ISSN: 0067-2904

Image Content Verification based on DWT and Chaotic Map Watermarking

Dina Riadh Alshibani*, Zinah Sadeq
Department of Computer Science, College of Science, Al-Mustansiriyah University, Baghdad, Iraq.

Abstract

Image content verification is to confirm the validity of the images, i.e. . To test if the image has experienced any alteration since it was made. Computerized watermarking has turned into a promising procedure for image content verification in light of its exceptional execution and capacity of altering identification.

In this study, a new scheme for image verification reliant on two dimensional chaotic maps and Discrete Wavelet Transform (DWT) is introduced. Arnold transforms is first applied to Host image (H) for scrambling as a pretreatment stage, then the scrambled host image is partitioned into sub-blocks of size 2×2 in which a 2D DWT is utilized on each sub-block to produce corresponding sub-block of DWT coefficients (LL, LH, HL and HH). Meanwhile, watermark image is encrypted using the introduced chaos-based enciphering algorithm. The watermarked image is obtained by updating the approximation coefficients (LH sub-band) of each 2×2 sub-block of DWT coefficients of the host image with the enciphered watermark image bits. Different investigational tests are performed to evaluate the act of the introduced approach. Investigation results clearly present that the proposed approach can detect and localize editing attacks perfectly.

Keywords: Index Terms— Arnold Transform, DWT, Duffing Map, Image Watermarking.

التحقق من محتوى الصورة باستخدام العلامة المائية المرتكزة على الخرائط الفوضوية و تحويل المويجات المنفصل

دينا رياض، زينة صادق
قسم علوم الحاسبات، كلية العلوم، الجامعة المستنصرية، بغداد، العراق.

الخلاصة

نظرا لانتشار الصور على الانترنت و اتاحتها للجميع اصبح من الضروري وجود طرق لغرض التاكد من صحة الصور و لاختبار ما إذا كانت الصورة قد شهدت أي تغيير منذ أن تم صناعتها.

من احدى اهم الطرق المستخدمة لهذا الغرض هي العلامة المائية. في هذا البحث تم اعتماد طريقة حديثة لاختبار الصور المنقوله من حيث التاكد من صحة المعلومات المتضمنة بالصورة تعتمد هذه الطريقة على الخرائط الفوضية ثنائية الأبعاد وتحويل المويجات المنفصلة (DWT).

تعمل الطريقة المقترحة بالتوازي من حيث المعالجة على الصورة الغلاف (Host Image) و الصورة المتضمنه (Watermark image) .حيث يتم تطبيق ارنولد ترانسفورم على صورة الغلاف كنوع من المعالجة الاولية لغرض خلط معلومات الصورة يعقب تلك العملية تقسيم الصورة الى مجموعه من البلوك الغير متداخلة

*Email: dinashibani@uomustansiriyah.edu.iq

بحجم 2*2 و من ثم تطبيق وتحويل المويجات المنفصلة على كل بلوك بالجهة المقابله و بنفس الوقت فان الصورة المتضمنه يتم تشفيرها باستخدام خوارزمية مقترحة تعتمد على الخرائط الفوضوية تعبق هذه المعالجة اخفاء الصورة المتضمنه بالغلاف من خلال تغيير و تحديث LH لكل بلوك من الغلاف ببتات الصورة المتضمنه. يتم إجراء اختبارات تحقيقية مختلفة لتقييم فعل الطريقة المقترحة. نتائج التحقيق تجعل من الواضح أن الطريقة المقترحة قادرة على كشف التلاعبات التي من الممكن حدوثها في الصورة الغلاف.

1. Introduction

The speed expansion of the internet technologies has made available huge amounts of data to anyone with internet access. With the assistance of effective image handling devices, then the digital data could be controlled and altered without leaving any trace on the original image. The straightforwardness and degree of such controls underline the necessity for image validation strategies in applications where verification and validity of the image substance is fundamental. As a result, in the earlier period, a range of verification methods based on digital signature has been introduced for confirming the validity of the image content and to keep them free from any form of exploitation. In signature-based methods, the significant downside is that they can identify any altered with an image, but without finding the locales of these changes. So, to overcome of this difficulty, computerized fragile watermarking based methods have been introduced for image content verification [1].

