I. J. Computer Network and Information Security, **2018, 6, 60-67**
Published Online June 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.06.06

Analysis of CRT-based Watermarking Technique for Authentication of Multimedia Content

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

Received: 07 March 2018; Accepted: 04 May 2018; Published: 08 June 2018

Abstract—Watermarking techniques are widely used for image authentication and copyright protection. Weaknesses of the "A novel CRT-based watermarking technique for authentication of multimedia contents," [12] are analyzed in this study. 4 attacks are proposed to analysis of this method. These attacks are most significant bits, modulo number, tamper detection probability calculation and algorithm analysis attacks. The proposed attacks clearly show that the crt-based method is a data hiding method but this method is not used as image authentication method. The title of presented method in Ref. [12] include "authentication" but the authors of Ref. [12] evaluated their method in view of copyright protection. The fragile watermarking methods for image authentication should consist of watermark generation, watermark embedding, watermark extraction and tamper detection but Ref. [12] has no watermark generation, tamper detection and tampered area localization algorithms. The proposed attacks are demonstrated that Ref. [12] cannot be utilized as an image authentication method and Ref. [12] is not effectively coded.

Index Terms—Watermarking analysis, Chinese remainder theorem, Image authentication, Algorithm Analysis, Watermarking.

I. Introduction

Nowadays, multimedia data transmissions and digital communication techniques are commonly used. Multimedia data consists of various data like text, image, sound, video, etc. Multimedia data transmission is generally used in areas such e-learning, web conference, social media, mobile applications, biomedical engineering [1-5].

Data hiding algorithms are generally used in information security use multimedia data. Data hiding is divided into two main categories. These are steganography and digital watermarking. The main purpose of the steganography to embed secret message into a seemingly innocent multimedia data in order to provide security of the data transmission. The digital watermarking methods have two main aims. These are copyright protection and authentication. In order to provide copyright protection, robust watermarking techniques are used. To provide robustness, quantization index modulation (QIM) and frequency transformations are generally used. Fragile and semi-fragile watermarking techniques are used to image authentication. Image authentication methods consist of watermark generation, watermark embedding, watermark extraction and tamper detection sections. In addition, an image authentication method should detect any modifications and should robust against cryptanalysis attacks. To provide image authentication by using watermarking, quick response (QR) codes, sparse coding, fuzzy, singular value decomposition (SVD), wavelet transformations, clustering, Chinese remainder theorem (CRT), etc., methods were used in the literature [1-12].

1.1. Problem Definition

In order to evaluate fragile watermarking method, cropping, collage and copy move attacks have been used in the literature. However, these attacks are not sufficient to evaluate robustness of an image authentication method against cryptanalysis. There is no standard to evaluate fragile watermarking for image authentication in the literature. Therefore, many methods that are not robust against cryptanalysis attacks were presented in the literature. One of them is Patra et al.'s [12] image authentication method. In this paper, Patra et al.'s [12] method is analyzed using 4 cryptanalysis attacks. These attacks are most significant bits (MSB), modulo value, tamper detection probability calculation and algorithm analysis.

1.2. Contributions

Technical contributions of this paper lies in below.

- 4 attacks are proposed to evaluate Patra et al.'s [12] method in view of cryptanalysis. These attacks can be generalized and used in all fragile watermarking methods.
- Algorithm analysis of the Patra et al.'s [12] method was performed and optimum data hiding algorithm based on CRT is presented in this paper.

1.3. Organizations

Organization of this paper is given as follows. Related Works are mentioned in Section 2, Description of the

Patra et al.'s method [12] is given in Section 3, Analysis of CRT based Watermarking Technique for Multimedia Content Authentication is presented in Section 4, Conclusions and Recommendations is given in Section 5.

