

Proposed Watermarking System Using Genetic Algorithm and Security Measures

Assist. Prof. Dr. Israa AbdulAmeer AbdulJabbar

ch_israa81@yahoo.com,
110033@uotechnology.edu.iq

University of Technology - Computer Science Department,
Baghdad, Iraq

Wala'a Dia'a Abdul Ghafoor

walaadiaa90@yahoo.com

University of Technology - Computer Science Department,
Baghdad, Iraq

Abstract: *This paper produces a proposed watermarking system to be used for protecting images from tampering by attackers and other third parties. This proposed system consists of three stages: pattern generation, watermark embedding and watermarking extracting. In the first stage, two patterns (primary and secondary) are generated from some features of the image that used as a watermark, then applying a genetic algorithm to get random, unique and robust primary pattern, This unique pattern that is generated from image used as a watermark and embeds this pattern in the original cover image instead of embedding the whole watermarking image inside the cover image. The primary pattern will be embedded in different three locations mainly diagonal, vertical and horizontal lines in the middle of the cover image. The receiver can retrieve this pattern to ensure that it is the same pattern that is generated from the watermark image. In addition to generate and embed secondary pattern that used to confirm*

between the sender and the recipient, if the secondary pattern doesn't match, the recipient tells the sender to resend the image again. Different experiments are applied to test the system and the results show the watermark is random, imperceptible, and robust enough against image cropping attacks, fully secure, and Peak Signal to Noise Ratio (PSNR) value of the watermarked image is better than the watermarked image of many previous watermarking system when compared with them.

Keywords: Primary pattern, Secondary pattern, Genetic Algorithm, Watermark embedding, Watermark extracting, PSNR, Image cropping attack, Randomness test.

1. Introduction

One of the best solutions to prevent modifying, redistributing multimedia and illegal copying is digital watermarking. Digital watermarking is a technique that embedded copyright or any other information into original data to protect it from illegal persons [1].

Most important problem that related with digital multimedia that transferred over internet is data authentication, and because this digital media are easily to copy and transmit. For this reasons many researchers are conscious of the issues like proof of ownership, copyright protection, etc that related to multimedia. As a result, many solutions have been proposed and are available [2].

New idea presented to protect the image by watermark, this watermark is not representing as a text or an image, it will be a pattern. The pattern here is represented as two types: primary and secondary, the primary pattern used as watermark and it will be embedded many times in different places inside the cover image, and the secondary pattern is used to confirm if the image is exposure to attack or not. Both proposed patterns are generated

from some features of the image that used as a watermark and these features will generate the initial population of Genetic Algorithm.

The aim of the proposed work is to embed a unique pattern that is generated from the watermark image, this pattern is extracted using genetic algorithm and is selected under some criteria's of security measures to generate a unique binary pattern to be embedded inside the cover image this lead to made the change on the cover image invisible and insensible as compared to embed whole or part of watermark image.

Section 2 will describe some related works, section 3 describes the proposed work, section 4 will describe the experiments and results and the conclusion will be in section 5.

2. Related work

C. Chin Lai (2011), proposed a technique of image watermarking that is depend on tiny genetic algorithm (GA) and singular value decomposition (SVD). SVD for the cover image have been modifying by multiple scale factors for embedding the watermark, the values of scale vector determine the strength of the watermark. tiny GA present methodical way to look the refinements of the scaling factors that are using to control the strength of watermark embedding, by searching for proper values to improve the robustness of the watermark and visual quality of watermarked image. The watermark successfully extracted after attacks by image processing operations [3].

J. Aguilar.et.al.,(2011), proposed the conjunction of (LSB) least significant bit, in multiplied classes random neural network. This proposed method design a training process for Watermark pattern, the learned pattern have been embedding in the original image, the pattern detecting process in the carrier image. The watermark removal is not behold in this proposed method, because this method studies the capability of detection for the neural approach of any tampering over the carrier image [4]

S. Sahand, Mohammadi Ziabari and et.al., (2013), developed watermarking algorithm without using correlation value, to

improve the security of watermark against attacks , increased the speed of embedding watermark and the removal of unintended watermark after embedding is reduced. In addition to use some pre-processing operations, Arnold transform to provide more security in the watermarking. After pre-processing each of watermark and image are decomposed by use DCT transform. The cover image have been divided into 8*8 blocks and DCT have been applied to get coefficients values. Then the number of blocks and number of coefficient in block is converted to 32 binary bits to build the chromosomes of genetic algorithm and the fitness function is the two criteria in evaluation of robustness and imperceptibility [5].