Verification and honesty confirmation are the main reasons behind utilizing computerized fragile watermarks [2]. A safe verification system is useful in demonstrating that no alteration or modification has taken place throughout conditions where the trustworthiness of an image can be investigated [3]. It presents an assurance that the image has not been altered or modified and also derived from the precise exporter. In fragile watermark technique, the valuable areas where the content is very significant that it requires verification to ensure that it has not been edited, spoiled or distorted.
For image content verification several image watermarking algorithms have been introduced for surveying. Xiang Zhou et al. [4] introduced a semi-fragile watermarking using wavelet transform to achieve image content verification. Their system achieves a good perceptibility and tolerant to compression of lossy type. Detection of watermark is violated by malicious modified of an image. Also, Illegal altered blocks are discovered in the precise locations in this scheme. HongJie He et al. [5] proposed a fragile watermarking scheme using wavelet transform to produce the embedded watermark. After that upgrading the security of the watermark is obtained through embedding the shuffling encryption into the least significant bit (LSB) of the steward image. That scheme gives a good watermark image quality and good temper detection. P. MeenakshiDevi et al. [6] introduced an authentication approach to fragile image through tamper localization using wavelet transform. A shared secret key is used to scramble the created watermark. The coefficients of watermark was gained using haar filter in the integer type of wavelet transform. A watermark was embedded into the coefficients using LSB matching mapping. Radu O. Preda [7] introduced a scheme using wavelet transform for image authentication by using semi-fragile watermark to achieve image with a good quality and a high resolution for tampering detection. An improvement in reconstructed watermark is achieved through using random transpose for the watermark.
In this paper, fragile watermarking method is used to identify and trace any image content alteration.

The introduced fragile watermarking system consists of three modules: enciphering of the watermark image, watermark insertion and watermark extraction. First, the enciphered watermark image is achieved by applying Exclusive-OR (EX_OR) operation between the generated chaotic patterns that is generated from employing the Duffing map with the binary watermark image. Then, the enciphered watermark image is embedded in HL coefficients of each sub-block, after applying the Arnold transform and DWT on the host image. Finally, the watermarked output image is gained by performing the IDWT followed by inverse Arnold transform. The remainder of this paper is organized in four following sections: in the next section chaotic system and DWT are briefly described. The introduced watermarking method is presented in section 3. Then the test results are presented in section 4 and the conclusions are given in last section 5.

2. Background

A number of the basic concepts and terminologies used in this paper will be explained in the subsequent segments.

2.1 Chaotic System

A chaotic system has been used recently for many applications to increase the security. The importance of these systems lies in their sensitivity to initial conditions, so even a very small difference in the parameters and the starting state of these systems causes a massive difference in the final state.

In addition to the above-mentioned property, topological mixing and dense periodic orbits are the properties of all chaotic systems. In mathematics, a chaotic function or map is a function that has several forms of chaotic behavior [8, 9].

Two types of chaotic maps are used in this paper, and brief descriptions of Arnold map and Duffing map are presented in the following subsection.

2.2 Arnold Transform

This transform is used as one type of chaotic methods; the objective of using this transformation is to emphasize the security. Applying this transform to host image is considered as a preprocessing step to confuse the relation of the pixels in the image [10, 11].The two-dimensional Arnold cat map is given as:

$$\begin{bmatrix} x_{m+1} \\ y_{m+1} \end{bmatrix} = \begin{bmatrix} 1 & q \\ p & qp+1 \end{bmatrix} \begin{bmatrix} x_m \\ y_m \end{bmatrix} \bmod M \quad (1)$$

Where q and p are positive integers, m=1, 2, 3… M in $M \times M$ matrix. x_m, y_m are the position of pixels and x_{n+1}, y_{n+1} are the transformed position after application of the Arnold transform.

Periodicity in this transform means that the original pixels in an image can be returned after a specific period of time. a, b and the period of time can be considered as keys.

2.3 Duffing Map

This map is a two dimensional discrete over time domain. It is an example of a dynamic system and chaotic behavior can be presented from this system. Duffing map can be defined [12]:

$$x_{Duff_{n+1}} = y_{Duff_n} \quad (2)$$

$$y_{Duff_{n+1}} = -p x_{Duff_n} + q y_{Duff_n} - y_{Duff_n}^3 \quad (3)$$

$(x_{Duff} x_{n+1}, y_{Duff_{n+1}})$ is a new coordinate derived from the $\left(x_{Duff_n}, y_{Duff_n}\right)$ Coordinates, p and q are two constant values and considered as control parameters. p=2.75 and q=0.2.

2.4 The Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is a powerful iterative technique based on sub-band coding for decomposition the input image into low frequency and high frequency which represents the approximation and the detail respectively

The objective of the transformation is to identify the areas in the host image where a secret image can be embedded effectively [13, 14].

DWT has different types of filters such as Daubechies Bi-orthogonal filters, Daubechies orthogonal filters and Haar wavelet filter. In this work Haar wavelet filter is applied on one level of the host image.

