I.J. Image, Graphics and Signal Processing, **2016, 1, 51-58**
Published Online January 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.01.06

Improving the Security of Spatial Domain Based Digital Image Watermarking using Chaotic Map and Cellular Automation

Chandan Saha, Md. Foisal Hossain and B. M. Shahnewaz Abdullah
Department of Electronics and Communication Engineering Khulna University of Engineering & Technology (KUET)
Khulna-9203, Bangladesh
E-mail: Chandan.ece2k10.kuet@gmail.com, foisalkuet@yahoo.com, shahnewazshaon@yahoo.com

Abstract—The security of digital image watermarking is improved by scrambling the watermark using different chaotic maps or cellular automata in such a way that an unauthorized person can't recover the watermark without the secret keys. In this proposed scheme three secret keys are used in which one key is used to make the watermark chaotic and other two keys are used for scrambling the cover image. In this scheme the cover image is scrambled by using the game of life cellular automation and the watermark is made chaotic by performing the X-OR operation between the binary watermark and logistic map. Although it increases the computational complexities, but the security of watermarking is improved by involving three secret keys. In addition, for ensuring imperceptibility and making the watermarking robust, a mask of size 3×3 is run over the scrambled cover image in which one bit of chaotic watermark is embedded in 3×3 block of cover image by modifying one of the neighbor pixels. Then the scrambled modified cover image is descrambled using game of life cellular automation for obtaining watermarked image. This proposed combined chaotic and cellular automata based watermarking scheme is compared with existing chaotic based watermarking schemes and gives satisfactory values of Peak Signal to Noise (PSNR), Mean Squared Error (MSE) and Normalized Correlation (NC).

Index Terms—Logistic map, game of life, cellular automation, scaling factor.

I. Introduction

Due to the development of information and communication technology, the security of information has attracted the interest of the researchers over the last decade [1]. Digital image watermarking is one of the effective schemes for providing such a security and it is a technique of embedding information called watermark into original image by ensuring the imperceptibility. There are two domains on which image watermarking is performed- *spatial domain and transformed domain*. The embedding procedure of spatial domain based watermarking is to embed the bits of watermark into bit planes of cover image directly. So in spatial domain, the computational complexity is low; normally it is used for fragile watermarking as well as the capacity is also high depending on the size of image. On the other-hand, in transformed domain, watermarks are embedded into the frequency coefficients; so the computational complexity is high as well as the capacity is low. The main feature of transformed domain based watermarking is that it shows the robustness against different image processing attacks. Different transforms such as Discrete Cosine Transform (DCT) [2], Discrete Wavelet Transform (DWT) [3] are used in watermarking techniques.

The security of digital image watermarking is improved by involving different chaotic maps such as Arnold's cat map, logistic map. Cellular automata show the complex characteristic which is used in different types of applications such as- random number generation, pattern recognition, games [4]. Wu *et al.* [5] proposed a chaos based robust spatial domain watermarking algorithm where for encrypting watermark 1-D logistic map is used and for encrypting embedding position of cover image 2-D Arnold's Cat map is used. Rawat *et al.* [6] proposed a chaotic system based fragile watermarking scheme for image tamper detection. In this scheme the authors proposed a chaos based watermarking technique for image authentication, tamper detection and localization where two chaotic maps- Arnold's Cat map and logistic map are used. Liu *et al.* [7] proposed an image fragile watermark scheme based on chaotic image pattern and pixel pattern. In this scheme the authors used the chaotic map for generating chaotic pattern image and watermark embedding procedure results from calculating the difference between host image and its chaotic pattern. Wenyin *et al.* [8] proposed semi fragile spatial watermarking based on local binary pattern operators where LBP is used for embedding and extracting watermark. Chaotic based watermarking is also performed on transformed domain. Dawei *et al.* [9] proposed a chaos based robust wavelet domain watermarking algorithm where DWT is used and chaotic watermark is embedded into the part of sub-band coefficients. Yantao *et al.* [10] proposed a robust chaos based DCT domain watermarking algorithm. In this scheme the author scrambled the watermark using chaotic map and then the chaotic watermark is embedded into LSB of the DCT coefficients which are determined by

another chaotic map with another secret keys. Rosline *et al.* [11] proposed normalized image watermarking scheme using chaotic system. Chrysochos *et al.* [12] proposed robust watermarking of digital images based on chaotic mapping and DCT. Song *et al.* [13] proposed a blind digital watermark method based on SVD and chaos. In this scheme the author encrypted the watermark using Tent chaotic map and embedded encrypted watermark into singular values of cover image. Image can be scrambled by using cellular automata. Dalhoum *et al.* [14] proposed Digital Image Scrambling Using 2D Cellular Automata where rules of game of life are used for scrambling image.