N.Mohananthini.et.al.,(2015), presented a comparison for different techniques of embedding digital watermarking by GA. The work demonstrates the basic 3 types of various watermarking schemes these schemes are generated by GA to get very good results values of PSNR and NC. The result shows that these 3 schemas have good robustness when compared it with other single watermarking schemas and produced good values of fidelity versus attack [6].

B. Saadoon Mahdi,(2015), presented intelligent method for digital image watermarking by used hybrid approach of visual cryptography and hash function which provide for the watermarking system authenticity and security. The watermark embedding in the cover image have been done by using three techniques which are artificial neural network ,genetic algorithm and human visual system model the result will be effective balancing between imperceptibility and robustness of the digital image by using middle frequency coefficients. watermarking extracting was done by use the same operations of the embedding and using overlapping approach in visual cryptography. This proposed method provided secure adaptive intelligent system and balancing between imperceptibility and robustness by extract the watermark from various types of attacks [7].

W. Song .et al. , (2015) , proposed watermarking algorithm based on genetic algorithm and wavelet packet decomposition. This proposed method have two important usage ,first to decide wavelet

packet base from large perpendicular based library, the other usage is to find suitable locations for embedding watermarks.

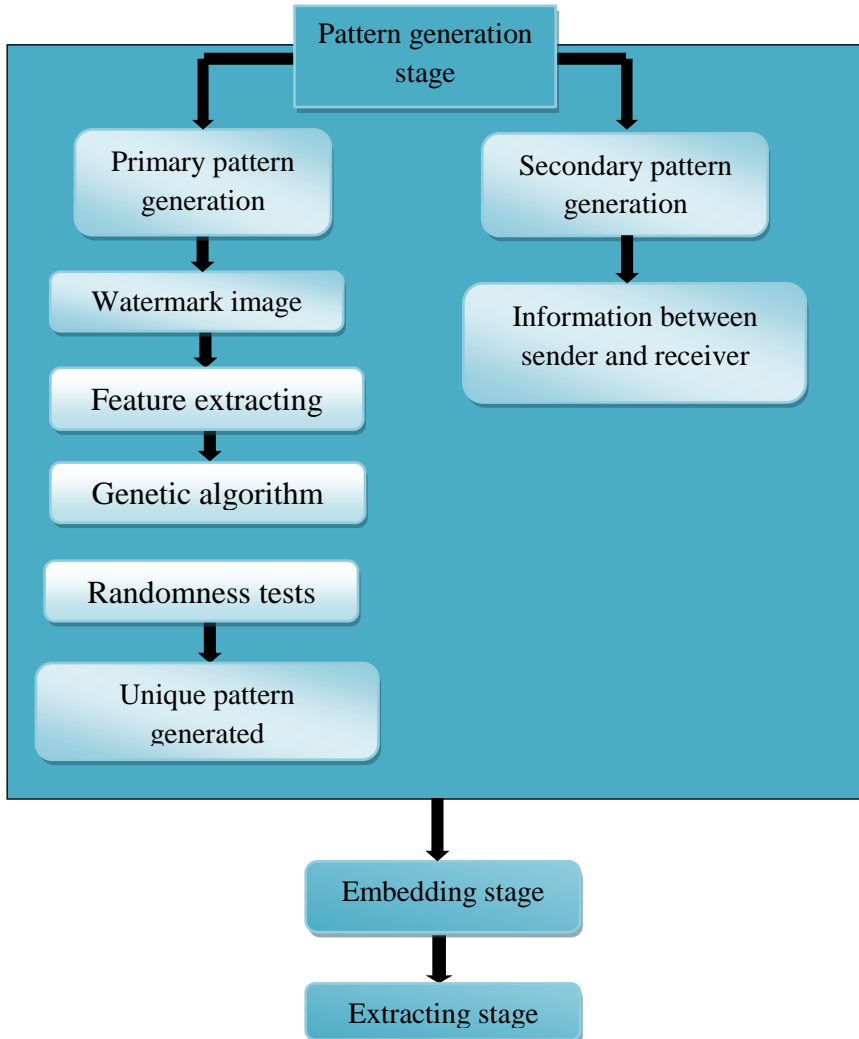


Figure (1): The main stages of the proposed work

This method used genetic algorithm for choosing a suitable base for wavelet packet transform and for choosing suitable coefficients in the sub bands that have been used for watermarking embedding .At the first time application genetic algorithm, the various wavelet packet base have been used to form various chromosomes and to

observe the selection of the translation base. At the second time focus on searching for robust method for embedding watermarking [8].