3. Methodology

Generally, the fragile watermarking approach involves three basic processes, watermark enciphering, watermark insertion and watermark extraction, alteration discovery and localization, which are clarified in the next sections.

3.1 Watermark Enciphering

To start, $M \times M$ chaotic values of x_{duff} and y_{duff} are generated. In view of the fact that the generated chaotic sequences are real values, they cannot be directly applied to image pixels. Thus the sequence is converting to a one-dimensional binary series of size $1 \times M \times M$ as follows:

$$S_{bin} = \begin{cases} 1, & x\text{duff} \geq \text{yduff} \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

Rearrange S_{bin} into a two-dimensional array of dimension $M \times M$ to get the chaotic image pattern C_p. Thereafter a binary chaotic watermark EW is obtained

by applying exclusive-or (EX_OR) operation between the original binary watermark W and C_P as follows:

$$\mathrm{EW}(\mathrm{i},\mathrm{j}) = \mathrm{EW}(\mathrm{i}-1,\mathrm{j}) \otimes \mathrm{W}(\mathrm{i},\mathrm{j}) \otimes C_p(\mathrm{k},\mathrm{j}) \quad (5)$$

where $\otimes$ denoted the Exclusive-OR operation, $\mathrm{i} = 1,2,\dots,\mathrm{M}$, $j = 1,2,\dots,M$, $k = M, M-1,\dots,1$.

In deciphering process, the same pervious steps are performed, but in backward order. A detailed representation of the chaotic pattern generation was given in Figure-1.

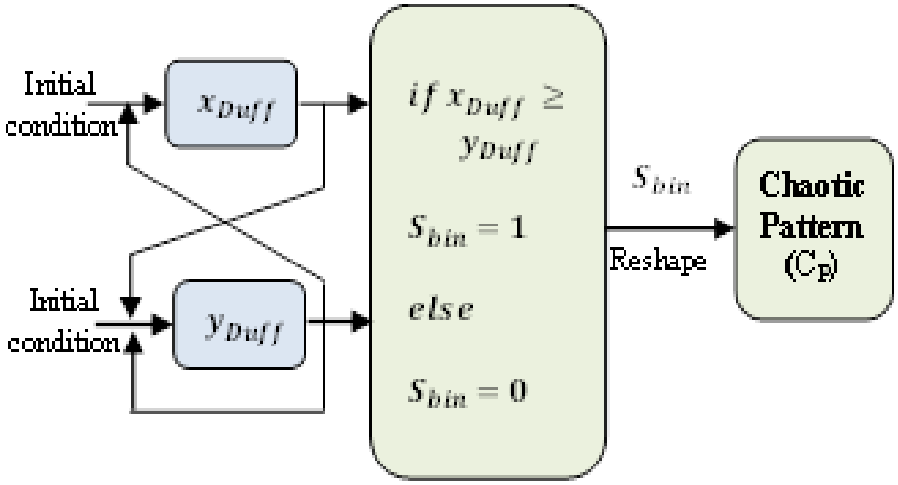


Figure 1- The outline of chaotic pattern generation

3.2 Watermark Insertion

The graphic depiction of the introduced insertion process was given in Figure-2. The base line of the embedding steps can be summarized as follows:

1. Read gray scale image of dimension $N \times N$ as Host image (H).
2. Scramble H, using Arnold transform. The result is denoted as H_{scr}.
3. H_{scr} is divided into sub-blocks of size 2×2 pixels. Single level decomposition of 2D DWT is applied to each sub-block of $H_{scr\ to}$ produce corresponding sub-block of DWT coefficients (LL, LH, HL and HH).
4. Read a binary image of size $M \times M$ as Watermark image (W), where $M = N\ /\ 2$.
5. EW is obtained by enciphering W as explained in section III. A.
6. Select HL coefficients of each sub-block result from step 3 for watermarking insertion. The insertion process is performed by modifying the coefficient of HL by the watermark bit as follows:

$$HLnew_{i,j} = \begin{cases} HLold_{i,j} + 0.5 & if\ \mathrm{EW} = 1 \\ HLold_{i,j} = HL_i & if\ \mathrm{EW} = 0 \end{cases} \quad (6)$$

where $i = 1,2,\dots,N/2,\ \ j = 1,2,\dots,N/2$.

7. Once all EW are inserted in the DWT blocks of H_{scr}, inverse of DWT is applied.
8. Inverse Arnold transform is applied to produce the watermarked image H'.