(a) (b) (c)

Fig.1. (a) Random Configurations Generated by Logistic Map Using Secret key (μ=3.9745 and x (1) =0.1245); (b) Jet-Plane Image; (c) Chaotic Jet-Plane Image using Logistic Map

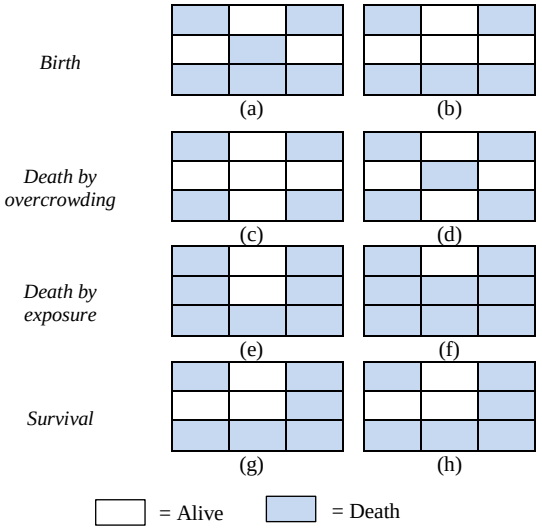

Fig.2. Rules of Game of Life

In this proposed scheme Game of life cellular automation [14] is used to scramble the cover image and the binary watermark is X-ORed with the logistic map in order to form the chaotic watermark. In this scheme watermarking is performed in spatial domain. For embedding chaotic watermark bits in spatial domain, one bit of chaotic watermark is embedded into 3×3 block of scrambled cover image by considering and modifying only one of the eight neighbors of 3×3 block [8].

The remainder of the paper is arranged as follows. The background of the proposed scheme including logistic map, game of cellular automation is described in Section II. The proposed scheme including scrambling, embedding, descrambling and extraction is described in Section III. The experimental results and comparison with the existing methods are described in Section IV. Finally the paper is concluded is Section V.

II. Background

The proposed watermarking scheme involved logistic map and game of life cellular automation techniques. These techniques are described in this section as follows:

A. Loistic Map

For improving the security of digital image watermarking, different types of chaotic maps have been proposed. Among them logistic map is the simplest chaotic map. This map is described by

$$x_{k+1} = \mu x_k(1 - x_k) \quad (1)$$

where, $0 < \mu \leq 4$. The values of μ and $x(1)$ are the initial conditions which can be used as the secret keys. This map is sensitive to initial conditions. Sensitive to initial condition means that the relationship between two logistic sequences with different initial conditions is statistically uncorrelated. Fig.1 (a) shows the random configurations generated by logistic map using secret key (μ=3.9745 and x(1)=0.1245). Fig.1 (b) shows the jet-plane image and Fig.1 (c) shows the chaotic jet-plane image using logistic map.

B. Game of Life Cellular Automation

Cellular Automata show the complex characteristics which are proposed by Stani-slaw Ulam and John Von Neumann in the 1940s [14]. The applications of cellular automata are in the fields of random number generation, pattern recognition, games etc. Game of life is a well-known example of cellular automation which is normally used in order to scramble the pixel positions of digital images.

The rules of game of life are applied to the initial matrix (GL) of size $M \times N$ which is formed in this paper by using logistic map. Either of two states such as death (0) or alive (1) is represented by each cell of $M \times N$ cells. The initial matrix GL is run for K times (called generations- used as secret key in this paper). Here Moore neighborhood is considered, so each cell updates its state (dead or alive) by considering the states of eight neighbors according to the rules of game of life. Fig. 1 shows the rules of game of life for scrambling digital images.

In case of rule of birth, where center cell is death and exactly three neighbor cells are alive at time t shown Fig. 2 (a) so the center cell will be alive at time $t+1$ shown in Fig. 2 (b). In case of rule of death by overcrowding, where center cell is alive and four (or more) neighbor cells are alive at time t shown Fig. 2 (c) so the center cell dies at time $t+1$ shown Fig. 2 (d). In case of rule of death by exposure, where center cell is alive and one (or none) neighbor cell is alive at time t shown Fig. 2 (e) so the center cell dies at time $t+1$ shown Fig. 2 (f). In case of rule of survival, where center cell is alive and two (or three) neighbor cells are alive at time t shown Fig. 2 (g) so the center cell survives at time $t+1$ shown Fig. 2 (h).