II. Related Works

In this section, some of the image watermarking, data hiding and watermarking cryptanalysis methods previously proposed in the literature are mentioned. Patra et. al. [12] proposed a CRT-based watermarking technique for image authentication. This method used CRT for image authentication and compared to SVD based watermarking technique. Patra et al. [13] presented CRT based watermarking technique in Discrete Cosine Transform (DCT) domain for JPEG compression. Nguyen et al. [14] suggested a reversible image authentication method in the Discrete Wavelet Transform (DWT) domain. This method has tamper detection ability. Zhou et al. [15] proposed binocular image authentication and tamper detection method. This scheme consists of data embedding, image authentication and tamper detection steps. This method was applied on stereoscopic images. Hu et al. [16] proposed an image authentication method in order to detect tampered region for demosaicking with the reversibility preserving property. This method suggested for RGB image authentication. Qi and Xin [17] presented semi-fragile watermarking technique for image authentication using singular value decomposition (SVD). This method used Mersenne Twister encryption algorithm to generate secure watermark. LL (Low- Low) sub-band was used to embed watermark. Caragata et al. [18] proposed two attacks on Teng et al.'s [19] method. Both attacks allowed the attacker to apply valid watermarks on tampered images, therefore rendering the watermarking scheme is useless. Caragata et al. [20] suggested a cryptanalysis of the Chaotic watermarking scheme for JPEG images authentication [21] using markov chains. Li et al. [22] analyzed a block based binary image watermarking technique was proposed by Zu et al. [23]. In Zu et al.'s method [23], authors used chaotic map to generate encryption key and Li et al. [22] applied modulo based XOR attack on the Zu et al.'s [23] method and they demonstrated that, Zu et al.'s method [23] did not provide information security and this method can be manipulated by using the presented attack. Ahmad et al. [24] proposed a robust watermarking method in wavelet domain. In order to provide robustness against geometrical and frequency attacks, three level DWT were used with alpha blending embedding method. Bansal et al. [25] presented a steganography method based on eight queens data hiding. Authors presented a robust steganography method against steganalysis methods by using this method. Dogan [26] presented a chaotic data hiding method. This method used chaotic map and pixel pairs. The chaotic map was utilized as Pseudo Random Number Generator (PRNG) and pixel pairs were utilized for data hiding. Tiwari and Sharma [27] presented a survey about semi-fragile image watermarking methods.

III. Description of CRT-based Watermarking Technique for Authentication of Multimedia Content

In this section, the analyzed method [12] is explained. Patra et al. [12] presented a CRT based image authentication method and this image authentication technique consists of two parts. These are watermark embedding and watermark extraction steps. In Patra et al.'s [12] article, authors claimed that the presented method was an image authentication method but this method have no tamper detection and watermark generation algorithms and they didn't present any experimental results about tamper detection and image authentication ability. Their method have watermark embedding and watermark extraction algorithms. The watermark embedding steps of the CRT-based watermarking technique are given below.

E1. Divide cover image into 8 x 8 size of non-overlapping blocks and select a random pixel 'X' using Pseudo Random Number Generator (PRNG) within each block.

E2. Convert 'X' to binary form.

E3. Calculate a 'Z' value from 6 least significant bits (Z=[0,63]) of 'X'.

E4. Calculate 'Y' value (Y={0,64,128,192}) using the 2 most significant bits (2MSBs) of X .

E5. Select two pair-wise co-prime numbers 'M1' and 'M2'.

E6. Calculate 'R1' and 'R2' using Eq. 1.

$$R_i = \mathrm{Z} \pmod{M_i} \tag{1}$$

E7. To embed 1, Z needs to be modified to according to condition in Eq. 2.

$$R_1 \geq R_2 \tag{2}$$

E8. In order to embed 0, Z needs to be modified to according to condition in Eq. 3.

$$R_1 < R_2 \tag{3}$$

E9. Reconstruct stego-pixel by using Eq. 4.

$$X' = Y + Z \tag{4}$$

E10. Repeat E1-E9 until size of watermark.

Block diagram of the watermark embedding is shown in Fig. 1.