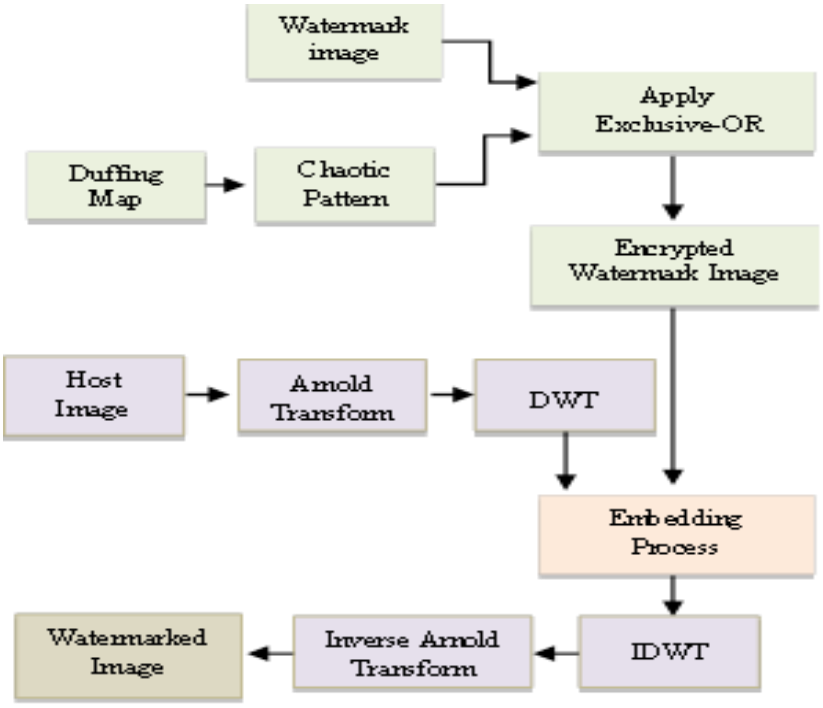


Figure 2- The outline of embedding process.

3.3 Watermark Extraction and Alteration Locates Process

A detailed description of the extraction and alteration locates process was given in Fig.3 .The base line of the extraction steps can be summarized as follows:

1. Read watermarked image H'.
2. Scramble H', using Arnold cat map. The result is denoted as H'_{scr}.
3. H'_{scr} is divided into sub-blocks of size 2×2 pixels. Single level decomposition of DWT is applied to each sub-block of H'_{scr} to produce corresponding sub-block of DWT coefficients (LL, LH, HL and HH).
4. The extracted watermark bit EW is obtained by selecting and modifying HL coefficients of each sub-block result from step 3 and as follows:

$$\mathrm{EW}_{i,j} = \begin{cases} 0 & if\ LH_{i,j} - fix(HL_{i,j}) = 0 \\ 1 & otherwise \end{cases} \quad (7)$$

where $i = 1,2,\ldots,N/2,\ \ j = 1,2,\ldots,N/2$.

5. Once all EW bits are obtained from the DWT blocks of H_{scr}. it will deciphered as explained in section III. A.

After the extraction of the watermark image, the alteration finding process will begin. The XOR operation will be implemented on both the original image and the extracting watermark images to distinguishes the variation between them, and depend on the difference result the image is determined such as altered or trustworthy. When the altered image is distinguished, the editing region will be determined using IDWT and the inverse Arnold scrambling.

