERIMENTAL RESULTS FOR SALT AND PEPPER NOISE ATTACK

Attack Salt and pepper noise (intensity)	**Cameraman** BER %	**Baboon** BER %	**House** BER %
0.1	0	0	0
0.2	0	0	0
0.3	0	0	0
0.4	0	0	0
0.5	0	0	0
0.6	0	0	0
0.7	0.98	0.78	0.78
0.8	4.49	5.18	5.57
0.9	19.92	19.04	19.73
1.0	48.93	50.10	48.73

TABLE II. EXPERIMENTAL RESULTS FOR FILTERING ATTACK

Attack	**Baboon**		**House**		**Lena**	
	BER %	PSNR dB	BER %	PSNR dB	BER %	PSNR dB
Median filter 3×3	0	36.34	0	35.56	0	42.11
Median filter 5×5	0	29.82	0.097	29.61	0	36.13
Median filter 7×7	0	26.71	0	26.40	0.20	32.97

TABLE III. COMPARISON RESULTS OF PSNR AND BER OF PROPOSED METHOD WITH OTHER METHODS

Attacks		**PSNR**		**BER %**	
		Method [12]	Proposed method	Method [13]	Proposed method
Cropping	50%	8.5	9.17	0	0
	75%	6.38	7.33	0	0
Salt and pepper noise		-	-	2.71	0
Median filter	3×3	33.15	42.11	1.53	0
	5×5	30.4	36.15	1.89	0

V. CONCLUSION

This paper proposed a new blind robust digital watermarking scheme for gray scale images. The binary watermark is embedded four times in different locations including number of non-overlapping blocks of host image. The logistic map is used to generate chaotic image pattern of watermark in order to provide high security. The extraction of watermark is based on probability of existing total number of binary bits '1' and '0' in a single block. The extraction of watermark is only possible with correct keys which show that the proposed scheme is secured. The experimental results also show that the proposed scheme is highly robust compared with other methods against some attacks, such as cropping, filtering and salt and pepper noise.

REFERENCES

[1] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," Vision, Image and Signal Processing, IEE Proceedings -, vol. 147, pp. 288-294, 2000.

[2] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," Physics Letters A, vol. 365, pp. 403-406, 2007.

[3] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.

[4] S. Kimpan, A. Lasakul, and S. Chitwong, "Variable block size based adaptive watermarking in spatial domain," presented at Communications and Information Technology, ISCIT 2004. IEEE International Symposium on, vol. 1, pp. 374-377, 2004.

[5] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," IEEE Trans. on Circuits and Systems for Video Technology, vol. 13(8), pp. 776-786, 2003.

[6] M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking of color images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 12(3), pp. 142-156, 2002.

[7] L. Chun-Shien, H. Shih-Kun, S. Chwen-Jye, and L. Hong-Yuan Mark, "Cocktail watermarking for digital image protection," Multimedia, IEEE Transactions on, vol. 2, pp. 209-224, 2000.

[8] L. M. Cheng, L. L. Cheng, C. K. Chan, and K. W. Ng, "Digital watermarking based on frequency random position insertion," presented at Control, Automation, Robotics and Vision Conference, vol. 2, pp. 977-982, 2004.

[9] W. Lu, H. Lu, and F.-L. Chung, "Robust digital image watermarking based on subsampling," Applied Mathematics and Computation, vol. 181, pp. 886-893, 2006.

[10] Q. Ying and W. Ying, “A survey of wavelet-domain based digital image watermarking algorithm," Com- puter Engineering and Applications, vol. 11, pp. 46- 49, 2004.

[11] L. Lian-Shan, L. Ren-Hou, and G. Qi, "A new watermarking method based on DWT green component of color image," in International Conference on Machine Learning and Cybernetics, vol. 6, pp. 3949-3954, 2004.

[12] Ibrahim Nasir, Ying Weng, Jianmin Jiang, “A New Robust Watermarking Scheme for Color Image in Spatial Domain”.

[13] B Surekha, Dr GN Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and Its Applications, Vol. 5 No. 1, January, 2011