BLIND ROBUST WATERMARK BASED ON CHAOTIC MAP AND FREQUENCY TRANSFORM IN A COLORED IMAGE

Firas Tareq Abdulateef¹, Nada Hussein M. Ali²

¹,²Department of Computer Science, University of Baghdad, Baghdad, Iraq

¹firas.cs11@gmail.com

Corresponding Author: Firas Tareq Abdulateef

https://doi.org/10.26782/jmcms.2020.08.00060

Abstract

As the internet is rapidly evolving, communication technologies have become insecure, so several techniques is produced to solve this issue. The digital watermark technique is one of these techniques which provides the protection of property rights. This paper present a technique for image watermarking images that aim to improve the degree of robustness of the watermarking system against noise attacks, also to enhance the quality of the watermark image. In addition, logistic map chaotic is used in this technique to make sure the watermark image where the watermark is available only to a authorize user. This scheme is considered as a blind scheme for both cover image and watermark. Firstly, the watermark logo is encrypted with the logistic map chaotic and then encoded into a string of binary values, the secret image is embedded within another image, i.e. cover image by decomposition of the host image using Haar wavelet transform. The experimental results of the presented work indicate that elevated values of imperceptibility have been indicated via MSE and PSNR parameters. The robustness of image watermark have been evaluated via NC, also it has been indicated for having high robustness against attacks.

Keywords: Haar wavelet transform, Image watermarking, Logistic map chaotic

I. Introduction

As the internet is rapidly evolving, along with the novel technologies related to multimedia services, also due to the fact that digital services are increasing, the multimedia data can might be extremely quickly distributed, modified, as well as duplicated. Thus, stopping the unauthorized usage of such contents become of high importance. With regard to such problem, the information hiding field is very effective solution [V]. Furthermore, digital watermarking can be considered as a significant and active area of development and studying. Copyright protection with regard to the digital information is now more possible due to the development of digital watermarking. Also, media data might be textual information that is related to
the copyright, author or an image. The digital watermarking can be defined as an approach permitting individuals adding investigation messages or secret copyright information to the digital media (documents, videos, audios, and images). The major difference between copyright protection and the copy protection is that the copy protection is limiting access to the copyrighted material, also inhibiting the copy process. For instances related to copy protection including encoded digital TV broadcasts, access controls to the copyrighted software using license servers as well as a copy protection methods on media[III].

The digital watermarking techniques categorized as visible watermark and invisible watermarks. Logos is a famous clarification of visible methods, this logo used for copyright protection by putting it at the corners of images or videos. Image watermarking applications such as integrity verification, authentication, and copyright protection using Invisible watermarks are advantageous. Sometimes, image watermarking technique using visible and invisible watermarking in simultaneously[VIII].

More profoundly, the digital watermarking techniques categorized as spatial or frequency domains. The time watermarking domain operated on image pixels directly, which make the embedding/extracting operations computationally less. However, these techniques lack more robustness. The frequency domains operate on data coefficients computed from transforming methods such as wavelet transform (WT) [XV].

Watermarking involves two processes as declared in figure 1:

I. An embedding process performed to embed watermark logo at the transmitting side.

II. An extraction process performed at the receiving side to extract watermark logo and judge the ownership.

Fig 1. The Main Watermarking Processes
II. Related Work

In this section, several types of research deal with watermarking methods have introduced in different domains and ways. Several image watermarking techniques manuscripts and the methods have been developed in the past and the latest studies related to the image watermarking techniques based on time domain and frequency transform domains are proposed in the literature review section. DWT watermarking techniques have commonly used, in DWT watermarking techniques decomposition the cover image into a set of sub-bands such as LL, HL, LH, and HH sub-bands.

In the year 2016, a study conducted by [XIV] suggested secure multiple watermarking approaches on the basis of SVD, DCT, as well as DWT. Cover medical images have been decomposed up to 2nd level related to DWT coefficients. Also, the LL related to host medical image has been transformed through SVD and DCT, the watermark medical image has been transformed via SVD and DCT. Singular value related to watermark image has been embedded in singular value regarding original image. Also, text watermark has been inserted at 2nd level related to host image’s HH. The experimental results showed that the suggested approach has the ability for withstanding a lot of signal processing attacks like Histogram equalization, Gaussian, JPEG, Salt-and-Pepper, and so on.

In the year 2017, a study conducted by [II] suggested DCT-based high robustness digital image watermarking approach. The method randomly selected each one of the blocks for DCT, also has been verified via various parameters like NC, PSNR, SSIM, with regard to evaluating the quality of the image in addition to the embedding proficiency.