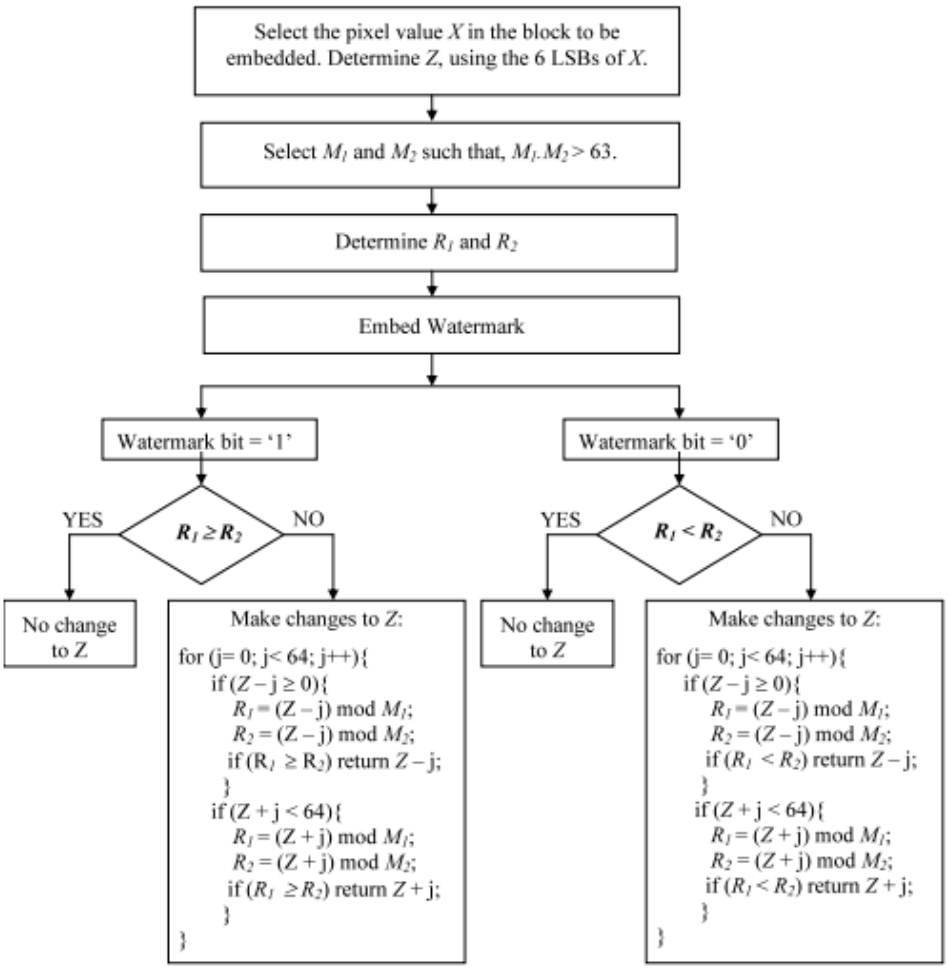


Fig.1. Block Diagram of the Watermark Embedding.

The extraction steps of the CRT-based watermarking method are given below.

X1. Use seed values to obtain random numbers.
X2. Use M_1 and M_2 pairwise co-prime numbers.
X3. Determine embedding pixel by using random numbers.
X4. Calculate Z by using Eq. 5.

$$Z = \left\lfloor \frac{X}{4} \right\rfloor \quad (5)$$

X is intensity of pixel and Z is 6LSBs of X.