3. The Proposed System

The proposed watermarking system is consisting of three stages: the first stage is the pattern generation (primary pattern and secondary pattern), the watermark embedding stage and watermarking extracting stage. Figure 1 show the stages of the proposed work.

3.1. Pattern Generation

The pattern generation process has two stages: Primary Pattern Generation and Secondary Pattern Generation.

3.1.1. Primary Pattern Generation

The primary pattern has been generated from the watermark image to be embedded in the cover image; this generated pattern has been done by using the genetic algorithm. The first population for GA has been generated by computing the image histogram with its features (probability, mean, standard derivation, energy and entropy), to get five values and after that compute the mean and the median filters to get three values to be finally eight values. These values are converted to binary, this is to generate a population of 64 bit in length, and this pattern will be the first population to GA. This pattern is unique, strong and random, and it will be selected after passing the 5 randomness tests of security measures which are represented by frequency test, serial test, poker test, run test and autocorrelation test.

Algorithm (1): pattern generation process

Input: Watermark image

Input: Watermark image

Output: unique pattern

Process:

Begin

- Step 1- Compute the histogram of the watermark image.
- Step 2- Compute histogram

X =width of image

Y =height of image

$M=x*y$

$$\text{Probability}(c) = \frac{H(c)}{M}$$

$$\text{Mean}(\text{image}) = \sum_{b=0}^{L-1} b \times \text{probability}(b)$$

$$\text{Standard derivation}(\text{image}) = \sqrt{\sum_{b=0}^{L-1} (b - \text{mean})^2 P(b)}$$

$$\text{Energy} = \sum_{b=1}^L (P(b))^2$$

$$\text{Entropy} = - \sum_{b=1}^L P(b) \log_2[P(b)]$$

- Step 3- Convert the values from step 2 to the binary representation.
- Step 4- Apply mean and median filters on watermark image to get string with 24 bit of length and then combine it with the string that have 40 bit of length to get string with 64 bit of length.
- Step 5- Apply genetic algorithm
Initial population=pattern with 64 bit
Random solution (initial population)
Divide pattern to eight chromosomes
Apply order crossover between the eight chromosomes as a fitness function
 Cr = the point of crossover
for $i = 1$ To Cr
 $T(i) = C1(i)$
 $C1(i) = C2(i)$

$C2(i) = T(i)$
Next
Target function (Randomness tests)
If the pattern pass the target function then
Embed the pattern in cover image
Else
This population return to made crossover between the
chromosomes and tested it by target function
If the population stay don't pass the target function then
Apply mutation on the chromosome that have smallest value
between other chromosomes.
Mu=position of mutation
For $i=1$ to 8
If $I = Mu$ then $C(i)=1$
Next
Test the population after mutation by target function
If it pass all tests then embedding it in the cover image
Else
Apply crossover and mutation until the target function is met
End

Algorithm (2): Randomness tests

Input: pattern

Output: unique pattern

Process:

- Step 1- Read the pattern P

- Step 2- For $i=1$ to p

Begin

Apply frequency test

$$T1 = (n0 - n1)^2 / n$$

Apply serial test

$$T2 = \frac{4}{n-1} - 1(n00^2 + n01^2 + n10^2 + n11^2) - \frac{2}{n}(n0^2 + n1^2) + 1$$

Apply pocker test

$$T3 = \frac{2^m}{k} (\sum_{i=1}^{2^m} ni^2) - k$$

Apply run test

$$T4 = \sum_{i=1}^k (b_i - e_i)^2 / e_i + \sum_{i=1}^k (g_i - e_i)^2 / e_i$$

Apply autocorrelation test

$$T5 = 2 \left(A(d) - \left(n - \frac{d}{2} \right) \right) / \sqrt{n - d}$$

If $T1 < 3.8415$ and $T2 < 5.9915$ and $T3 < 14.0671$ and $T4 < 9.4877$ and $T5 < 1.96$ Then

Embedding pattern according to algorithm (3)

Else

Apply genetic algorithm to generate new pattern

- *Step 3- unique pattern generated*

End

End

3.1.2. Secondary Pattern Generation

The secondary pattern is generated to be the verification pattern between the sender and the receiver. This pattern consists of information for primary pattern that is generated from genetic algorithm such as the way of randomness, number of crossover, number of mutation, mean, median filters values, number of bit that is chosen to embed in it, and ASCII code for letter (M and S) that is representing the main and the secondary diagonal, and any information that agreed between the sender and the receiver. This information is collected and converted to binary representation to generate the secondary pattern with (64-bit) of length. This pattern must be verified between the two parties and any bit missed this mean there is a tamper on watermarking image, the receiver can tell the sender to resend watermarking image again.

