I.J. Information Technology and Computer Science, **2018, 12, 27-32**
Published Online December 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2018.12.04

Quantum-Dot Cellular Automata based Fragile Watermarking Method for Tamper Detection using Chaos

Turker Tuncer
Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: turkertuncer@firat.edu.tr

Sengul Dogan
Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: sdogan@firat.edu.tr

Received: 12 October 2018; Accepted: 18 November 2018; Published: 08 December 2018

***Abstract*—**Fragile watermarking techniques have been widely used in the literature for tampered areas localization and image authentication. In this study, a novel quantum-dot cellular automata based fragile watermarking method for tampered area localization using chaotic piecewise map is proposed. Watermark generation, embedding, extraction and tampered area localization phases are consisted of the proposed quantum dot cellular automata and chaos based fragile watermarking method. In the watermark generation phase, quantum dot cellular automata and piecewise map which is a chaotic map are utilized. A block based method is utilized as authentication values embedding and extraction phases. To detect tampered areas, generated watermark and extracted watermark are compared. Also, block counters are used to tamper detection. In order to evaluate this method, capacity, imperceptibility and image authentication ability were utilized as performance metrics and the results of these metrics clearly illustrated that the presented method is suitable for image authentication and tamper detection.

***Index Terms*—**Fragile watermarking, quantum-dot cellular automata, chaotic maps, tamper detection, information security.

I. Introduction

Internet usage is common and cheap nowadays. People share a lot of data using internet-connected smartphones every day. Identification of these data is an important research area of today [1]. Watermarking is used to determine the ownership of the electronic medias. A watermarking system is given Fig. 1 [2] [3].

Watermark methods can be classified as follows [4]:

- Document type: Image, video, text, voice, audio, etc.
- Information variation: blind, half-blind, non-blind
- Human perception: invisible, visible
- Domain: transformation, spatial

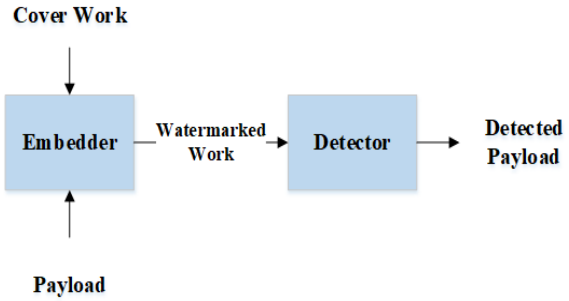

Fig.1. The general graphical outline of the watermarking model.

These methods have been varied according to the purpose of the watermarking in the literature. For example, in determining the owner of the data, it may be desirable that the marker be visible or invisible. At the same time, the user may prefer to image or text as marker [5] [6] [7].

It is desirable that a watermarking algorithm be resistant to attack so that the marker on the watermarked object is preserved. watermark embedding techniques are designed in literature [8] [9]. In the image watermarking applications, image is most used media in the literature. Arora et al. [10] suggested a hybridized watermarking technique. The marker was embedded to both spatial domain and frequency domain using Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) in their proposed method. Seetha et al. [11] presented a watermarking techniques for Drug's images. This method involved transparent digital watermarking techniques by using Alpha Channels and Alpha Blending techniques. In order to measure the durability of the method, the crop attack was performed in curve, brightness, contrast, invert and color balance. Xie et al. [12] suggested a new technique to prevent counterfeiting for QR codes. In their watermarking method, DWT was used to separate into non-overlapping rectangular areas.

The marker was embedded to multi-channel in cover image. Roy et al. [13] analyzed the impact of attacks in watermarking techniques and a robust watermarking method was proposed to increase robustness against this attack. Moosazadeh and Ekbatanifard [14] proposed a robust watermarking techniques for images. In their method, YCoCg-R color space, Arnold transform map and Discrete Cosine Transform (DCT) were used to increase robustness. YCoCg-R color space and DCT provided robustness and Arnold transform ensured security of this method.

A. Motivation and Contributions

In this study, a novel quantum-dot cellular automata and chaos based fragile watermarking method for tampered area localization.

The contributions of this paper are given as below.

- The quantum computation is a popular research area for information technologies. In this paper, quantum dot cellular automata are used to watermark generation phase of an image authentication method. Quantum dot cellular automata generally used for CMOS technologies. The polarization equation of the Quantum-dot cellular automata is used for watermark generation. In this view, this paper presents the first Quantum-dot cellular automata based fragile watermarking method for image authentication as we know.
- In order to provide security of the proposed method chaotic maps are used to encrypt watermark. In this work, quantum and chaos are used together and they provided to present a successful image authentication method.