In the year 2018, a study conducted by [XII] suggested digital image watermarking approach for hiding related information in the colored digital images. Images have been converted into YCbCr color space, the method embedded the watermark information with the use of wavelets transforms as well as SVD. It applied the QR code as watermark. The computational experiments on various cover images showing that to embed QR code has been more efficient in comparison to the other watermarks with regard to more effective information-carrying capacity, imperceptibility, as well as robustness.

In the year 2018, a study conducted by [XI] suggested robust and secure watermarking scheme on the basis of DC coefficient modifications in pixel domain in addition to the modified logistic map. Also, a cover image was divided into (8x8) sub-blocks and rather than computing the DC coefficient with the use of DCT watermark bits have been embedded through changing the DC coefficients regarding a lot of blocks in the spatial domain. The suggested approach has been computationally effective as the DC coefficient that hold the information was computed in the pixel domain rather that utilizing the DCT on an image block.
In the year 2019, a study conducted by [X] suggested image watermarking for color image-based frequency domain method. In this scheme, the Discrete Wavelet Transform was used after transforming images from RGB into YCbCr color space. The logistic map procedure has been used on watermark to shuffle this image before embedding it into the cover image. The imperceptibility and robustness of this method are measured by using Peak signal to noise ratio and normalized correlation measurements. It is shown that the proposed algorithm gives watermarked image with good imperceptibility with PSNR value equal 40dB and SSIM at least 0.997. The proposed method is also resistant against different attacks like as noise attacks, filter attacks, histogram equalization, sharpening, JPEG compression, and image cropping.

In the year 2019, a study conducted by [IX] a hybrid watermarking system based on non-blind image watermarking technique and Arnold scrambling transform has been presented to advance the robustness and imperceptibility of watermarked image. In this paper, the watermark has been used is colored and RGB image is converted to the YCbCr model. To improve the correlation between the cover and watermarked image, embedding process has been embedded the singular values of watermark in the Y channel of cover image using key strength value. For more security Arnold Transform method has been used to scramble the watermark image before its embedding in cover image. To calculate the imperceptibility, secrecy metrics such as; PSNR and SSIM have been chosen, whereas NC have been used to calculate the correlation between two image such as extracted watermark with original watermark. For robustness, the presented work has also been examined against several attacks.

### III. Theoretical Principles

The following subsections produce a brief description of the main concepts introduced in this research.

#### Haar Wavelet Transform (HWT)

The wavelet transform method has been comparable to hierarchical sub-band systems, in which sub-bands have been logarithmically spaced in frequency domain. The major ideas related to DWT with regard to 2D images specified in the following way: Initially, images are decomposed into 4 parts with low, middle, as well as high frequencies (LL, HL, LH, HH sub-bands) via critically subsampling the vertical and the horizontal channels utilizing the sub-band filters. Furthermore, the sub-bands indicated as HL, LH, as well as HH represents wavelet coefficients to obtaining the next wavelet coefficients. Furthermore, the sub-band LL will be decomposed and critically sub-sampled; such procedure will be repeated a few times, which has been specified via applications at hand. Figure 2 describes an example related to the image decomposed into 10 sub-bands for 2 levels. Each one of the levels has many band's information like HH, LH, LL, as well as HL frequency bands[VI].
In its development a lot of researches for improving DWT filter’s performance. The DWT along with Haar filter is referred to as HWT, with the use of these filters, the wavelet transformations have benefits including effective memory usage, straightforward and rapid. The next section will provide the decomposition process carried out via the Haar filter[XVI].

The output of Haar function is the result of average and difference between each pair in the series of size N to produce a new series (have two sub-signals) of size N/2 using Equations 1 & 2 respectively. The process of Haar wavelet is recursively and can be continued until the resolution (length of the signal) equal to 1 [IV].

\[ l(i) = s(2i) + s(2i + 1) \quad i \in \{0, ..., N/2\} \] (1)
\[ h(i + N/2) = s(2i) - s(2i + 1) \quad i \in \{0, ..., N/2\} \] (2)

Where s is the original signal, l represents the average (details), h represents the differences (approximates), also N is the resolution (length) [IV].

**Logistic Map Chaotic**

The major type related to the discrete-time systems Chaos model. The major properties related to Logistic map have been highly sensitive to the initial conditions, indicating that the small changes in initial values are going to be producing considerably distinctive values. Thus, because of such sensitivity property, Logistic map-based sequence has been random. Also, initial values have been indicated as seed values, such seed values specified as the secret keys, just authorized users will have the ability for producing the same sequence following utilizing the same seed values[XVII]. Equation 3 is specified as in follows:

\[ X_{n+1} = rX_n(1 - X_n) \quad X_n \in [0,1] \quad r \in (0,4) \] (3)
When $3.5699456 < n < 4$, mapping works in a chaotic state.