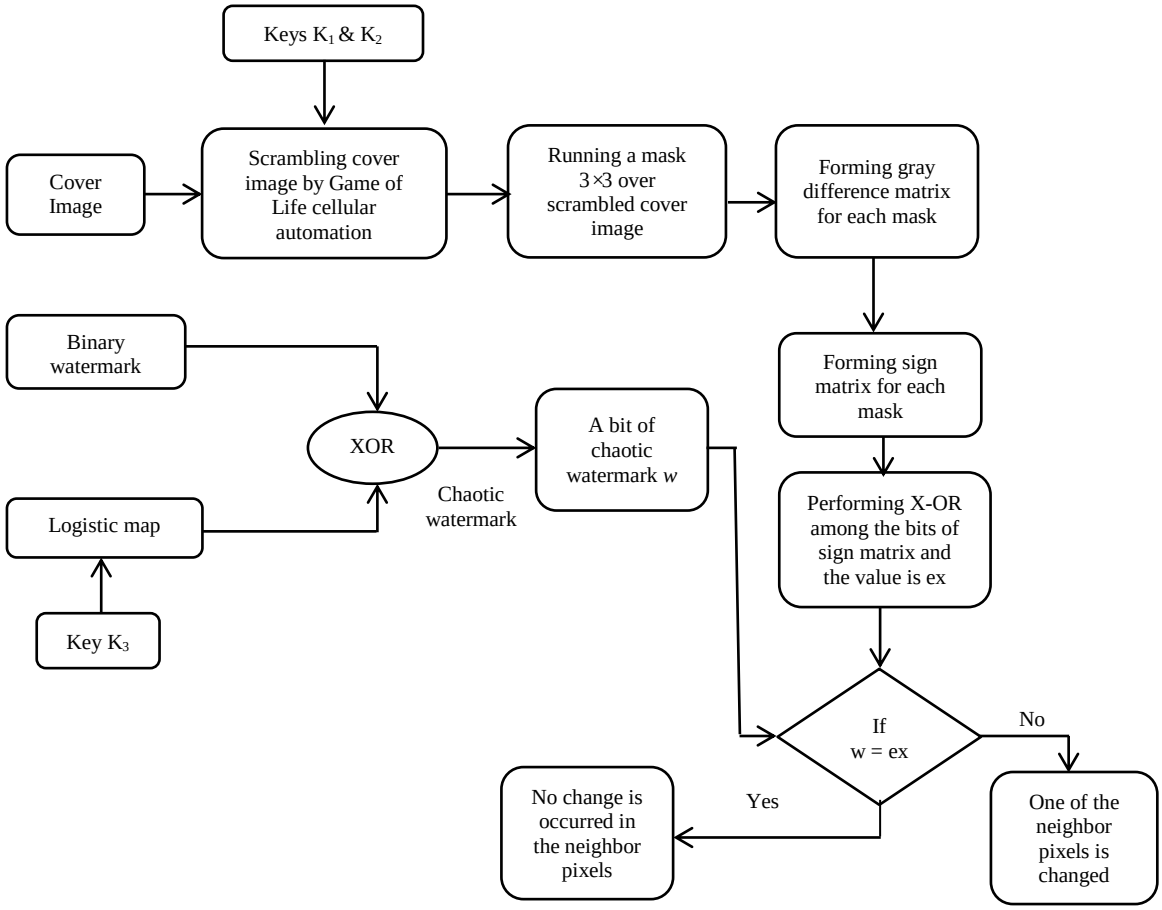

Fig.3. Block Diagram of Cover Image Scrambling and Chaotic Watermark Embedding Procedure