B. Organization

The organization of the rest of this article is given as follows. The quantum-dot cellular automata are presented in Section 2, the piecewise chaotic map is given in the Section 3, the proposed method is explained in Section 4, experimental results are discussed in the Section 5, conclusions and recommendations are given in Section 6.

II. Quantum-Dot Cellular Automata

Quantum-dot Cellular Automata (QCA) have been presented for electronic circuits and CMOS technologies. QCA consists of square shapes (cells) and each of them is nano-sized and a QCA cell consists of 4 quantum dots. These dots occupied by a pair of electrons and these placed diagonal due to coulomb repulsion. To measure this alignment, Eq. 1 is used [15].

$$P = \frac{p_1+p_3-p_2-p_4}{p_1+p_2+p_3+p_4} \quad (1)$$

Where P measure polarity and pi are probability of presence an electron in quantum cell. The QCA cells samples are shown in Fig. 2 [16].

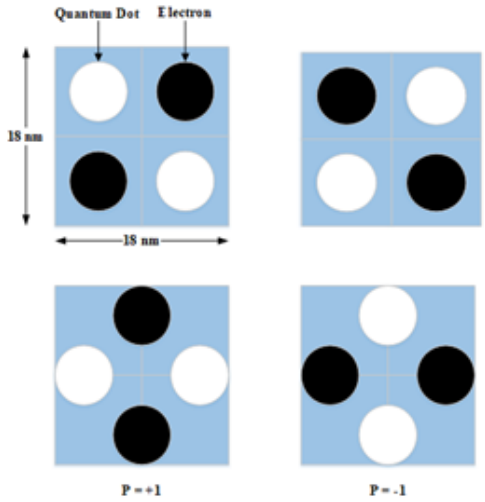

Fig.2. The samples of quantum cells.

In this paper, QCA is used for watermark generation.

III. Piecewise Linear Chaotic Map

Piecewise linear chaotic map (PLCM) is one of the widely used chaotic map in the literature. Chaos is very popular research area and it uses in optimization, cryptography, SBOX generation, random number generation, etc. Therefore, PLCM utilized as a pseudo random number generator (PRNG) for diffusion in this paper. The mathematical definition of the PLCM is given as below [17].

$$x_{n+1} = F(x_n, p) = \begin{cases} \frac{x_n}{p}, 0 \le x_n < p \\ \frac{x_n - p}{0.5 - p}, p \le x_n < 0.5 \\ 0, x_n = 0.5 \\ F(1 - x_n, p), 0.5 < x_n < 1 \end{cases} \quad (2)$$

Where p is piecewise value and p= (0,0.5), x_0 is starting value and x_0= (0,1). F represents four segmented PLCM function.

IV. The Proposed Fragile Watermarking Method

In this paper, a novel QCA and PLCM based fragile watermarking method is presented. The components of the proposed method are authentication values (watermark) generation, embedding, extraction and tampered area localization. They are explained in the sub-sections.

A. Watermark Generation

In this phase, QCA and PLCM used for watermark generation. Firstly, 2MSBs (most significant bit) are calculate for each pixel and probability of these values are calculated as using histogram. Then, secondary image is created by using these probabilities and secondary image is divided into 2 x 2 size of non-overlapping block to create a quantum cell. To calculate polarity of each cell,

Eq. 1 is used and polarities are normalized. After that, PLCM is utilized as PRNG and 2 bits values are generated. The generated random values and normalized polarities are XOR in diffusion section to generate watermark. The steps of the proposed watermark generation are given as below.

Step 1: Load cover image.

Step 2: Calculate 2MSBs of the cover image.

$$MI = \left\lfloor \frac{CI}{64} \right\rfloor \quad (3)$$

Step 3: Divide MI into 2 x 2 sized non-overlapping blocks

Step 4: Calculate polarity of each block using QCA and Eq. 1.

Step 5: Create secondary image using Eq. 4.

$$SI = round(3\frac{P - P_{min}}{P_{max} - P_{min}}) \quad (4)$$

Step 6: Generate random numbers using Eq. 2.

Step 7: Generate watermark using Eq. 5.

$$wm = SI \oplus rv \quad (5)$$

Where wm is watermark, SI is secondary image, rv randomly generated values.

B. Watermark Embedding

In this study, block based watermark embedding algorithm is used. To embed watermark, 2 x 2 size of blocks are utilized. The block based methods improve fragility and imperceptibility of the watermarking. The pseudo code of the watermark embedding procedure is illustrated in Algorithm 1 [17].