The initial sensitivity in addition to the long-term un-predictability specified via the Chaos. Also, the chaotic sequences created via chaotic equation have high sensitivity to the initial conditions and the initial values, arbitrary small change might be producing almost totally distinctive from chaotic series. Thus, using the chaotic series as watermark signal, along with simple generation, a lot of data in addition to a sensitivity to the initial conditions, also the benefits of a chaotic series related to initial value, the generated models as watermark embedding in addition to key extraction, not just practical, yet also straightforward [XVIII].

IV. The Proposed Watermarking System

The proposed watermarking system suggested in the present research based on two processes; embedding process that embeds the watermark in original media content on one side (i.e. sender), and extracts process that extracting watermark in other side (i.e. receiver).

Watermark Embedding Process

In this section, the original color image is used with RGB color space with $(512 \times 512)$ and color watermark image of size $(32 \times 32)$ are used as an input to the proposed. The block diagram that outline the main parts of the suggested watermark embedding process given in figure 3.

The basic steps of the watermark embedding method are as follows:

1. Isolated host RGB cover image into three color components and convert into Y-Cb-Cr color image and select the Y-component in the embedding process.
2. Y-image is selected in proposed method.

3. Apply one level of HWT using Haar wavelet transform on the host image to obtain $LL, LH, HL, HH$.

$$LL, HL, LH, HH = HWT(I)$$

4. Scramble the watermark image using Logistic map chaotic.

5. Convert the watermark image into a binary watermark.

6. Choose the HH band in the embedding process.

7. Embedding the watermark bit with the LSB procedure in a HH band of HWT.

$$ For \ i \in \{w_j\} \ and \ j = 1, ..., k \ and \ all \ m, n \ do $$

$$ Embedding \ using \ \text{LSB}(w_j, y(n, m)) $$

8. Apply inverse HWT to the center quarter region to obtain a watermarked image.

9. Reconstruct watermarked color component YCbCr.

10. Convert ycbcr image to RGB image.

**Watermark Extraction process**

This process used to separate the hidden information from the watermarked images. The proposed work suggested in this paper based on blind extraction process. This process consists a number of steps for the proposed extraction method that mean the original image is not required to get the watermark image, where input to this phase is the watermarked image and output retrieved is the hidden watermark. The block diagram shown in figure 4 outlines the main parts of the suggested extracting process. The watermark extracting method steps illustrated as follows:

![Proposed Extraction Process](image.png)

Fig 4. Proposed Extraction Process
1. Select the watermarked image to obtain the watermark image.
2. Get three color components by separating watermarked image.
3. Convert them into Y-Cb-Cr color image.
4. Y-image is selected separately.
5. Apply one level of HWT using Haar wavelet transform on the second region of the original image to obtain LL, LH, HL, HH.
   \[ LL, HL, LH, HH = HWT(I) \]
6. Extract the watermark from the HH band to each watermarked image.
7. Descramble the watermark using logistic map to obtain an extracted watermark image.

V. Result analysis and discussion

The proposed paper is implemented using the visual studio 2017 (C# programming language) is used to develop the proposed watermarking system and examined by using three standard images, which are considered as the cover images. They are color scale images of size 512 × 512, identified as: Lena, Girl and Gold hill are shown in figure 5. The watermark image is defined as a color image with size 32 × 32. It is identified as Koala and penguins. These images are shown in figure 6. In terms of imperceptibility and robustness are investigated the performance of presented model against attacks. The imperceptibility means the visualization quality of the human of the cover image should not be influenced much even after watermark embedding. The similarity of watermarking technique images must be almost same between cover image and the watermarked image [I]. The PSNR is utilized for analyzing the watermarked images’ visual quality, and it has the ability of displaying the watermarked image’s perceptual transparency, in concerns to the original cover [VII]. The PSNR can be characterized by the formula below:

\[
PSNR = 10 \times \log_{10} \left( \frac{f_{\text{peak}}}{MSE} \right) \tag{4}
\]

And also the Mean Square Error (MSE) can be characterized by the formula below:

\[
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [W(i,j) - W'(i,j)]^2 \tag{5}
\]

The evaluation of the watermark extraction process’s robustness utilizes NC parameter. It is responsible for measuring the coefficients of correlation between the obtained watermark W’ and the initial inserted one. The NC can be characterized by the formula below [XIII].