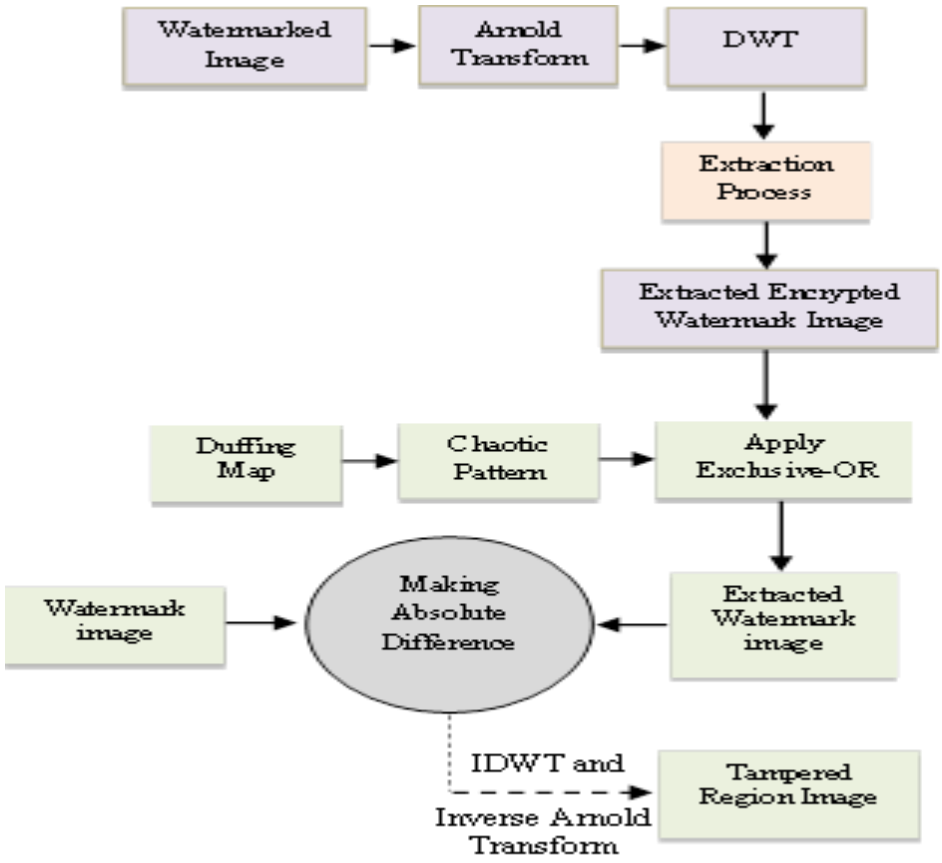


Figure 3- The outline of extraction and alteration locates process

4. The Results

To assess the effectiveness of the introduced approach, various experiments are implemented. Note that the proposed method has been performed using Matlab R2013a programming language, the Windows-7 operating system has been used to perform the experiments using the laptop computer processor: Intel Pentium dual CPU T230, 1.60 GHz, and (4GB) RAM. Also, the time complicity of the proposed approach is calculated using $\Theta(n^2)$. Finally, the averaging time that consumed for inserting/extraction on grayscale images and with size 256×256 is lower than 10 ms and both the insertion/extraction has the same speed.

In all the experiments, 256×256 gray scale image is used as the host image while the watermark image is a binary logo of dimension 128 × 128 . The factors of Arnold transform used in the introduced method are for q=1, p=1. The factors of Duffing map are chosen as Xduff(0) = 3.743 and YDuff(0) = 0.543.

Two metrics, the peak signal-to-noise ratio (PSNR) and the Normalized Cross Correlation (NCC) were used to evaluate the watermarked image (H') by compared with the host or original image (H), where the PSNR formula is [15]:

$$\mathrm{PSNR} = 10\ \log_{10}\frac{255^2}{\mathrm{MSE}} \tag{8}$$

And the mean-square error (MSE) equation is:

$$\mathrm{MSE} = \frac{1}{\mathrm{W}\times\mathrm{H}}\ \sum_{i=1}^{W}\sum_{j=1}^{H}(x - x')^2 \tag{9}$$

NCC is defined as [16]:

$$NCC = \sum_{i=1}^{k1}\sum_{j=1}^{k2}\left(x_{i,j} * x'_{i,j}\right)\frac{1}{\sum_{i=1}^{k2}\sum_{j=1}^{k1}(xi,j)^2} \quad (10)$$

Usually, the correlation coefficient values are varies between -1 to +1 and the perfect correlation is closer to 1. The results of quality evaluation based on the watermarking approach by using two measures PSNR and NCC presents in Table-1.

Fig. 4 and Fig. 5 show the outcomes of the introduced, method which explain the performance of the introduced method.

Figure-4 demonstrates the host, watermark and watermarked images provided in Figure- 4(a, b, c). All the values of the pixels in both the host and watermarked images and in different output are equal to zero. As shown in Figure-4 (d), the watermarked image is of good quality. Figure-5 (a, b) demonstrates the watermark and output extracted images .The pixels are equal to zero values in EX-OR output of the watermark and the extracted watermark images. Figure- 5(c) shown that the watermarked image is trustworthy.