3.2. Watermarking Embedding

In the watermarking embedding step, the primary and the secondary patterns are embedded in the main diagonal and the secondary diagonal of the cover image.

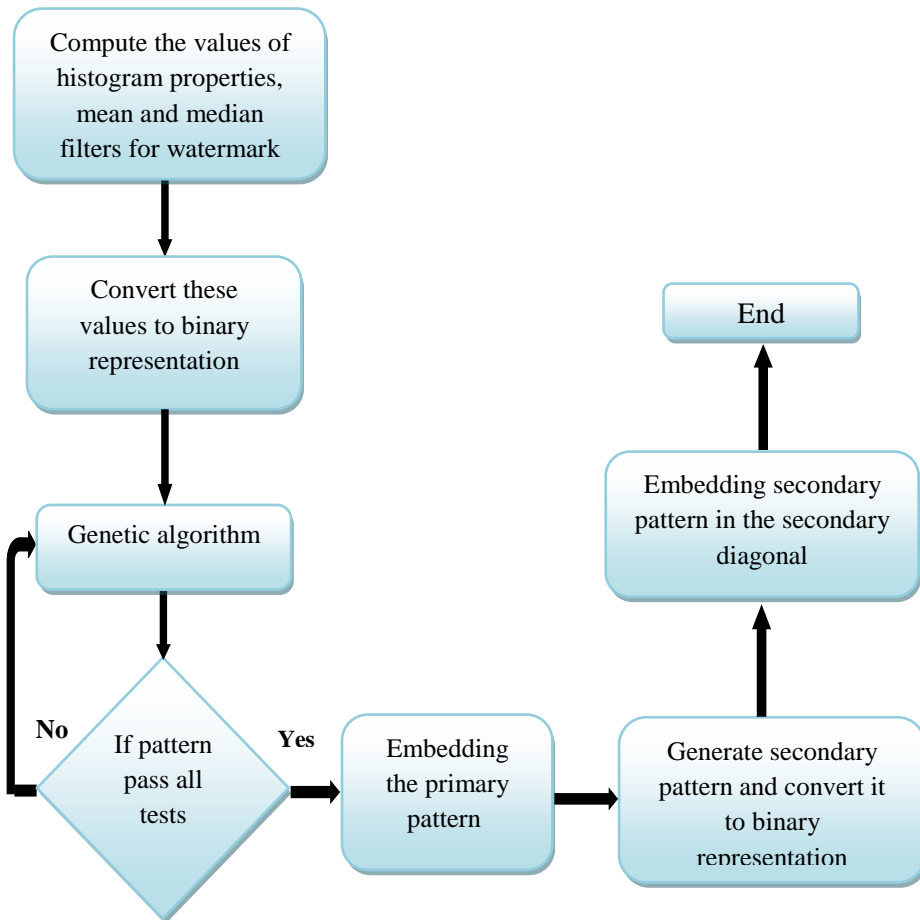


Figure (2): The process of pattern generation and watermark embedding

Algorithm (3): Watermarking Embedding

Input: cover image and the binary pattern

Output: Watermarked image.

Process:

Begin

Step 1-Read and display the cover image and determine its size.

Step 2- for $k=1$ to 64

Begin

Read the binary pattern string $P(k)$

Set the LSB to replace one bit of pattern $P(k)$ with pixel(i,j)

Next k

End

Step 4-Show the Watermarked image.

End

3.3. Watermark Verification and Extracting

This stage is consisting of two steps: In the first step the secondary pattern are extracted from the secondary diagonal of the cover image and matched with the pattern that previously agreed between both the sender and the receiver. If the secondary pattern is matched, then, the second step is implemented to get the primary pattern and extract the watermark, otherwise, a tamper is detected by the receiver and notify the sender to repeat the process and resend the cover image again.

