Proposed Watermarking Technique to Protect Image Using Genetic Algorithm

Israa A. AbdulJabbar* ,Ph.D.(Asst.Prof.) Wala'a D. AbdulGhafor*

Abstract

This paper presents a proposed watermarking technique used for protecting images from tampering by the attackers and other third parties. This technique is consisting of three stages: pattern generation, watermark embedding and watermarking extracting. In proposed work, 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 patterns, the primary pattern will be embedded in the main diagonal of the cover image. In addition to generate and embed the secondary pattern in the secondary diagonal of the cover image, the purpose of secondary pattern is to ensure a secure connection between the sender and the receiver. When the sender sends the image, the recipient at first extract the secondary pattern, if this pattern is matched with original embedded one, this mean the image are kept from attackers and the receiver can extract the primary pattern, and, if the secondary pattern not matched, the recipient tells the sender to resend the image again. As a result the proposed technique gives good results when applied on different cover images, since the embedded watermark is imperceptible and unique enough to detect the tamper.

Keywoeds : Image watermarking ; genetic algorithm ; primary pattern ; secondary pattern ; watermark embedding ; watermarking extracting

*University of Technology

1. Introduction

With the advances of technology, it is easy to contact the Internet, as well as become easily to send and receive different types of files, such as images, audio, video. But sending these files via internet is not secure, someone can modify or tampering these files, so there must be a technique to protect these files that are sent over the Internet. Watermarking is one of these techniques to protect the personal property from tampering by attackers through adding watermark to media files images, video and audio. [1]

This watermark must be hard to remove by attackers and in the same time there is no distortion in the image after embedding the watermark. A cover image is the digital image that will be used to contain watermark image. Watermark image is the image that embedded into cover image. [2]

There are two types of digital image watermarking: non blind watermarking and blind watermarking. Non blind watermarking mean that the watermark image contain visible watermark, while blind mean that the watermarking contain non visible watermark. [2]

The digital image watermarking contains three steps: embedding step, transmission step, and extracting step. In embedding step the watermark image is embedding in cover image, in transmission step the sender send watermarked image to recipient via internet, the extracting step the recipient extract the watermark from cover image. [3]

Through these years optimization algorithm have been used for watermarking because this algorithms have the ability to find the best solution. Genetic algorithm is one of the most important of these algorithms. Genetic algorithm has been used in many problems of watermarking optimization and various watermarking domains. [4]

The parameters are represented through encode binary string that called chromosome, and the elements that is in the binary string or genes have been adjusted to minimize or maximize the fitness values. The fitness function has been selected according to particular application and the type of optimization required. The process of genetic algorithm has been started with a set of proposed solutions that are generated randomly and try to produce other possible solutions to realize the desired optimization. This is the reason of wide application uses the genetic algorithm in optimizations areas. [5]

There are many researches produced digital image watermarking techniques, some of them are mentioned below:
Memon , N.D. Memon , P.W. Wong (2001) [6] introduced a buyer-seller technique. This work is proposed to embed watermark by third party instead of buyer or seller. The embedding watermark is done by third party to prevent false accusations of violation by seller. And this is to save original image from expose to third party.

Cauvery N. K. (2011) [7] proposed a technique that utilize genetic algorithm to satisfy robustness and fidelity, in this technique the image is divided into three parts that is refer to its color (R,G,B) and use genetic algorithm to generate key of 64bit,the set of bits inside key represent positions in image that indicate the embedded watermark.

Venkatesan et al. (2012) [8] presented a new technique for (GA) that depend on the center of mass selection operator (CMGA) to obtain optimal location for inserting watermark in cover image, by concentration on fidelity optimization.

Sridevi T,S Semeen Fatima (2013) [9] proposed watermark algorithm that utilize (GA) and discrete wavelet transformation to improved robustness and fidelity of watermarked image and used fuzzy inference system to satisfy the strength of embedding rely on human visual system(HVS) properties for image. The algorithm gives better results and good quality for the watermark image.