Table 1- PSNR and NCC Values

Images	PSNR	NCC
Mustansiria	43.8389	0.9999
Lena	43.7668	0.9997
baboon	43.8675	0.9995

4.1 Performance under Item Placing Attack

In conducting this test, two types of item placing attacks are implemented in the introduced method. In the first type of item placing attack the watermarked Al_Mustansiria image is altered by adding two additional clocks in the image, where the clocks are derivative from the same watermarked image. Figure-6 (a) show the altered image while Figure- 6(b) demonstrates the extracted output watermark from Figure- 6(a). Figure- 6(c) shows the EX_OR output with some noise comparing with the Figure- 5(c) which presents EX_OR output of non-edited image. The result indicated that watermarked image has been subjected to some sort of editing. The alteration discovery outcome is shown in Figure- 6(d). In the second type of item placing attack the watermarked Al_Mustansiria image is altered by adding a welcome sign, where the welcome sign is derivative from another watermarked image Figure- 7(e).Figure- 7(a) displays the altered image, while Figure- 7(b) displays the extracted watermark from Figure- 7(a). Meanwhile, Figure- 7(c) displays the output of EX_OR with some noise comparing with the EX_OR result of non-manipulated image that presents in Figure- 5(c). Also, this result indicated that the watermarked output image has been exposed to various sort of editing. The detected altered region is shown in Figure-7(d).

4.2 Performance under Text Addition

To carry out this test, Figure- 8(a) display the text ‘Mustansria University" which fused in with the watermarked image, while the extracted watermark images are presented in Figure- 8(b). The EX_OR production presented with some noise in Figure-8(c) when compared the EX_OR output of non-manipulated image. The test result indicated that watermarked image has been exposed to some sort of editing and the localized distorted sections shown in Figure- 8(d).

4.3 Performance under Substance Elimination

In conducting this test, Figure- 9(a) shows the eliminating the item clock and the years of establishment in the watermarked image while the extracted watermark is presented in Figure- 9(b). The output of EX_OR in Figure- 9(c) presents some kind of noise comparing with the EX_OR output of the non-editing image as presented in Figure-5(c). Also the result shows that watermarked image has been exposed to specific kinds of altering while the localized distorted sections is presented in Figure- 9(d).

4.4 Insertions Capacity

The final deliberation in assessment of the introduced method is the insertion capacity. The capacity of the introduced method is about (25%) of the host image size.

5. Conclusion

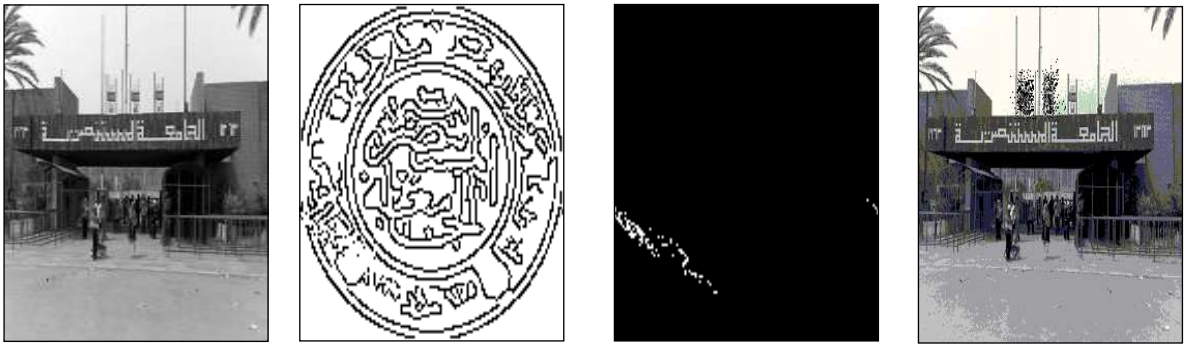
An introduced method of the fragile watermarking which depend on both chaotic maps and DWT transform and used in the image content detection is implemented. The chaotic Arnold transform is used on the host image to strengthen the watermark. The invisibility of the introduced watermarking method is calculated using both PSNR and NCC metrics and the experimental results shows that the PSNR value about 43 dB and NCC value about 0.99. Also, the introduced method of alter detection is experienced with a variety of content changes, difficult manipulations and different images. In addition, the introduced method performed well in efficiently localizing the altered region. In future this method can be experienced with further wavelet transform techniques by a number of image quality measurements and with faster simulation.

(a) (b) (c) (d)

Figure 4-The outcome of introduced method . (a) Mustansiria image, (b) Watermark image, (c) Watermarked image, (d) Difference between (a) and (c)

(a) (b) (c)

Figure- 5 The outline of extraction and alteration locates process. (a) Watermark image, (b) Extracted Watermark, (c) XOR-ed production



(a) (b) (c) (d)

Figure 6-Item placing attack from same image. (a) Tampered image, (b) Extracted watermark, (c) XOR-ed output, (d) Tampered region