Copyright reserved © J. Mech. Cont.& Math. Sci.
Firas Tareq Abdulateef et al

741
\[ NC(w, w') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} w(i,j) \times w'(i,j)}{\left( \sum_{i=1}^{M} \sum_{j=1}^{N} w(i,j)^2 \right) \left( \sum_{i=1}^{M} \sum_{j=1}^{N} w'(i,j)^2 \right)} \] (6)

The value of the NC has been defined in the [0, 1] interval. The optimal value is equal to 1, NC value at least 0.75 is considered an acceptable value [XIII].

In the proposed watermarking system, logistic map chaotic is used to scramble the watermark image using initial value equal to 3.9 and with one iteration as declared in figure 7.

After the implantation of embedding procedure, the resultant image is yield and it is known as watermarked image as declared in figure 8 below.
The performance of the proposed model is tested by calculating the PSNR, NC, and MSE respectively between the watermarked image and the cover image to the all test images. In addition, NC metric is used to make sure the similarity between images (extracted image and the Watermark image). Table 1 provides MSE, PSNR and NC between the tests original and the watermarking images using two different logo images Kola and Penguins respectively.

Table- 1: MSE PSNR, and NC of the Presented Scheme

| Cover/Logo images | Color Koala | Color Penguins |
|-------------------|-------------|----------------|
|                   | MSE | PSNR | NC | MSE | PSNR | NC |
| Lena              | 0.016 | 42.11 | 0.997 | 0.016 | 42.11 | 0.997 |
| Goldhill          | 0.013 | 42.561 | 0.999 | 0.013 | 42.561 | 0.999 |
| Girl              | 0.050 | 39.636 | 0.993 | 0.052 | 39.551 | 0.993 |

The obtained results of Table 1 using the cover image with (512×512) and color watermark with (32×32) show that Lena image and Goldhill image are have high PSNR value compare to other test images. A better explanation that one may say that these images having high imperceptibility than other images. Figure 9 illustrates a plot diagram for PSNR of all images.

Fig 9. PSNR Results between the Different Watermarked Images.
Extraction algorithm is used to retrieve the source watermark image; or logo image; from the watermarked image. Figure 10 declare the extracted color logo without attack of NC=1.

Fig 10. Extracted Logo Images

Firstly, the watermarked image was contaminated with additive Gaussian and Salt and Pepper noises of different noise powers. The proposed watermarking algorithm is considered robustness against the previous attacks. Where, the NC metric is calculated during Salt and Pepper and Gaussian attack to show the watermark robustness against the noise attacks. Table 1 shows the results under salt and pepper attacks, while the results of Gaussian attack are shown in Table 2.

**Table- 2: NC metric under Salt and Pepper Attack**

| Logo  | Koala image | Penguin image |
|-------|-------------|---------------|
|       | No attack   | Salt Pepper   | No attack   | Salt Pepper   |
|       |             | (0.01)       | (0.01)      | (0.02)       |
| Lena  | 1           | 0.940        | 1           | 0.966        | 0.926         |
| Goldhill | 1         | 0.949        | 1           | 0.960        | 0.923         |
| Girl  | 1           | 0.945        | 1           | 0.948        | 0.912         |

**Table- 3: NC Metric Under Gaussian Attack of Test I**

| Logo  | Koala image | Penguin image |
|-------|-------------|---------------|
|       | No attack   | Gaussian      | No attack   | Gaussian      |
|       |             | (0.01)       | (0.01)      | (0.02)       | (0.02)       |
| Lena  | 1           | 0.924        | 1           | 0.964        | 0.921         |
| Goldhill | 1         | 0.930        | 1           | 0.956        | 0.911         |
| Girl  | 1           | 0.917        | 1           | 0.937        | 0.909         |
The obtained results from Table 1 and 2 respectively shown the robustness of watermark under salt& pepper and Gaussian attack for all test images in proposed watermarking system. Figure 11 and 12 illustrate NC values of all test images.

**Fig 11. NC Values under Salt and Pepper Attack**

**Fig 12. NC Values under Gaussian Attack**

**X. Conclusion**

This paper will outline the most conclusions reached after studying the problem and the proposed solution. This thesis suggests a technique of image watermarking using invisible watermarking. Image watermarking based on HWT with YCbCr color model. The embedding process done by applying the LSB on HWT coefficients (HH band) to make the watermarking scheme more robustness against noise attacks and more imperceptibility. The proposed work has been applied
on three cover images like Lena, Goldhill, and Girl image with size (512×512) and Koala and Penguins logo with size (32×32). The proposed watermarking algorithm performance has been calculated using PSNR, MSE and NC. The watermark robustness is calculated under attacks against attacks by using NC values. Watermarked image imperceptibility is calculated by using PSNR. In addition, we applied the logistic map to increase the assurance of the watermark image. Thus, the watermark image and can obtain only by authorized user. The approach results based on using a color cover image and a color watermark image, which obtain high imperceptibility and robustness against attacks. According to the results which were discussed in this paper, propose to improve the proposed algorithms to obtain high robustness against the geometric attacks. In addition, we propose to embed another digital signal like audio into the image using the same scheme.