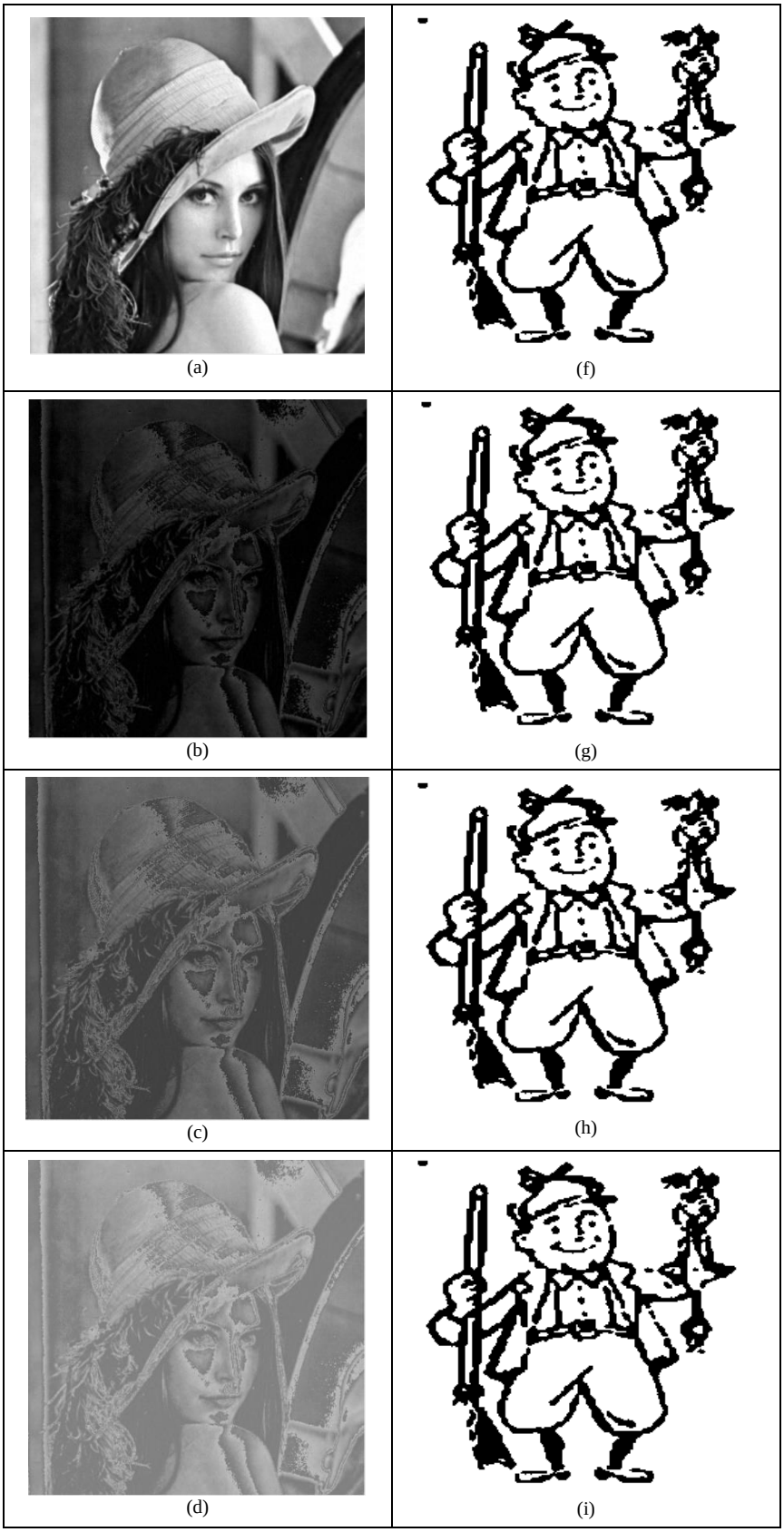
X5. Calculate R_1 and R_2 by using Eq. 1.
X6. If $R_1 \geq R_2$, watermark bit is 0, otherwise watermark bit is 1.
X7. Repeat X3-X6 steps until size of watermark.

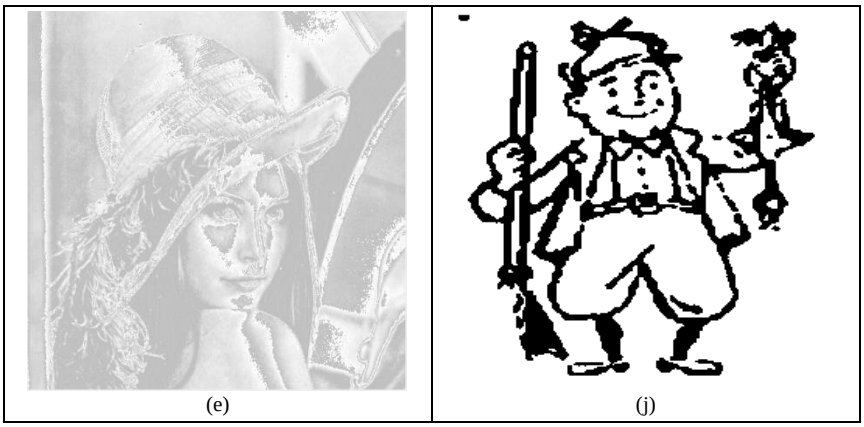
IV. Analysis of CRT-based Watermarking Technique for Authentication of Multimedia Content