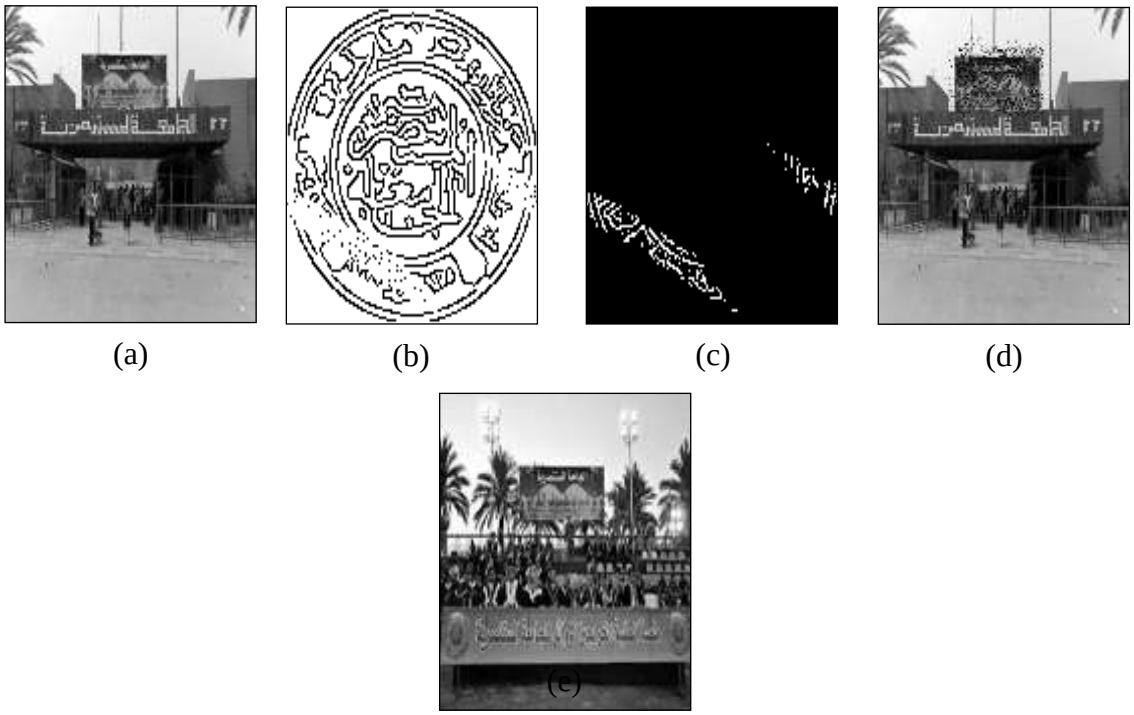


Figure 7-Item placing attack from different image. (a) Tampered image, (b) Extracted watermark, (c) XOR-ed output, (d) Tampered region, (e) watermarked image

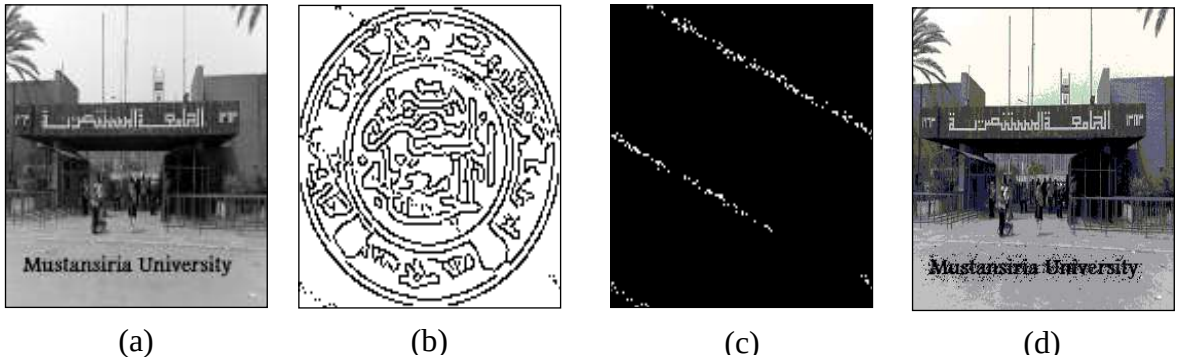


Figure 8-Text addition attack. (a) Tampered image, (b) Extracted watermark, (c) XOR-ed output, (d) Tampered region