N. Mohananthini , G. Yamuna (2015) [10] present a comparison of digital watermarking techniques using genetic algorithms. This method explains the main three categories of multiple watermarking techniques like segmented, successive, and composite watermarking. They are using genetic algorithm to optimize (maximize performance) the results of both peak signal to noise ratio (PSNR) and normalized correlation (NC) in multiple watermarking techniques. The result improve that the multiple watermarking techniques be realized more robustness when compare it with single watermark techniques and also give good robustness and fidelity against attackers by using genetic algorithm.

AbdulAmeer I. Mallalah S. (2016) [11] Introduced watermarking protocol to protect digital image through producing copyright registration for any cover

image. The registration is done by the server for only one time for any input image and retaining the time and the date of the registration in a secure authentication process. This process used both encryption and digital signature to generate invisible embedded watermark as well as using visible watermark shown on the lower-right image corner.

This paper proposed a watermarking technique that embedded unique and robust primary and secondary patterns. These patterns that are generated from watermark image's features using genetic algorithm with full randomness security measures. The primary pattern is embedded in the main diagonal of the cover image and it will be the watermark. The secondary pattern is embedded in the secondary diagonal of the cover image which will be extracted later by the receiver to ensure a secure connection between sender and receiver as well as to ensure that there is no tampering in watermarking image.

2. Genetic Algorithm

The Genetic algorithm (GA) is search model depend on basis of the naturaly selection and genetics. Genetic algorithm in the first stage encode the variables of the problem to the limited length string of alphabets of the same problem, the string that is selected as a solution to the problem is called chromosome while the alphabets is referred as the genes and it is content value are called alleles. Genetic algorithm work by encoding the parameters of the problem instead of the parameters themselves like in the traditional optimization techniques. This is done in order to reach to the best solution of the problem and it will be need a measure to evaluate generated solutions and choose or reminded only the best solutions or near to the best solution for the problem. This can be done by a mathematical or objective function called fitness function used by genetic algorithm to guide the work to be near to the best solution or best solution for the problem.

Another thing important in the genetic algorithm is the population of the problem, unlike the traditional methods the genetic algorithm depend on the population selected solutions. The size of the population is usually determine by the user and it consider as one of the important factor that effected the work of genetic algorithm and its performance. For example, if the size was small, this may be getting defective solutions of the problem.

Otherwise, it may be taking needless expenses of valuable computing time. [12] the steps of GA is described below [12] :-

1-**Initialization step:** initial population is generating randomly through the search space.
2-**Evaluation step:** after initialization step of the population the fitness values for filtered solutions are evaluating.
3-**Selection step:** combines more copies of solutions that have the best fitness values and then select best solution from the candidate solutions.
4-**Recombination step:** incorporate two or more parental solutions to generate new solutions, may be better solutions.
5**-Mutation step**: is randomly modifies a solution. There are several distinctions of mutation, but it generally include one or more changed to the individual's trait or traits.
6-**Replacement step:** in this step the population that is generated from selection, recombination and mutation is replace with original parental population. There are several techniques for replacement like generation-wise replacement, steady-state replacement methods and elitist replacement.
7-**Repeat** the steps from 2 to 6 until termination condition is met.

3-The Proposed Technique

As mentioned before, the proposed technique consist three steps which are: the first step is generating pattern from watermark image by using genetic algorithm and generating secondary pattern that is used to confirm between sender and receiver, the second step is embedding the two patterns in different locations of cover image, and the third step is extracting these patterns from the specific locations.