Algorithm 1. Pseudo code of the block based watermark embedding method.

Input: Cover image (CI) with size of M x N, watermark (wm) size of M/2 x N/2,
Output: Watermarked image (WI) with size of M x N.

```
WI = ⌊CI/2⌋ x 2
row=1;
for i=1 to M step by 2 do
    col=1;
    for j=1 to N step by 2 do
        value = wm_{row,col}
        r = ⌊value/2⌋;
        c = value (mod 2)
        if WI_{i+r,j+c} > 0 then
            WI_{i+r,j+c} = WI_{i+r,j+c} − 1;
        else
            WI_{i+r,j+c} = WI_{i+r,j+c} + 1;
        endif
        c=c+1;
    endfor j
    r=r+1;
endfor i
```

C. Watermark Extraction

In order to watermark extraction, a block based method is presented. The pseudo code of the proposed method is given as Algorithm 2 [18].

Algorithm 2. Pseudo code of the block based watermark extraction method.

Input: Cover image (WI) with size of M x N
Output: Watermarked (wm) with size of M/2 x N/2.

```
WI = ⌊CI/2⌋ x 2
row=1;
for i=1 to M step by 2 do
    col=1;
    for j=1 to N step by 2 do
        counter = 0;
        for k=0 to 1 do
            for l=0 to 1 do
                if WI_{i+k,j+l} (mod 2) = 1 then
            wm_{r,c} = counter;
            break;
        endif
        counter=counter+1;
        endfor l
    endfor k
    c=c+1;
endfor j
r=r+1;
endfor i
```

D. Tamper Detection

In order to tampered area localization, firstly control counters are used. For each block, 3 pixels must be even and a pixel must be odd. Then, watermark generation and watermark extraction algorithm are implemented. To detect tampered areas, extracted and generated watermarks are matched. Steps of the tamper detection algorithm of the QCA and PLCM based watermarking method.

Step 1: Divide watermarked image into sized non-overlapping blocks.

Step 2: Count even and odd pixels and detect tampered areas using Eq. 6.

$$TI_{i:i+1,j:j+1} = \begin{cases} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, counter_{even} = 3 \; and \; counter_{odd} = 1 \\ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, counter_{even} \neq 3 \; or \; counter_{odd} \neq 1 \end{cases} \quad (6)$$

Step 3: Apply watermarking generation algorithm to watermarked image.

Step 4: Extract watermark from watermarking image using Algorithm 2.

Step 5: Detect tampered areas using Eq. 7.

$$TI_{i:i+1,j:j+1} = \begin{cases} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, ew = gw \\ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, ew \neq gw \end{cases} \quad (7)$$

Where *ew* is extracted watermark and *gw* is generated watermark [19].

V. Experimental Results

In order to measure performance metrics of the proposed method, the test image which are shown in Fig. 3 and capacity, imperceptibility and image authentication ability are used.

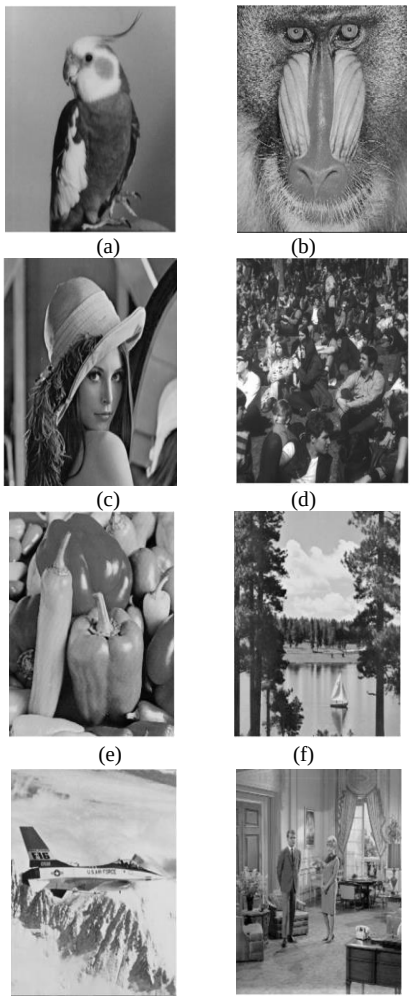

Fig.3. The gray level test images (a) Parrot, (b) Baboon, (c) Lena, (d) Crowd, (e) Peppers, (f) Sailboat, (g) F16, (h) Couple

Size of these test images is 512 x 512 and these are gray level images. The performance metrics are given as below.