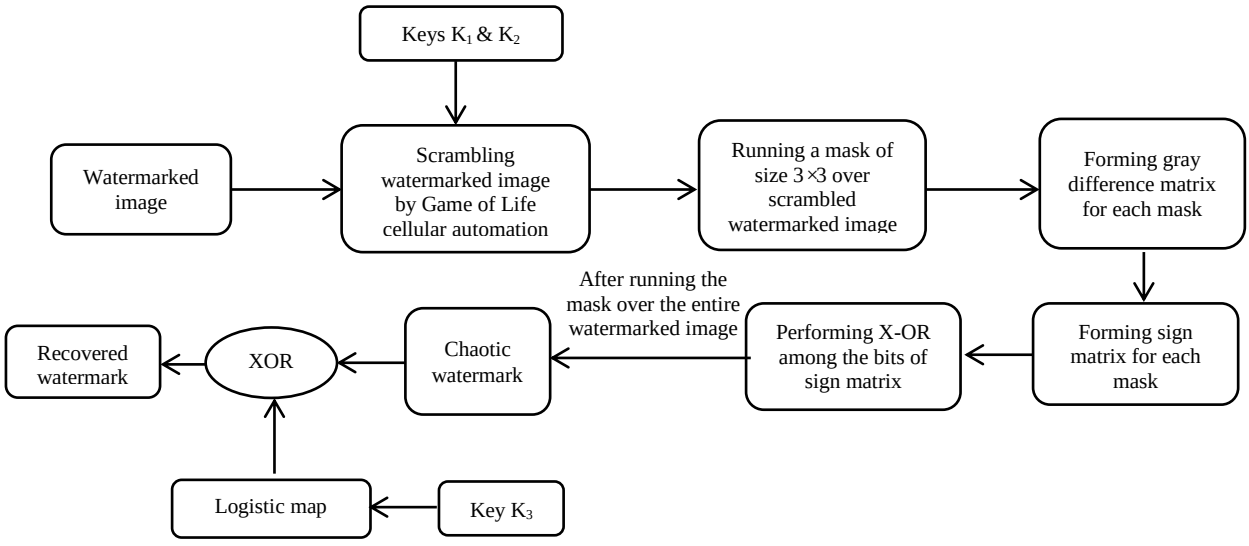

Fig.4. Block Diagram of Watermark Extracting Procedure

p_1	p_2	p_3
p_8	p_c	p_4
p_7	p_6	p_5

(a)

d_1	d_2	d_3
d_8		d_4
d_7	d_6	d_5

(b)

b_1	b_2	b_3
b_8		b_4
b_7	b_6	b_5

(c)

Fig.5. (a) Gray Values of 3×3 Mask; (b) Gray Difference Matrix; (c) Sign Matrix

III. Proposed Method

The proposed watermark embedding algorithm and the proposed watermark extraction algorithm are explained in this section.

A. Embedding Algorithm

A gray-scale image of size 255×255 is considered as a cover image and a binary image of size 85×85 is

considered as watermark. Cover image scrambling by using game of life cellular automation and chaotic watermark embedding procedure into scrambled cover image is shown in Fig. 3. The scrambling and embedding algorithm is described as follows:

- Then another logistic map G_0 of size equal to cover image is generated using key *K1* for performing the rules of game of life upon it.
- The rules of game of life are applied to the matrix G_0 to obtain first generation G_1, rules applied to G_1 to obtain second generation G_2 and this process is repeated for *K2* (key) number of generations.
- For the first generation of game of life G_1, pixels of the cover image are scrambled according to $G_1 (x, y) = 1$
- For the second generation of game of life G_2, pixels (that are not scrambled in case of first generation) are scrambled according to $G_2 (x, y) = 1$ and $G_1 (x, y) \neq 1$.
- Step 5 is repeated from iteration third generation to *K2* generation.
- After completing *K2* iterations, remaining of the pixels are scrambled according to $G_{K2} (x, y) = 0$.
- At first, a logistic map is generated using key *K3*. By performing the X-OR operation between binary watermark and generated logistic map, a binary chaotic watermark is obtained.
- For embedding binary chaotic watermark into the scrambled cover image, a mask of size 3×3(shown in Fig. 5 (a)) is run over the scrambled cover image of size 255×255.
- The gray difference matrix (shown in Fig. 5 (b)) is obtained by calculating the difference between the center pixel and neighbor 8 pixels.
- If the gray difference is positive (or zero) then one is assigned or if the gray difference is negative then zero is assigned in order to form sign matrix.
- X-OR is performed among the bits of sign matrix (shown in Fig. 5(c)) which is given by

$$ex = b_1 \oplus b_2 \oplus b_3 \oplus \ldots\ldots\ldots\ldots \oplus b_8 \quad (2)$$

- Only one bit of chaotic binary watermark is embedded in 3×3 mask of scrambled cover image. Suppose *w* is one of the bits of binary chaotic watermark of size 85×85. If *w* is equal to *ex*, then no change is occurred in the neighbor pixels of 3×3 mask. If *w* is not equal to *ex*, then one of the neighbor pixels is changed according to the following steps:

  a. From the absolute values of gray differences of gray difference matrix, the minimum value d_{min} is determined as well as the pixel value p_{min} corresponding to d_{min} is also determined.

  b. Gray value of that pixel is changed as follows:

$$p_{mod} = (p_{min} - d_{min}) - \alpha; \text{ if } b_{min} = 1 \quad (3)$$

$$p_{mod} = (p_{min} + d_{min}) + \alpha; \text{ if } b_{min} = 0 \quad (4)$$

  where, p_{mod} is the modified pixel, b_{min} is the binary bit of sign matrix and α is scaling factor ranging from 1 to 5.