In the first step the histogram of the watermark image is computed with its properties. Here, these properties are used to represent probability, mean, standard derivation, energy and entropy. Each property generated 8-bit value length, after that mean and median filters have been applied on the same watermark image to obtain three 8-bit values length, finally these eight values converting to binary representation which will be represent the initial GA population. The fitness function of the proposed genetic algorithm is a five randomness tests security. [13] These test security are:

frequency, serial, pocker, run and autocorrelation test. The criteria of GA applied here will be stopped only when the 64-bit pattern passing all these security tests. If the pattern fails to pass one of these tests, the genetic algorithm will be repeated again until it get robust pattern pass all these tests. This pattern will be consider as the **primary pattern** and it will be used as invisible watermark. After that, the **secondary pattern** is generated, which will consist of eight values or information. These information will be a verification key between sender and receiver and used to discover any tampering through the transmission media.

In watermark embedding step, the primary pattern will be embedded in the main diagonal of a cover image and the secondary pattern will be embedded in the secondary diagonal of the same cover image.

In extracting step, when the receiver get the watermarking image, he/she first extract the secondary pattern and if it is extracted the same information sent by the sender, he/she, will extract the primary pattern from the main diagonal, else, the receiver notify the sender to resend the watermarking image again because of discovering a tamper in the watermarking image made by a third party. Fig.(1) and Fig.(2) show the block diagram of the proposed technique:

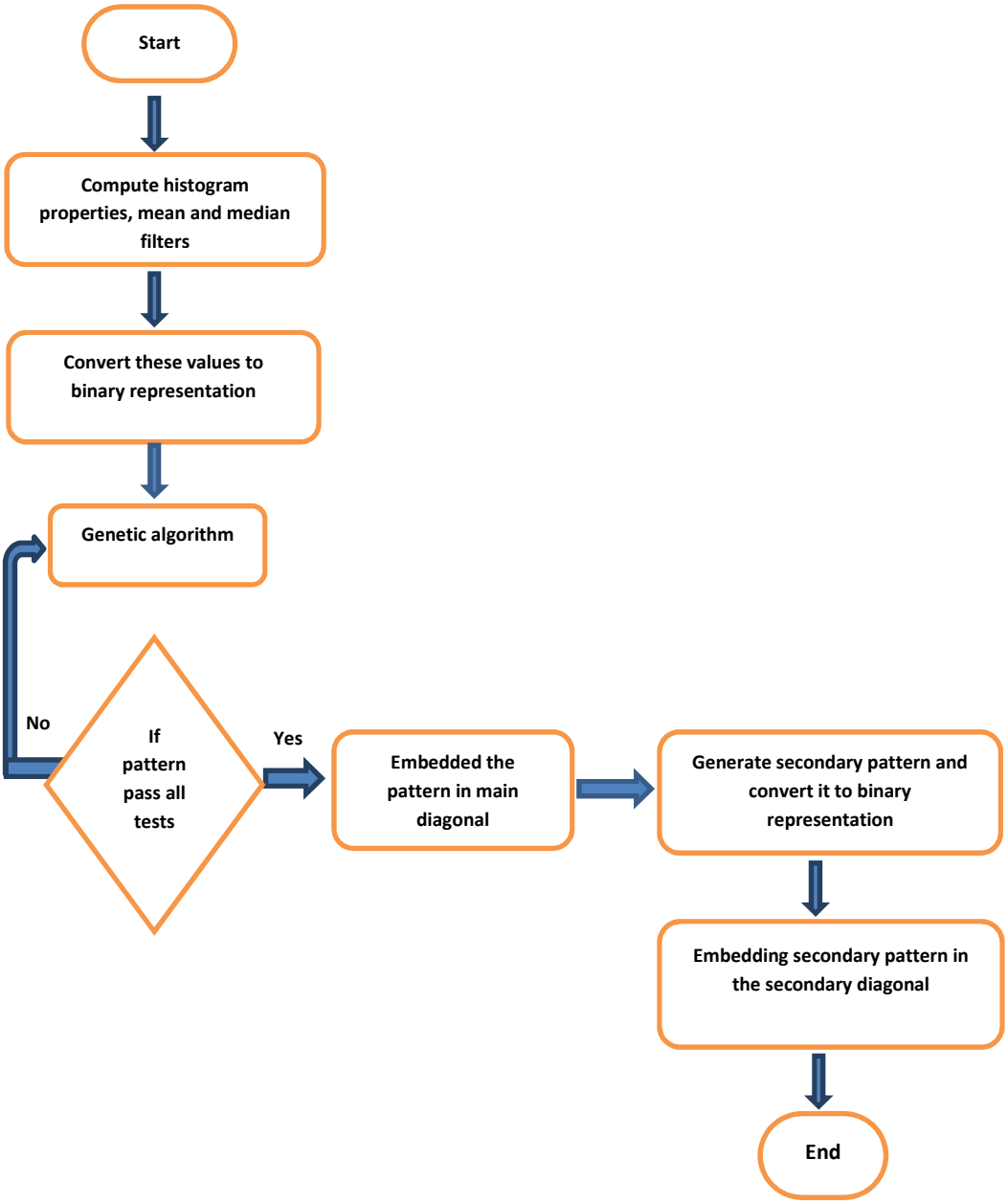

Figure 1: Block diagram of pattern generation and watermark embedding of the proposed technique

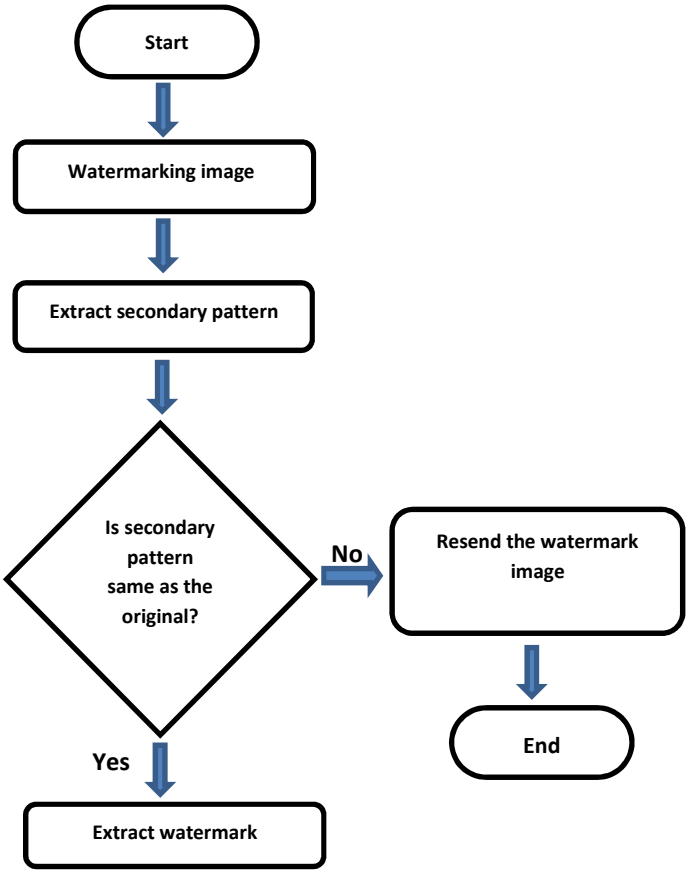

Figure 2: Block diagram of pattern verification and watermark extraction of the proposed technique

3.1 Pattern Generation

The pattern generation process has two stages as shown below:-

3.1.1 Primary Pattern Generation

The primary pattern is generated from the image and used as a watermark embedded in the cover image; this is done by using the genetic algorithm. At the beginning, the population of genetic algorithm is generated by compute the image histogram's properties as well as the mean and the median filters in order to generate a population of length 64 bits as shown below :-

histogram properties	binary coding
Probability=1	10000000
Mean=2	01000000
Standard derivation=3	11000000
Energy=4	00100000
Entropy=5	10100000
Mean filter=6	01100000
Median filter=7	11100000

The pattern become:

1000000001000000110000000010000010100000011000001110000 0

then this pattern represent the population of genetic algorithm to generate unique and strong pattern and more randomness that pass all the randomness tests.