A. Capacity

Capacity is one of the most used performance metric for image authentication and watermarking method. In this paper, 2 bits watermark is embedded into 2 x 2 sized non-overlapping blocks. Therefore, the capacity of the proposed QCA and PLCM method is calculated as $\frac{2 \text{ x } \frac{M}{2} \text{ x } \frac{N}{2}}{M \text{ x } N} = 0.5$ bit per pixel (bpp) [20].

B. Imperceptibility

To measure imperceptibility, peak signal-to-noise ratio (PSNR) is generally used and mathematical description of the PSNR are given as Eq. 8 [21].

$$PSNR = 10 \log_{10} \frac{255^2 \, x \, M \, x \, N}{\sum_{i=1}^{M} \sum_{j=1}^{N} (CI_{i,j} - WI_{i,j})^2} \quad (8)$$

In this paper, block based watermark embedding algorithm is utilized as data hiding function. This algorithm uses ±1 operator for embedding watermark and Therefore, the theoretical worst PSNR is calculated as $10 \log_{10} \frac{255^2}{1} = 48.13$. The practical PSNR results were obtained from test images and imperceptibility results of the 8 gray level test images are listed in Table 1.

Table 1. PSNR Values of the Proposed QCA and PLCM based Fragile Watermarking Method.

Images	**PSNR**
Parrot	51.19
Baboon	51.22
Lena	51.18
Crowd	51.17
Peppers	51.18
Sailboat	51.20
F16	51.17
Couple	51.16
Average	**51.18**

To better understand to visual quality effectiveness of the proposed method, a few previously presented methods in the literature were used to obtain comparisons. The comparison results were listed in Table 2.

Table 2. The imperceptibility comparison results

	Chang et al.'s method [22]	Wu and Lin's 1 Scheme [23]	Wu and Lin's 2 Scheme [23]	Tuncer's method [24]	The proposed method
Lena	42.28	51.10	51.15	**51.18**	**51.18**
Baboon	42.31	51.10	51.15	51.17	**51.22**
Peppers	42.30	51.12	51.12	51.17	**51.18**
F16	42.27	51.14	51.14	**51.17**	**51.17**

Table 2 demonstrated that the proposed method has best visual quality among the others and these results proved the effectiveness of the proposed method in view visual quality.

C. Image Authentication Ability

The most important evaluation criteria are image authentication ability for image authentication methods. In order to measure this metric, detection rate (DR) is used and the mathematical description of the DR is given as Eq. 9.

$$DR = \frac{Detected \; pixels}{All \; modified \; pixels} \quad (9)$$

To evaluate this capability, an attack which is shown in Fig.4 was used.

Fig.4. The attack for evaluation image authentication capability (a) original image (b) attacked image (c) tampered area

In this attack, DR is calculated as 0.94.

The capacity, imperceptibility and image authentication ability results are clearly illustrated that the QCA and PLCM based method is successful fragile watermarking method.

VI. Conclusions and Recommandations

In this paper a novel quantum based watermarking method is presented for tampered areas localization using chaos. This method uses QCA and PLCM for watermark generation and generated watermarks are embedded into images using block based data hiding method. Block based data hiding method improves imperceptibility and fragility. The proposed method is the first method to use quantum and chaos together up to now. In the experimental results section, payload, imperceptibility and image authentication were used to evaluate performance of this method and this section showed that, this method has high capacity, visual quality and image authentication ability.

In the future studies, novel chaotic quantum based image authentication, data hiding and watermarking methods may be presented in the literature.

References

[1] V. Potdar, S., Han, E. Chang, “A survey of digital image watermarking techniques”. In 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), pp. 709-716, IEEE, 2005.

[2] C. Honsinger, Digital watermarking. Journal of Electronic Imaging, 11(3), 414, 2002.

[3] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, “Digital watermarking and steganography”. Morgan kaufmann, 2007.

[4] S. Dogan, T. Tuncer, E. Avci, A. Gulten, “A robust color image watermarking with Singular Value Decomposition method”. Advances in Engineering Software, 42(6), pp.336-346, 2011.

[5] F. Hartung, B. Girod, “Watermarking of uncompressed and compressed video”. Signal processing, 66(3), pp. 283-301, 1998.

[6] M. Barni, F. Bartolini, V. Cappellini, A. Piva, “A DCT-domain system for robust image watermarking”. Signal processing, 66(3), pp. 357-372, 1998.