An image authentication method should be fulfilled sensitivity, tolerance, tamper detection, storage and visibility criteria [28]. However, the most of fragile watermarking method in the literature are not evaluate in view of cryptanalysis. This case clearly demonstrate that classical evaluation criteria are insufficient for image authentication in fragile watermarking methods because the classical criteria use statically moments such as PSNR (Peak Signal Noise-To-Ratio), NCC (Normalized Cross Correlation), BER (Bit Error Rate), FPR (False Positive Rate), SSIM (Structural Similarity), Q (Quality), etc. In this paper, Patra et al.'s [12] method is re-evaluated in view of cryptanalysis and the presented attacks show that CRT-based watermarking technique cannot authenticate an image because CRT is modulo function. The most important weakness of modulo based data embedding functions are not to have image authentication ability against to modulo based attacks. Furthermore, Patra et al.'s method [12] uses 6LSBs of the pixel values to embed watermark. 2MSBs of pixels are not used to create authentication bit. This situation is highlighted significant weaknesses. This paper shows 4 weakness of crt-based fragile watermarking algorithm. These are given below.

A1. In Ref. [12], the authors used 6LSBs for data embedding and 2MSBs of the image is not affected watermark. In this case, we can modify 2MSBs of the pixels. In this paper, 2MSBs of

watermarked image are attacked and watermark is extracted lossless. In this attack, 0, 1, 2 and 3 are set to 2MSBs of all the pixels respectively but watermark is extracted lossless. This attack is given in Fig. 2.