3.1.2 Secondary Pattern Generation

The secondary pattern is generated to be the verification pattern between the sender and the receiver. This pattern is consist of information that is generated from genetic algorithm such as the way of randomness, number of crossover, number of mutation, mean and median filters values, number

of bit that is chosen to embed in it, ASCII code for letter (M and S) that is represent 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 64 bit secondary pattern of length for example:

Secondary pattern information's	**binary representation**
Number of random generation= 1	10000000
Number of crossover=2	01000000
Number of mutation=4	00100000
Mean filter value =10	01010000
Median filter value=15	11110000
bit number that embedded in it=7	11100000
ASCII code for M=109	11010110
ASCII code for S=115	01001110

The pattern become:
1000000001000000001000000101000011110000110101100100111 0

This pattern must be verified between the two parties and any bit missed this mean there is a tamper on watermarking image, so the receiver 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.

Algorithm (1): illustrate the process of embedding watermark

Input: Cover image

Output: Watermarking image

Process:

1- Compute the histogram of the image that will be used as a watermark.

2-Compute the properties of the histogram represented by mean, standard derivation, probability and entropy and the energy.

3-Convert these values to binary representations for getting string with 40 bit of length.

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 of 64-bit length.

5-Divided the final string to eight chromosomes with length of 8 bit to be the population of genetic algorithm.

6-Applying the genetic algorithm operators (selection, crossover and mutation) to generate new population.

7-Test the new population with randomness tests, here frequency test, serial test, pocker test, run test and autocorrelation test have been used.

8- If this population pass all these tests, the primary pattern that is embedded in the least significant bit of pixel in the main diagonal will be generated. This is done by replacing the first bit of image pixel with one bit of pattern and then converting this new binary value to decimal value then combine it with value of the same pixel for example:

Pixel value=193436**8** bit value that want to embedded =1

Binary representation of 8 = 00010000

After embedding the bit it become =10010000, converting it to decimal value it become=9

then the new value of pixel =1934369

9- Embed secondary pattern in the secondary diagonal of cover image by use the same embedding way.

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.

The process of watermark verification and extracting is shown in Algorithm (2).

Algorithm (2): Watermark Verification and Extracting Procedure

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.
2- If the pattern is same as the original pattern that is sent by the sender go to next step,
else, the receiver tells the sender to resend the watermarking image again and repeat step
3- Extracting the first pattern from embedding location (main diagonal).
4- Compute the histogram of the image to be used as a watermark.
5- Compute the properties of the histogram mean, standard derivation, probability, entropy and energy.
6- Convert these values to binary representation to get string with 40 bit length.
7- 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.
8- Dividing the final string to eight chromosomes with 8 bit length to be the population of genetic algorithm.
9- Applying GA operators, selection, crossover and mutation to generate the new population.
10- Test the new population with the five security measures.

11-If the pattern passing all the randomness tests, this mean that the result of step 3 matched the result of GA and the watermark will be retrieve.

4. Experimental result

To implement the proposed watermarking technique, the sender select the image that used as watermark image and computing its histogram then applied mean and median filters as shown in fig (3)