- After embedding all the bits of chaotic watermark into scrambled cover image, the modified scrambled cover image is obtained.
- The pixels of modified scrambled cover image return back to their original positions according to $G_1 (x, y) = 1$.
- Pixels that are not descrambled in case of first generation return back to their original positions according to $G_2 (x, y) = 1$ and $G_1 (x, y) \neq 1$.
- Step 15 is repeated from iteration third generation to *K2* generation.
- After completing *K2* iterations, remaining of the pixels return back to their original positions according to $G_{K2} (x, y) = 0$.
- When all the pixels of modified scrambled cover are descrambled to their original positions, then watermarked image is obtained.

B. Extraction Algorithm

Chaotic watermark is extracted from watermarked image and binary watermark is recovered from chaotic watermark by using logistic map. The whole procedure is shown in Fig. 4.

- Using the secret keys K1 and K2, steps 1 to 6 (described in section) are repeated for scrambling the watermarked image.
- A mask of size 3×3 is run over the scrambled watermarked image.
- The gray difference matrix is obtained by calculating the gray the difference between the center pixel and neighbor 8 pixels of 3×3 mask.
- If the gray difference is positive (or zero) then one is assigned or if the gray difference is negative then zero is assigned in order to form sign matrix.
- Chaotic watermark is obtained from the result after performing X-OR operation among the binary bits of sign matrix.
- A logistic map is generated using the secret key K3. Then the binary watermark is recovered after Performing the X-OR operation between the chaotic watermark and generated logistic map.