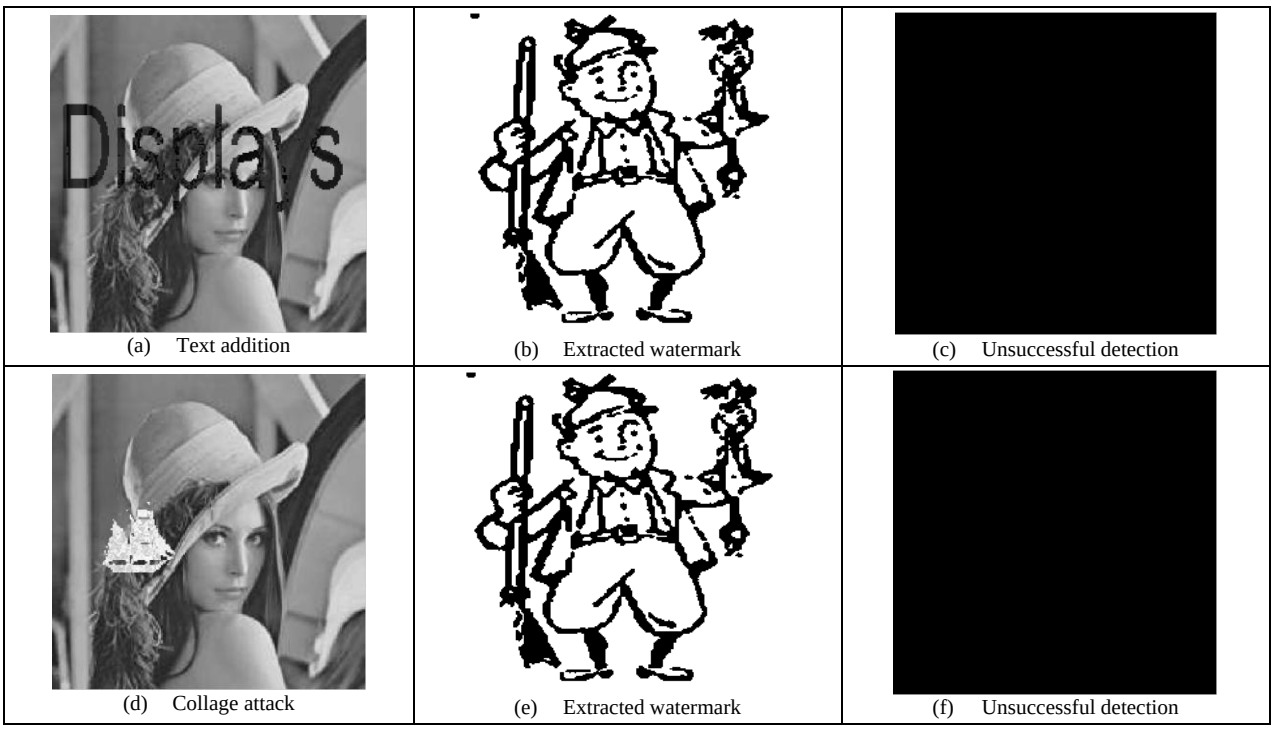




(e) (j)

Fig.2. Attacked Images using A1. (a) Original Watermarked Image (b) The Watermarked Image of which 2MSBs set to (00)2 (c) The Watermarked Image of which 2MBSs set to (01)2 (d) The Watermarked Image of which 2MBSs set to (10)2 (e) The Watermarked Image of which 2MBSs set to (11)2 (h-j) Extracted Watermark from a-e.

Additionally, meaningful bits attacks that are text addition and binary collage attacks were applied on the watermarked image. The result of this implementation is shown in Fig. 3.



(a) Text addition (b) Extracted watermark (c) Unsuccessful detection

(d) Collage attack (e) Extracted watermark (f) Unsuccessful detection

Fig.3. Undetected Modification on a Watermarked Image

A2. In Patra et al.'s [12] method, M_1 and M_2 should be co-primes and $M_1 \cdot M_2$ shuld be greater than 63, but the condition of both M_1 and M_2 must be smaller than 63 is missing. In Patra et al.'s method [12], there is no information about this situation. Pixel value cannot be modified if $M_1>63$ or $M_2>63$. Because this method used 6LSBs of a pixel for watermark embedding. This case was not determined in Patra et al.'s [12] paper.

A3. Tamper detection probability of Patra et al.'s [12] method is very low because this method used 6LSBs of a pixel in a 8 x 8 size of blocks for watermark embedding. The general equation of the tamper detection probability is given Eq. 6.

$$\Pr(Td) = \frac{1}{w \cdot h} \cdot \frac{6}{8} \quad (6)$$

Pr(Td) is tamper detection probability, *w* is width of sub-block, *h* is height of sub-block. In Patra et al.'s paper [12], 6LSBs of an 8 bit pixel were used. The 2MSBs were not utilised. Afterwards a single pixel in the block was used for watermark embedding. Thus, in case of an 8 x 8 sized block, the tamper detection probability is about 0.01171875. This value is very low for an image authentication method.

A4. In Para et al.'s method [12], it was claimed that

the watermark embedding algorithm is a fast algorithm, but complexity of the algorithm is $O(n^3)$. The watermark embedding algorithm presented in Patra et al.'s [12] article is not well optimised. An optimum watermark embedding algorithm belonging to Patra et al.'s method [12] is given in Algorithm 1.

Algorithm 1. Optimum Watermark Embedding Algorithm of CRT-Based Watermarking Technique for Authentication of Multimedia Content

Input: Cover image CI which size of W x H, b x b sized sub-blocks, random numbers *x1* and *y1* which size of $\frac{W}{b} x \frac{H}{b}$, watermark wm which size of $\frac{W}{b} x \frac{H}{b}$, m_1 and m_2 co-prime numbers which $m_1.m_2>63$ and $m_1<63$, $m_2<63$.
Output: Watermarked image WI which size of W x H

```
WI=CI;
row=0;
for i=1:b:W do
    col=0;
    for j=1:b:H do
        x=WI(i+x1(row+1,col+1),j+y1(row+1,col+1));
        t = ⌊x/64⌋;
        z= x (mod 64);
        r1=z (mod m1); r2=z (mod m2);
        if(wm(row+1,col+1)=1 and r1<r2) then
            d= m2-r2;
            if(z+d<64) then
                z=z+d;
            else
                z+d-m2;
            endif
        else if(wm(row+1,col+1)=0 and r1≥r2) then
            d= m1-r1;
            if(z+d<64) then
                z=z+d;
            else
                z+d-m1;
            endif
        endif
        WI(i+x1(row+1,col+1),j+y1(row+1,col+1))=64t+z;
        col=col+1;
    endfor
    row=row+1;
endfor
```