Algorithm (4): Watermark Verification and Extracting

Input: Cover image, the watermark image

Output: the secondary and the primary patterns

Process:

- ***Step 1-*** Extract the secondary pattern from the embedding location (secondary diagonal), by take the least significant bit of pixel and convert it to binary representation and retrieve the first bit of this binary value until get the all pattern of 64 bit.
- ***Step 2-*** If the pattern is same as the original pattern that is sent by the sender then go to next step, else, the receiver tells the sender to resend the watermarking image again and repeat step 1.
- ***Step 3-*** Retrieving the first pattern from the main diagonal.

- *Step 4-* Repeat the same steps as indicated in algorithm (1).

If the pattern passing all the randomness tests, then, the result of step 3 is matched with the result of step 4 and there is no attack.

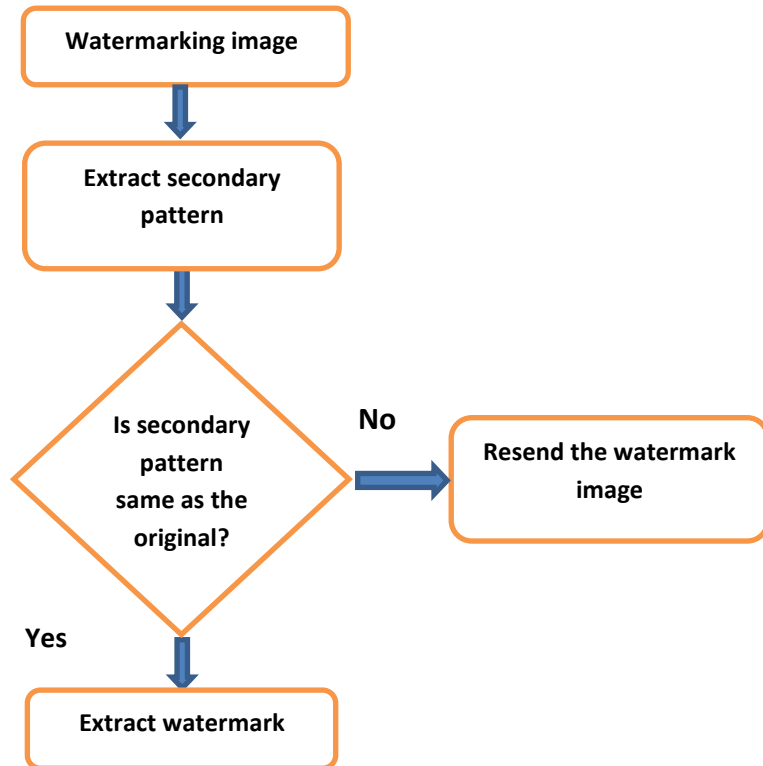


Figure (2): The pattern extracting of the proposed system

4. Experimental and results

The experiments are applied on different set of sample images and all are shown in table (1).



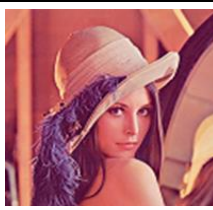









Table (1): The Sample of Images Used
















		
A	b	c
		
D	e	f
		
G	h	i

After embedding watermark in a tested images (cover images), Peak Signal to Noise Ratio (PNSR) and Normalize correlation (NC) are used to test the watermarked images without any attacks between watermarked and original images. The number of embedding bits is 64 bits have been embedded four times in a cover image with size (256×256) , one time for the secondary

pattern and three times for primary pattern. The results shows high imperceptibility, where the average value of PSNR is 62.2 and the average value of NC is 0.9999. Below the results for the testing images is shown in table (2).

Table (2): PSNR and NC results of the proposed system

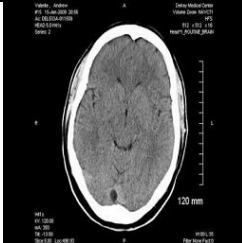

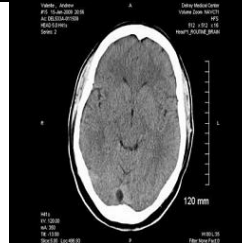



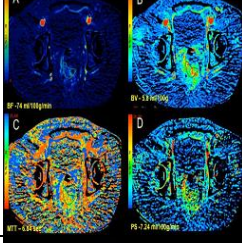

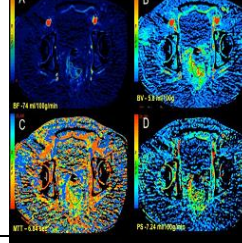



No.	Original image	The image used as a Watermark	Watermarked image	PSNR For watermarked image	NC
1				62.5421	0.9999
2				62.7850	0.9999
3				62.4624	0.9999
4				62.5421	0.9999