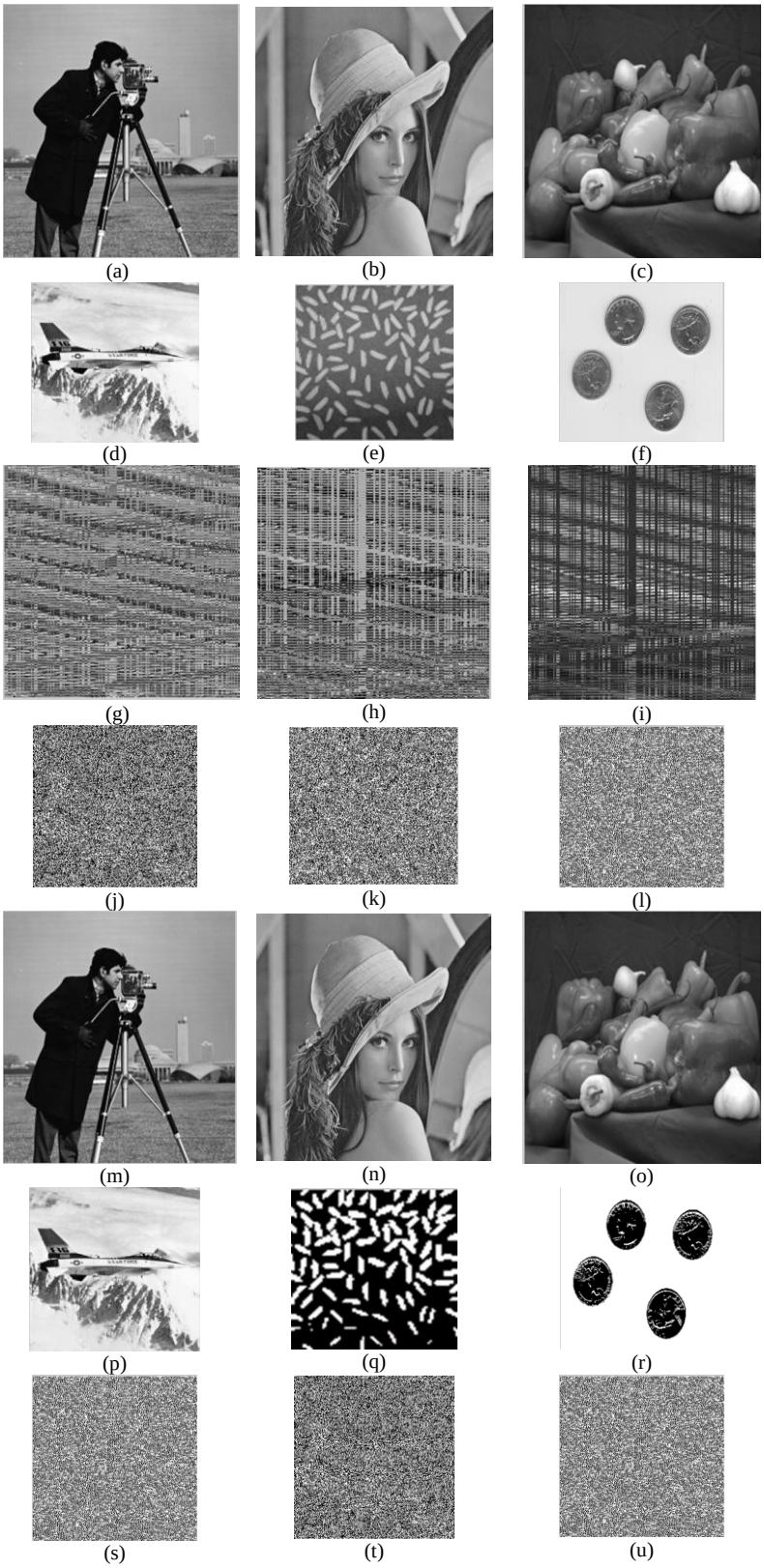

Fig.6. (a)-(c) Original Cover Images; (d)-(f) Watermark Images; (g)-(i) Scrambled Cover Images using Cellular Automation for First Generation; (j)-(l) Chaotic Watermarks using Logistic Map; (m)-(o) Watermarked Images; (p)-(r) Recovered Watermarks; (s)-(u) Extracted Watermarks using Wrong Keys.

IV. Experimental Results and Comparison

We have evaluated our proposed scheme in case of different gray scale images. Three gray scale images (Cameraman, Lena, Peppers) of size 255×255 are used as

the original cover images which are shown in the first row of Fig. 6. Three images (jet-plane, rice, coins) of size 85×85 are used as the watermarks which are shown in the second row of Fig. 6. The third row of Fig. 6 shows the scrambled cover images using game of life cellular automation for first generation as well as the forth row shows the chaotic watermarks using logistic map. Three watermarked images are shown in the fifth row of Fig. 6. Three recovered watermarks are shown in the sixth row of Fig. 6. Three extracted watermarks using wrong keys are shown in the seventh row of Fig. 6.

There are three performance evaluating parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Correlation (NC) are used in order to the evaluate performance of this proposed scheme. In order to implement this watermarking procedure and also evaluate the performance of this scheme, MATLAB (v. 13.0.1) is used.

MSE is used to measure the error between host image *X* and watermarked image *Y* which is defined as follows:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2 \qquad (5)$$

PSNR is an important performance evaluating parameter in order to find out similarity between host image and watermarked image and basically it is used for estimating the imperceptibility. PSNR is calculated from MSE which is defined as follows:

$$PSNR = 10log_{10}\left[\frac{max^2}{MSE}\right] \qquad (6)$$

where, $max = M \times N$

NC is another performance evaluating parameter in order to find out the similarity between the original watermark and extracted watermark NC is used which is defined as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(W(i,j)\times W'(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)^2} \qquad (7)$$

where, *M* and *N* are rows and columns of image. *W* and W' are the original watermark and extracted watermark respectively.

Table 1. MSE and PSNR Values of Watermarked Images (Cameraman, Lena and Peppers) for Different Values of Scaling Factor

Scaling Factor α	Cameraman		Lena		Peppers	
	MSE	*PSNR*	*MSE*	*PSNR*	*MSE*	*PSNR*
1	1.7036	45.8510	0.4439	51.6922	0.3219	53.0872
1.5	1.8852	45.4112	0.5410	50.8325	0.4274	51.8568
2.0	2.0962	44.9505	0.6615	49.9594	0.5591	50.6898
2.5	2.3365	44.4791	0.8053	49.1053	0.7172	49.6086
3	2.6062	44.0047	0.9724	48.2864	0.9015	48.6150
3.5	2.9053	43.5329	1.1628	47.5098	1.1122	47.7030
4	3.2338	43.0677	1.3765	46.7771	1.3492	46.8642
4.5	3.5916	42.6119	1.6135	46.0871	1.6124	46.0900
5	3.9788	42.1673	1.8738	45.4375	1.9020	45.3727