Algorithm 1 and Patra et al.'s method [12] embedding algorithms are the same. However, complexity of the Algorithm 1 is $O(n^2)$ while the complexity of Patra et al.'s embedding algorithm is $O(n^3)$. We can see that, embedding algorithm in Patra et al.'s method [12] has some flaws. This algorithm demonstrated that if the attackers add values which are smaller than d, Patra et al.'s [12] image authentication method cannot detect these values. Therefore, the attacker can apply the addition attack on the images. They also used the PRNG to select the watermarked pixels in the blocks, but they didn't give any information about PRNG used. Besides, in order to provide information security is not enough only using the PRNG.

V. Conclusions and Recommendations

There is no standard for fragile watermarking in the literature. Therefore, authors have used statistically metrics to evaluate their methods. However, these evaluation metrics is not sufficient for fragile watermarking evaluation in view of image authentication. The main problem of fragile watermarking method not used cryptanalytics approach. Patra et al.'s method [12] is analyzed in this article. 4 weaknesses of Patra et al.'s method [12] are found and they are demonstrated that Patra et al.'s method [12] cannot be used for image authentication. Modulo and bit attacks were used on watermarked image and tamper detection probability is calculated. In the Patra et al.'s [12] method, 6LSBs were utilized for data hiding and this method used 8 x 8 size of non-overlapping blocks. They used a pixel in the block. The first attack showed that this method does not detect attacks on the 2MSBs of the pixels. In the second attack, tamper detection probability of the Patra et al.'s [12] was calculated and the tamper detection probability was calculated approximately 1.2%. This is an unacceptable level. In the third attacks defined limits of modulo values. If M_1 and M_2 are selected bigger than 63. The watermark embedding process does not execute. The final attack is about algorithm analysis. The Patra et al.'s method was not coded optimally because complexity of the Patra et al.'s [12] method is $O(n^3)$ but the optimum time complexity of CRT based watermarking method is $O(n^2)$. The optimum code was shown in Attack 4. Also, the presented algorithm in Attack 4 demonstrated that, the Patra et al.'s method cannot detect some addition attacks. The results showed that Patra et al.'s method [12] was

easily cracked and it is not useful and not well optimized. Thus, this method does not use as a watermarking but can be used as a data hiding method.

In the future, the proposed attacks may be used to create a watermarking standard.

REFERENCES

[1] H.M. Al-Otum, Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique, J. Vis. Commun. Image Represent. 25 (2014) 1064–1081.

[2] C.S. Chan, An image authentication method by applying hamming code, Pattern Recogn. Lett. 32 (2011) 1679–1690.

[3] J.H. Chen, W.Y. Chen, C.H. Chen, Identification recovery scheme using quick response (QR) code and watermarking technique, Appl. Math. Inform. Sci. 8 (2014) 585–596.

[4] A. Tareef, A. Al-Ani, A highly secure oblivious sparse coding-based watermarking system for ownership verification, Expert Syst. Appl. 42 (4) (2015) 2224–2233.

[5] T. Tuncer, A probabilistic image authentication method based on chaos, Multimedia Tools and Applications (2018), 1-18.

[6] W.C. Wu, Z.W. Lin, An image content protection and tampering localization scheme using singular values, in: Proceedings of the 3rd International Scientific Conference on Engineering and Applied Sciences, Okinawa Japan, July 2015, pp. 238–247.

[7] W.C. Chen, M.S. Wang, A fuzzy c-means clustering-based fragile watermarking scheme for image authentication, Expert Syst. Appl. 36 (2009) 1300–1307.