References

I. Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. Digital watermarking and steganography. Morgan kaufmann, 2007.

II. De, S., Bhaumik, J., Dhar, P., and Roy, K. "DCT-Based Gray Image Watermarking Scheme." Communication, Devices, and Computing. Springer, Singapore, pp: 181-189, 2017.

III. D.M. Jose, R. Karuppathal, and A.V. Kumar, "Copyright Protection using Digital Watermarking." Copyright Protection using Digital Watermarking, 2012, online: https://pdfs.semanticscholar.org/d536/5a1f9d8ae04f3932eec02b898a91cd7aa0e1.pdf?_ga=2.236295046.623200384.1588546901-125568524.1547477851. Accessed 15-5-2020.

IV. Fiscella, M. Combining CMOS-based microelectrode arrays with genetic labeling to study visual processing in the retina. Diss. ETH Zurich, 2014.

V. Hamidi, M., El Haziti, M., Cherifi, H., and El Hassouni, M. "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform." Multimedia Tools and Applications, Vol. 77, No.20, pp: 27181-27214, 2018.

VI. Hsieh, M. S., Tseng, D. C., and Huang, Y. H. "Hiding digital watermarks using multiresolution wavelet transform." IEEE Transactions on industrial electronics, Vol. 48, No.5, pp: 875-882, 2001.
VII. Kang, X. B., Zhao, F., Lin, G. F., & Chen, Y. J. "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength." Multimedia Tools and Applications, Vol. 77, No.11, pp: 13197-13224, 2018.

VIII. Mousavi, S. M., Naghsh, A., and Abu-Bakar, S. A. R."Watermarking techniques used in medical images: a survey." Journal of digital imaging, Vol. 27 No.6, pp: 714-729, 2014.

IX. Pandey, M. K., Parmar, G., Gupta, R., and Sikander, A. "Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space." Microsystem Technologies, Vol. 25, No. 8, pp: 3071-3081, 2019.

X. Pugar, F. H., and Arymurthy, A. M. "Blind Color Image Watermarking Based on 2-level Discrete Wavelet Transform, M-ary Modulation, and Logistic Map." 2019 12th International Conference on Information & Communication Technology and System (ICTS), pp: 235-240, 2019.

XI. Parah, S. A., Loan, N. A., Shah, A. A., Sheikh, J. A., and Bhat, G.M. "A new secure and robust watermarking technique based on logistic map and modification of DC coefficient." Nonlinear Dynamics, Vol.93, No.4, pp: 1933-1951, 2018.

XII. Patvardhan, C., Kumar, P., and Lakshmi, C. V. "Effective color image watermarking scheme using YCbCr color space and QR code." Multimedia Tools and Applications, Vol. 77, No.10, pp: 12655-12677, 2018.

XIII. Sabbane, F., and Tairi, H. "Medical image watermarking technique based on polynomial decomposition." Multimedia Tools and Applications, Vol. 78, No.23, pp: 34129-34155, 2019.

XIV. Singh, A. K., Dave, M., and Mohan, A. "Hybrid technique for robust and imperceptible multiple watermarking using medical images." Multimedia Tools and Applications, Vol.75, No.14, pp: 8381-8401, 2016.

XV. Soualmi, A., Alti, A., and Laouamer, L. "A new blind medical image watermarking based on weber descriptors and Arnold chaotic map." Arabian Journal for Science and Engineering, Vol. 43, No.12, pp: 7893-7905, 2018.

XVI. Sudibyo, U., Eranisa, F., Rachmawanto, E. H., and Sari, C. A. "A secure image watermarking using Chinese remainder theorem based on haar wavelet transform." 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE). IEEE, pp: 208-212, 2017.

XVII. Trivedy, S., and Pal, A. K. "A logistic map-based fragile watermarking scheme of digital images with tamper detection." Iranian Journal of Science and Technology, Transactions of Electrical Engineering, Vol. 41, No.2, pp: 103-113, 2017.

XVIII. Yu, G., and Zhao, X. J. "Study Based on Chaotic Encryption and Digital Watermarking Algorithm." Recent Advances in Computer Science and Information Engineering. Springer, Berlin, Heidelberg, pp: 619-625, 2012.

Copyright reserved © J. Mech. Cont.& Math. Sci.
Firas Tareq Abdulateef et al