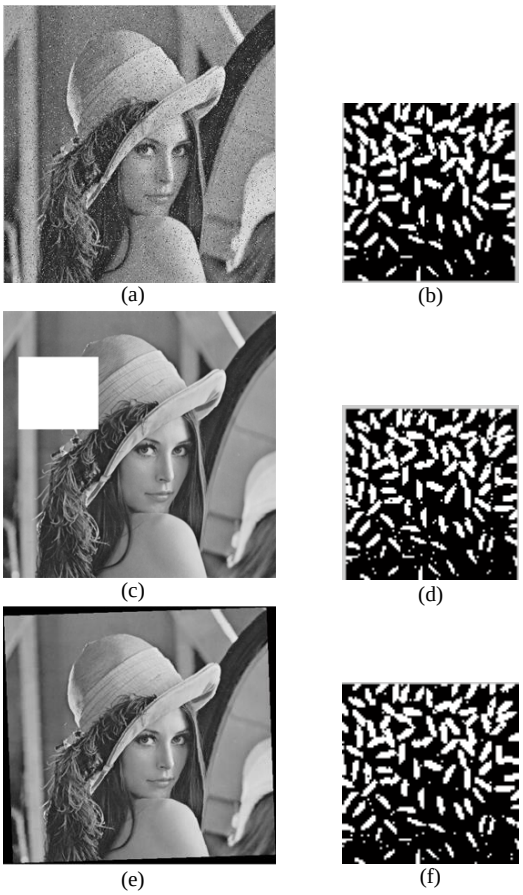

Fig.7. (a) Watermarked Image Attacked by Salt & Pepper Noise; (b) Its Corresponding Recovered Watermark Image; (c) Watermarked Image Cropped by 10%; (d) Its Corresponding Recovered Watermark Image; (i)-(e) Rotated by 2 Degree; (f) Recovered Watermark Image.

The scaling factor α is very important for this proposed scheme in order to embed and extract watermark. Table 1 represents the PSNR and MSE values of three watermarked images (Cameraman, Lena and Peppers) for scaling factor ranging from 1 to 5. The PSNR values are decreasing as well as MSE values are increasing with the increasing of scaling factor. From the results it is shown that the PSNR and MSE values attain satisfactory values for scaling factor 1 to 5.

Fig. 7(a) shows the watermarked image under salt & pepper noise attack and Fig. 7(b) shows its corresponding recovered watermark. Watermarked image cropped by 10% and rotated by 2 degree which is shown in Fig. 7(c) and Fig. 7(e) respectively. Their corresponding recovered watermark images are shown in Fig. 7(d) and Fig. 7(f) respectively.

Table 2. Performance against Different Attacks

Attack Type	Cameraman	Lena	Peppers
	NC	*NC*	*NC*
No attack	1.0000	1.0000	1.0000
Salt & pepper (0.005)	0.9724	0.9732	0.9782
Cropping (10%)	0.9523	0.9627	0.9724
Image rotation (angle 5)	0.9045	0.9196	0.9256

Table 3. Comparison Results of PSNR

Images	Method [12]	Method [11]	Method [6]	Proposed Method
	PSNR	*PSNR*	*PSNR*	*PSNR*
Cameraman	35.16	45.42	50.14	51.51
Lena	35.15	45.35	50.49	51.76
Peppers	36.50	43.13	51.71	53.08

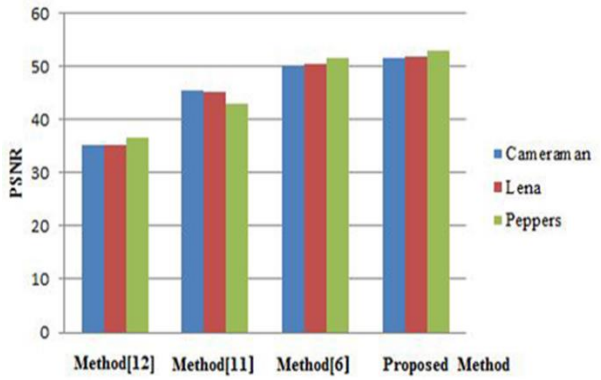

Fig.8. Comparison Results with other Methods

Table 2 shows the performance of the proposed scheme in terms of Normalized Correlation (NC) against three attacks. The values of NC are satisfactory in case of three attacks.

Table 3 shows the comparison results of PSNR with three existing methods in [12], [11] and [6]. Graphical representation of comparison with other three existing chaotic methods is shown in Fig. 8. From the comparison results, it can be seen that our proposed method outperforms than other three methods in terms of PSNR.

V. Conclusions

Improving the security of spatial domain based digital image watermarking has been proposed in this paper. In this proposed spatial domain based watermarking scheme, three secret keys are used in order to improve the security of watermarking. From logistic map one secret key is obtained and from game of life cellular automation other two secret keys are obtained. The watermark is made chaotic using logistic map and the cover image is scrambled using game of life cellular automation. So, three secret keys must be required to recover the watermark. In addition only one bit of chaotic watermark is embedded in 3×3 block of scrambled cover image which ensures the imperceptibility and robustness. Then the scrambled modified cover image is descrambled using game of life cellular automation for obtaining watermarked image. This proposed scheme is evaluated in terms of PSR, MSE and NC.

From the experimental results it is demonstrated that this proposed scheme gives satisfactory values of PSNR for different images. Scaling factor is very significant for keeping the PSNR values high and MSE values low as well as it is also very important for embedding and extracting watermark. This proposed scheme is robust against attacks such as salt & pepper, cropping and rotation. In addition, this proposed scheme is compared with three existing chaotic based watermarking methods. This proposed method gives satisfactory performances than other three methods.