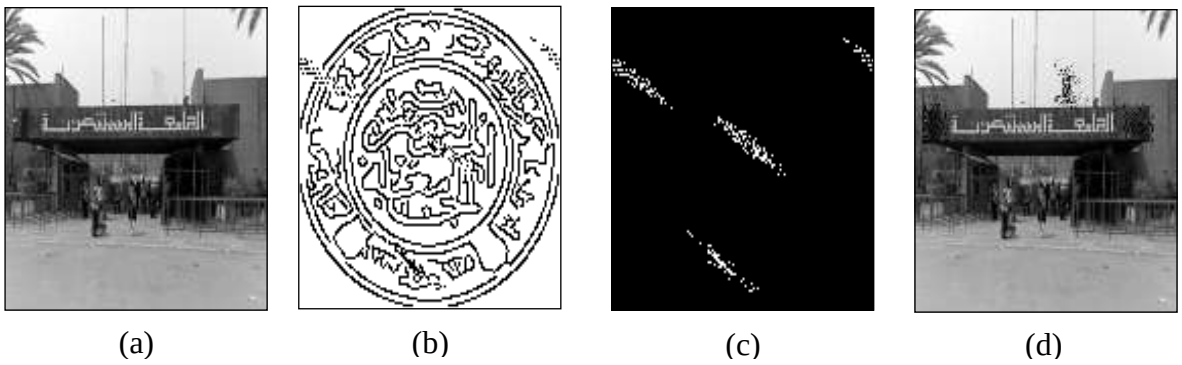


Figure 9-Substance attack. (a) Tampered image, (b) Extracted watermark, (c) XOR-ed output, (d) Tampered region.

References

1. Rawat S. and Balasubramanian R. **2011**. A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-International Journal of Electronics and Communications*, **65** (10): 840-847.
2. Barreto P.S., Kim H.Y. and Rijmen, V. **2002**. Toward secure public-key blockwise fragile authentication watermarking. *IEE Proceedings-Vision, Image and Signal Processing*, **149**(2): 57-62.
3. Fridrich J., Goljan M. and Baldoza A. C. **2000**. New fragile authentication watermark for images. *Proceedings 2000 International Conference on Image Processing*, **1**(1): 446-449.
4. Zhou X., Duan X. and Wang, D. **2004**. A semifragile watermark scheme for image authentication. *Proceedings of the 10th International Multimedia Modelling Conference:* 374-377. DOI: 10.1109/MULMM.2004.1265022 .
5. He, H., Zhang, J. and Tai, H. **2006**. A wavelet-based fragile watermarking scheme for secure image authentication. In: Yun Qing Shi and Byeungwoo Jeon (eds), *Digital Watermarking*. Jeju Island, Korea: IWDW,Springer, 422-423.
6. MeenakshiDevi, P., Venkatesan, M. and Duraiswamy, K.***2009***. A fragile watermarking scheme for image authentication with tamper localization using integer wavelet transform. *Journal of Computer Science*, **5**(11): 831-837.
7. Preda, R. O. **2013**. Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement* , **46**(1): 367-373. . doi.org/10.1016/j.measurement.2012.07.010
8. Rastogi, S. and Thakur, S. **2013**. Security Analysis of Multimedia Data Encryption Technique Using Piecewise Linear Chaotic Maps. *International Journal on Recent and Innovation Trends in Computing and Communication*. **1**(5): 458-461.
9. Keyvanpour, M. and Bayat, F. M. **2011**. An Effective chaos-based image watermarking scheme using fractal coding. *Procedia Computer Science*. **3**: 89-95. doi.org/10.1016/j.procs.2010.12.016
10. Sui, M. and Li, J. **2013**. The medical volume data watermarking using arnold scrambling and 3D-DWT. *Mechatronic Sciences, Electric Engineering and Computer (MEC)*, Proceedings 2013 International Conference. Shengyang, China :1120-1124. doi:10.1109/MEC.2013.6885231
11. Joshi, A. and Kumari, M. **2015**. Encryption of RGB image using Arnold transform and involutory matrices. *International Journal of Advanced Research in Computer and Communication Engineering*, **4**(9): 489-494.
12. Srinivasu, P. N. and Rao, S. **2015**. A Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel. *International Journal of Computer Applications*. **I**. doi:10.5120/21212-3915.
13. Sharma, P. and Swami, S. **2013**. Digital image watermarking using 3 level discrete wavelet transform. Conference on Advances in Communication and Control Systems: 129-133.
14. Rathi, N. and Holi, G. **2014**. Securing Medical Images by Watermarking Using DWT DCT and SVD. *International Journal of Computer Trends and Technology*, **12**(2): 67-74.
15. Gaata, M. T. **2016**. An Efficient Image Watermarking Approach based on Fourier Transform.*International Journal of Computer Applications*, **136**(9): 8-11.
16. Gao, T. and Chen, Z. **2008**. A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, **372** (4): 394-400.