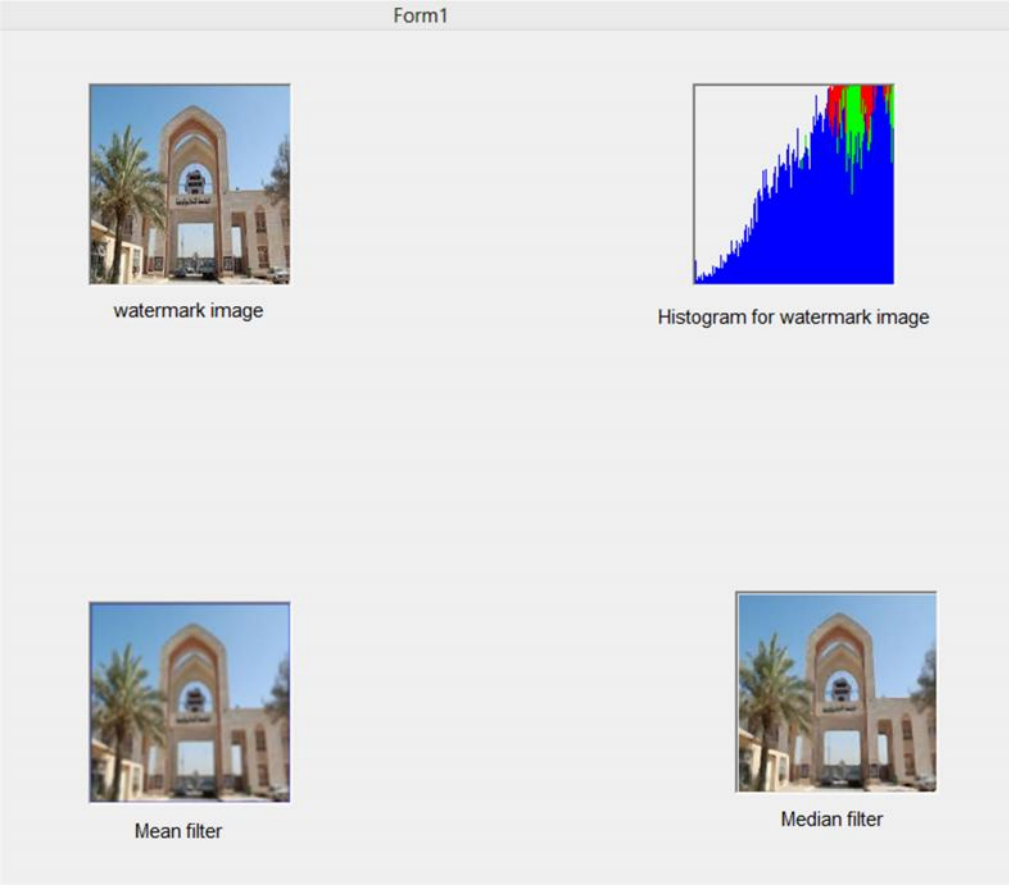

Figure3: watermark image and histogram.

Mean and Median filters for watermark image to generate pattern with 24 bit of le

After that the histogram properties have been computed to generate the 64-bit pattern using genetic algorithm as shown in fig (4).

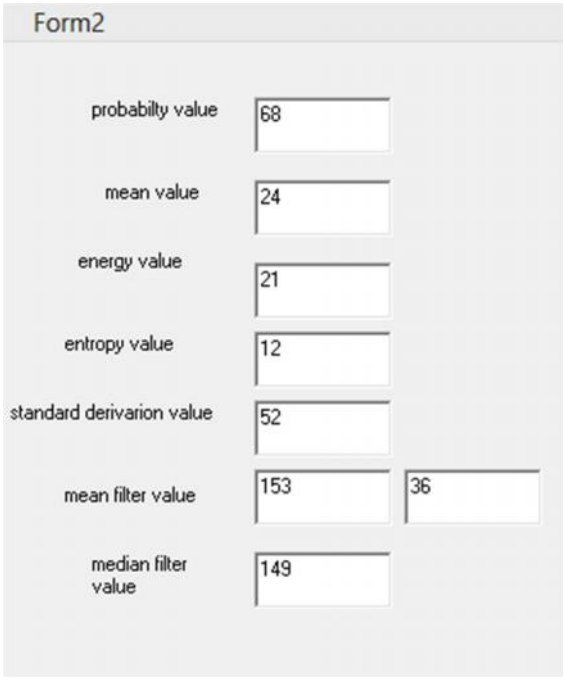

Figure 4: the histogram with five values of its properties and three values of mean and median filters values.