References

[1] T. Minamoto and R. Ohura, "A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic," *Sci. Direct Journal of Applied Mathematics and Computation*, pp-306-319, 2014.

[2] Chandra M. B. and Srinivas K. S., "Robust multiple image watermarking scheme using Discrete Cosine Transform with multiple descriptions," *International Journal of Computer Theory and Engineering*, vol. 1, pp. 1793–8201, 2009.

[3] B.L. Gunjal and R.R. Manthalkar, "Discrete Wavelet Transform based strongly robust watermarking scheme for information hiding in digital images," Third Int. Conf. Emerging Trends in Engineering and Technology. India, pp. 124-129, Nov 2010.

[4] R.-J. Chen and J.-L. Lai, ''Image security system using recursive cellular automata substitution,'' *Pattern Recognition*, vol. 40, no. 5, 2007, pp. 1621-1631.

[5] X. Wu, Z.-H. Guan and Z. Wu, "A chaos based robust spatial domain watermarking algorithm", *Advances in Neural Networks – ISNN 2007*, vol. 4492, pp. 113-119, 2007.

[6] S. Rawat, B. Raman. "A chaotic system based fragile watermarking scheme for image tamper detection", *Sci. Direct International Journal of Electronics and Communication*, vol. 65, pp. 840-847, 2011.

[7] S.-H. Liu, H.-X. Yao, W. and Y.-L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel pattern", *Applied Mathematics and Computation*, vol. 185, pp. 869–882, 2007.

[8] Z. Wenyin and F. Shih, "Semi fragile spatial watermarking based on local binary pattern operators", *Optics Communications*, vol. 284, pp. 3904–3912, 2011.

[9] Z. Dawei, C. Guanrong and L. Wenbo, "A chaos based robust wavelet domain watermarking algorithm", *Chaos, Solutions & Fractals*, vol. 22, pp. 47–54, 2004.

[10] G. Z. Yantao, M. Yunfei and L. Zhiquan, "A robust chaos based DCT domain watermarking algorithm", *International Conference on Computer Science and Software Engineering*, vol. 3, pp. 935 - 938, 2008.

[11] G. Rosline, S. Maruthuperumal, "Normalized image watermarking scheme using chaotic system", *International Journal of Information & Network Security*, vol.1, no.4, pp. 255-264, October 2012.

[12] E. Chrysochos, V. Fotopoulos, and A. N. Skodras, "Robust watermarking of digital images based on chaotic mapping and DCT", *16th European Signal Processing Conference (EUSIPCO 2008)*, Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP.

[13] J. Song, J. Song and Y. Bao, "A blind digital watermark method based on SVD and chaos", *Procedia Engineering*, vol. 29, pp. 285–289, 2012.

[14] A. Dalhoum, M. MAhafzah, A. Awwad, I. Aldamari, A. Oterga and M. Alfonseca "Digital image scrambling using 2D cellular automata", *14th IEEE international Symposium on Multimedia*, 10-12 December 2012, Irvine, CA,US.

[15] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Digital Signal Processing, vol. 33, pp. 134–147, 2014.

[16] S.Maruthuperumal and G.Rosline Nesa Kumari, "Permutation-based Homogeneous Block Content Authentication for Watermarking," International Journal of Image, Graphics and Signal Processing (IJIGSP), Vol.5, No.2, pp. 25-30, 2013.

Authors' Profiles

Chandan Saha was born on 29 November, 1993 in Bangladesh. He has received B.Sc. degree in Electronics and Communication Engineering from Khulna University of Engineering & Technology in 2015. His research interests are digital image watermarking, digital signal processing and biomedical signal processing.

Md. Foisal Hossain received his B.Sc. Engineering degree in Electrical and Electronic Engineering from Khulna University of Engineering & Technology (KUET), Bangladesh in 2002. He received M. Sc. in 2008 and PhD in 2011 from University of the Ryukyus, Okinawa, Japan. He is currently an associate professor with the department of Electronics and Communication Engineering, at Khulna University of Engineering & Technology (KUET), Khulna, Bangladesh. His research interests include image processing, signal processing and object tracking.

B. M. Shahnewaz Abdullah was born on 29 December, 1993 in Bangladesh. He has received Bachelor of Science degree in Electronics and Communication Engineering from Khulna University of Engineering & Technology recently. His research interests are digital image processing, medical image watermarking.

How to cite this paper: Chandan Saha, Md. Foisal Hossain, B. M. Shahnewaz Abdullah,"Improving the Security of Spatial Domain Based Digital Image Watermarking using Chaotic Map and Cellular Automation", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.1, pp.51-58, 2016.DOI: 10.5815/ijigsp.2016.01.06