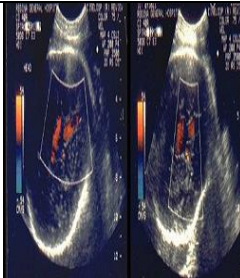

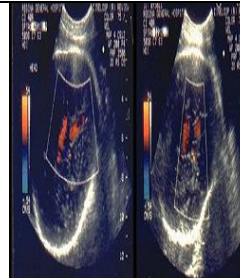


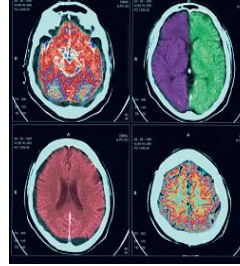
5				62.3834	0.9999
6				62.2271	0.9999
7				62.3834	0.9999
8				62.0732	0.9999
9				62.7034	0.9999

The second experimental results deal with another type of images that are the medical images. The table (3) shows the different important medical images that created by use new medical techniques. This type of images needs high imperceptibility without tampered the quality of watermarked image. The result of this test

and the value of PSNR after embedding for the medical image is shown in the table (3).

Table (3): PSNR and NC for some medical images.

No.	Original image	Watermark image	Watermarked image	PSNR for watermarked image	NC
1				63.3759	0.9999
2				63.0340	0.9999
3				63.6402	0.9999
4				62.2271	0.9999

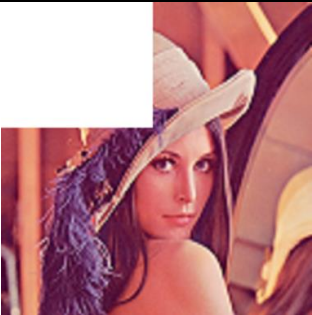

5				61.9217	0.9999
6	<p>R and NC for</p> 			62.9503	1

4.1. The Robustness of the proposed method

The Third type of the experimental results deals with the robustness of the proposed method after applying cropping attack on watermarked image. In this proposed system the cropping attack is applying on watermarked image Lena in different sides and can retrieve the whole pattern from image which have been attacked. Table (4) shows different cropping regions on Lena image.

/




Table (4): Different cropping attack on watermarked image with the results of pattern retrieval process

No.	Cropping image	Watermark retrieval
1		2 patterns from 3 patterns
2		2 patterns from 3 patterns
3		3 patterns from 3 patterns
4		2 patterns from 3 patterns

5		1 pattern from 3 patterns
6		2 pattern from 3 patterns
7		2 patterns from 3 patterns
8		3 patterns from 3 patterns

9		1 pattern from 3 patterns
---	---	----------------------------------

Table (5): comparison among the proposed work with some previous technique

Author	Watermarking Technique	Image that use to embed watermark	Image size	PSNR	Proposed System PSNR
[7]	Using ANN, GA, human visual system model, and DCT.		512*512	58.5232	63.6402
[8]	Using GA and wavelet packet decomposition		512*512	45.21	61.55
[5]	Using DCT and GA		256*256	49.7	61.9

[4]	Using conjunction of (LSB), in the multiple classes' random neural network.		256*256	51.241	63.205
-----	---	---	---------	--------	--------

5. Conclusions

For pattern generation, the proposed two patterns are generated from the histogram and the histogram's properties of the selected image that used as a watermark image. The histogram properties used in current work were represented by mean, standard deviation, probability, entropy, and energy. These properties will be the initial population for GA.

Using of genetic algorithm to generate unique binary code of (64-bit) length . The pattern generation and selection were done after passing the five randomness tests of security measures represented by frequency test, serial test, pocker test, run test and autocorrelation test. The using of these measures created a full stochastic, secure, and unique pattern which is difficult to guess by the third parties and robust enough against attackers. The proposed watermarking system can be used for proving the authenticity of owner and for protecting the original owner image. This is because it guaranteed a secure connection between the sender and the receiver, especially with the existing of the secondary pattern that is used to discover any tampering in the original cover image. The receiver can retrieve the pattern and invert the process to verify the originality of the image, and if the third party tries to tamper the embedded watermark it will be ambiguity and secure enough to suggest it .When embedding the pattern in the main diagonal of the cover image the resulted watermark from the embedding process is imperceptible and invisible and the cover image is same as the original without any change.