[8] T. Tuncer, A novel image authentication method based on singular value decomposition, Journal of the Faculty of Engineering and Architecture of Gazi University, 32,3, (2017), 877-886.

[9] E. Avci, T. Tuncer, D. Avci, A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain. Arabian Journal for Science and Engineering, (2016), 1-9.

[10] T. Tuncer, E. Avci, Data Hiding Application with Gokturk Alphabet Based Visual Cryptography Method, Journal of the Faculty of Engineering and Architecture of Gazi University, Vol 31, No 3, pp. 781-789,2016.

[11] C. Qin, X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content",Journal of Visual Communication and Image Representation, 31 (2015),154-164.

[12] J. C. Patra, A. Karthik, C. Bornand, A novel CRT-based watermarking technique for authentication of multimedia contents, Digital Signal Processing 20,(2010), pp. 442–453.

[13] J. C. Patra, J.E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing 20,(2010), pp. 1597–1611.

[14] T.-S. Nguyen, C.-C. Chang, X.-Q. Yang, A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain, International Journal of Electronics and Communications (AEÜ), 70,(2016), pp.1055-1061.

[15] W. Zhou, L. Yu, Z. Wang, M. Wu, T. Luo, L. Sun, Binocular visual characteristics based fragile watermarking scheme for tamper detection in stereoscopic images, International Journal of Electronics and Communications (AEÜ), 70,(2016), pp. 77–84.

[16] Y.-C. Hu, C.-C. Lo, W.-L. Chen, Probability-based reversible image authentication scheme for image demosaicking, Future Generation Computer Systems, 62, (2016), pp. 92-103.

[17] X. Qi, X. Xin, A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, J. Vis. Commun. Image R., 30, (2015), pp. 312-327.

[18] D. Caragata, J. A. Mucarquer, M. Koscina, S. E. Assad, Cryptanalysis of an improved fragile watermarking scheme, International Journal of Electronics and Communications (AEÜ), 70, (2016), pp. 777-785.

[19] Teng L, Wang X, Wang X. Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme, International Journal of Electronics and Communications (AEÜ), (2013), 67(6),540–547.

[20] D. Caragata, S. E. Assad, M. Luduena, An improved fragile watermarking algorithm for JPEG images, International Journal of Electronics and Communications (AEÜ), 69, (2015), pp. 1783-1794.

[21] H. Wang, K. Ding, C. Liao, Chaotic watermarking scheme for authentication of JPEG images. In: International symposium on biometrics and security technologies. 2008. pp. 1–4.

[22] M. Li, J. Zhang, W. Wen, Cryptanalysis and improvement of a binary watermark-based copyright protection scheme for remote sensing images, Optik 125 (2014) 7231–7234.

[23] P. Zhu, F. Jia, J.L. Zhang, A copyright protection watermarking algorithm for remote sensing image based on binary image watermark, Optik 124 (2013) 4177–4181.

[24] A. Ahmad, G.R. Sinha, N. Kashyap, 3-Level DWT Image Watermarking Against Frequency and Geometrical Attacks, I.J. Computer Network and Information Security, 2014, 12, 58-63.

[25] A. Bansal, S.K. Muttoo, V. Kumar, Security against Sample Pair Steganalysis in Eight Queens Data Hiding Technique, I. J. Computer Network and Information Security, 2016, 8, 39-46.

[26] S. Dogan, A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map, I. J. Computer Network and Information Security, 2018, 1, 1-9.

[27] A. Tiwari, M. Sharma, Semifragile Watermarking Schemes for Image Authentication- A Survey, I. J. Computer Network and Information Security, 2012, 2, 43-49.

[28] R. Christian, D. Jean-Luc, A survey of watermarking algorithms for image authentication, EURASIP J. Appl. Signal Process., 6, (2002) 613–621.

Authors' Profiles

Türker 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.

How to cite this paper: Türker TUNCER,"Analysis of CRT-based Watermarking Technique for Authentication of Multimedia Content", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.6, pp.60-67, 2018.DOI: 10.5815/ijcnis.2018.06.06