[7] C. S. Collberg, C. Thomborson, “Watermarking, tamper-proofing, and obfuscation-tools for software protection”. IEEE Transactions on software engineering, 28(8), pp. 735-746, 2002.

[8] C. W. Tang, H. M. Hang, “A feature-based robust digital image watermarking scheme”. IEEE transactions on signal processing, 51(4), pp. 950-959, 2003.

[9] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, F. Davoine, “Digital watermarking robust to geometric distortions”. IEEE Transactions on Image Processing, 14(12), pp. 2140-2150, 2005.

[10] S. M. Arora, “A DWT-SVD based Robust Digital Watermarking for Digital Images”. Procedia Computer Science, 132, 1441, 2018.

[11] C. Seetha, S. Goollawattanaporn, C. Tanprasert, “Transparent Digital Watermark on Drug's Images”. Procedia Computer Science, 21, pp. 302-309, 2013.

[12] R. Xie, C. Hong, S. Zhu, D. Tao, “Anti-counterfeiting digital watermarking algorithm for printed QR barcode”. Neurocomputing, 167, 625-635, 2015.

[13] R. Roy, T. Ahmed, S. Changder, “Watermarking through image geometry change tracking”. Visual Informatics, 2018.

[14] M. Moosazadeh, G. Ekbatanifard, “An improved robust image watermarking method using DCT and YCoCg-R color space”. Optik-International Journal for Light and Electron Optics, 140, pp. 975-988, 2017.

[15] M. B. Khosroshahy, M. H. Moaiyeri, S. Angizi, N. Bagherzadeh, K. Navi, “Quantum-dot cellular automata circuits with reduced external fixed inputs”. Microprocessors and Microsystems, 50, pp. 154-163, 2017.

[16] S. Seyedi, N. J. Navimipour, “An optimized design of full adder based on nanoscale quantum-dot cellular automata”. Optik-International Journal for Light and Electron Optics, 158, pp. 243-256, 2018.

[17] Y.F. Wang, M.D. Xie, A.M. Ji, Research on a Piecewise Linear Chaotic Map and Its Cryptographical Application, Fourth International Conference on Fuzzy Systems and

Knowledge Discovery (FSKD 2007), 24-27 Aug. 2007, Haikou, China.
[18] T. Tuncer, Y. Sönmez, Block based data hiding method for images, European Journal of Technique, (2017) 7(2) 85-95.
[19] T. Tuncer, A probabilistic image authentication method based on chaos, Multimedia Tools and Applications, 2018, https://doi.org/10.1007/s11042-017-5569-x.
[20] S. K. Lee, Y. H. Suh, Y. S. Ho, Reversiblee image authentication based on watermarking. In Multimedia and Expo, 2006 IEEE International Conference on IEEE, pp. 1321-1324, 2016.
[21] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform". IEEE transactions on image processing, 13(8), pp. 1147-1156, 2004.
[22] C.C. Chang, Y.P. Hsieh, C. H. Lin, Sharing secrets in stego images with authentication. Pattern Recogn, 41(10):3130–3137, 2008.
[23] W. C. Wu, Z. W. Lin, SVD-based self-embedding image authentication scheme using quick response code features. J Vis Commun Image R 38:18–28, 2016.
[24] T. Tuncer, A probabilistic image authentication method based on chaos. Multimedia Tools and Applications, 1-18, 2018.

Authors' Profiles

Turker TUNCER was born in Elazig, Turkey, in 1986. He received the B.S. degree from the Firat University, Technical Education Faculty, Department of Electronics and Computer Education in 2009, M.S. degree in telecommunication science from the Firat University in 2011 and Ph.D. degree department of software engineering at Firat University in 2016. He works as research assistant Digital Forensic Engineering, Firat University. His research interests include data hiding, image authentication, cryptanalysis, cryptography, image processing.

Sengul DOGAN received her Ph.D degree in Electrical and Electronic Engineering from the University of Firat, Elazig, Turkey, in 2011. She is currently an Assistant Professor in the Digital Forensics Engineering Department of Firat University. Her research interests cover Data Hiding, Information Security, Digital Forensics, Image Processing and Optimization Techniques.

How to cite this paper: Turker Tuncer, Sengul Dogan, "Quantum-Dot Cellular Automata based Fragile Watermarking Method for Tamper Detection using Chaos", International Journal of Information Technology and Computer Science(IJITCS), Vol.10, No.12, pp.27-32, 2018. DOI: 10.5815/ijitcs.2018.12.04