References:

- [1] S. S. Sudha, K. K. Rahini , "Prevention of watermarking attacks using cryptography method", International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, No.2, pp. 5050-5053, 2014.
- [2] K. Ramanjaneyulu, K. Rajarajeswari, "An oblivious and robust multiple image watermarking scheme using genetic algorithm", International journal of multimedia & its applications vol.2, No.3, pp.167-174, 2010.
- [3] C.Chin Lai," A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", Digital Signal Processing, www.elsevier.com/locate/dsp, Vol. 21, No.4, pp. 522–527, 2011.
- [4] J. Aguilar, J. Anderson, "A Neural Watermark Approach", Electronic notes in Theoretical computer science, 281 (2011), pp. 35–50.
- [5] S. Mohammadi Ziabari, R. Ebrahimi Atani, K. Keyghobad, A. Riazi, "The Optimized Image Watermarking Using Genetic Algorithm", Current Trends in Technology and Science, Vol. 2, No.6, pp. 359-363, 2013.
- [6] N. Mohananthini, G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms", Journal of Electrical Systems and Information Technology, Vol. 3,pp. 68–80,2016.
- [7] B. Saadon Mahdi, "Hybrid Techniques for Proposed Intelligent Digital Image Watermarking", Eng. & Tech. Journal, Vol. 33, Part (B), No.4, pp.702-713, 2015.
- [8] W. Song, Xi. Sun, C. Liu, L. Tang, "A New Watermarking Frame Based on the Genetic Algorithms and Wavelet Packet Decomposition", Vol. 6, No.3, pp. 613-621, 2015.

اقتراح نظام العلامة المائية باستخدام الخوارزمية الجينية ومقاييس الأمنية

أ.م.د. إسرائ عبد الامير

ch_israa81@yahoo.com,

110033@uotechnology.edu.iq

الجامعة التكنولوجية - قسم علوم الحاسوب - بغداد - العراق

ولاء ضياء عبد الغفور

walaadiaa90@yahoo.com

الجامعة التكنولوجية - قسم علوم الحاسوب - بغداد - العراق

المستخلص

هذه الورقة قدمت طريقة مائية مقترحة تستخدم لحماية الصور من العبث من قبل المهاجمين والأطراف الثالثة الأخرى. وهي تتكون من ثلاث مراحل: توليد النمط، تضمين العلامة المائية واستخراج العلامة المائية. في المرحلة الأولى، يتم إنشاء نمطين (الابتدائي والثانوي) من بعض ميزات الصورة التي تستخدم كعلامة مائية، ثم تطبيق خوارزمية جينية للحصول على نمط أساسي عشوائي وفريد وقوي، وهذا النمط الفريد الذي يتم إنشاؤه من الصورة المستخدمة كعلامة مائية وتضمين هذا النمط في صورة الغلاف الأصلي بدلا من تضمين الصورة المائية بأكملها داخل صورة الغلاف. هذا النمط هو 64 بت التي تم إنشاؤها باستخدام خوارزمية جينية واختيارها بعد اجتياز اختبارات العشوائية الخمسة. سيتم تضمين النمط الأساسي في ثلاثة مواقع مختلفة (القطر الرئيسي، الخط العمودي والأفقي في منتصف صورة الغلاف)، بالإضافة إلى توليد وتضمين النمط الثانوي الذي يستخدم للتأكيد بين المرسل والمستلم وإذا كان هذا النمط غير متطابق المستلم يقوم بإخبار المرسل بإعادة إرسال الصورة مرة أخرى. تم تطبيق تجارب مختلفة لاختبار هذا النظام والنتائج تظهر ان العلامة المائية عشوائية، غير محسوسة وقوية بما فيه الكفاية ضد هجمات الاقتصاص للصورة، آمنة تماما، وقيمة ذروة الإشارة الى نسبة

الضوضاء لصورة العلامة مائبة أفضل من صور العلامة المائبة للعديد من نظام
العلامات المائبة السابقة عند المقارنة معهم.

الكلمات الرئيسية: النمط الاولي، النمط الثانوي، الخوارزمية الجينية، تضمين العلامة
المائية، استخلاص العلامة المائية، ذروة الإشارة الى نسبة الضوضاء، هجوم
الاقتصاص للصورة، إختبار العشوائية.