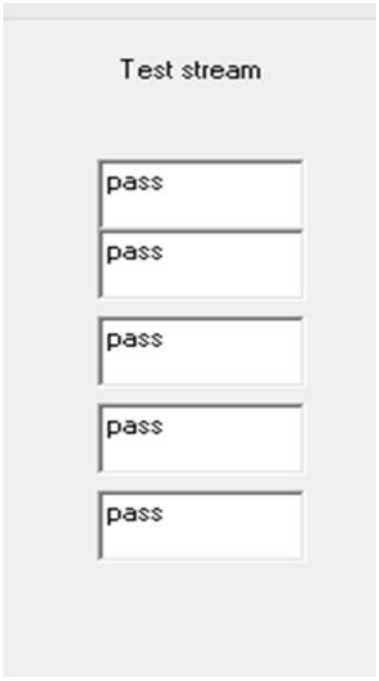

Figure 5: Test stream result

Figure (5) show the security test that have been used in order to select the pattern that must be pass all of these test.
To show the embedding process, university of technology image is used as original cover image as indicated in figure (6) and the final result of embedding is shown in figure (7) where the two patterns are embedded in the main and secondary diagonals of the cover image using LSB method.

Figure 6: Cover image

Figure 7: After embedding primary and secondary patterns

Figure (8) shows the process of watermarking retrieval from the watermarking image. First, the secondary pattern is verified correctly then the primary one is retrieved.

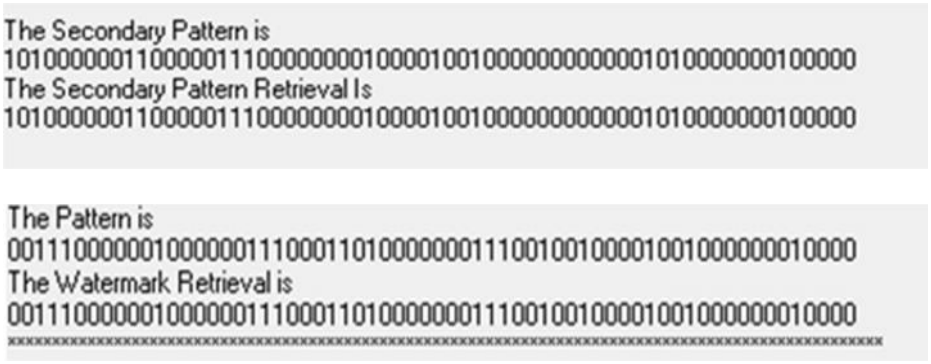

Figure 8: primary, secondary patterns and its retrieval

5- Conclusions

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

The purpose of using of genetic algorithm is to generate intelligent binary code of 64-bit length for each pattern. The generated pattern is selected after passing all the five randomness security test measures represented by frequency test, serial test, pocker test, run test and autocorrelation test. Using of these measures will create a full stochastic, secure and unique pattern which is difficult to guess by the third parties.

The proposed watermarking technique can be used for intrusion detection purposes and for protecting the original owner image, this is because is guaranteed a secure and an intelligent 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.

6- Future works

Some suggestions are given below to increase the optimality of watermarking technique as future works :

1- Evaluate the robustness of the proposed technique using many evaluation measures like peak signal to noise ratio PSNR, mean square error MSE, and Normalized Correlation NC to compare the watermarked image against the original image.
2- Embedding the pattern generated by the proposed GA using swarm intelligence optimization instead of embedding it in the main diagonal of image to increase the randomness of the watermark position in the image.
3- Using biometric features like fingerprint, iris or palm as a pattern to protect the owner image and embedded it using discrete wavelet transform DWT or any other watermarking technique.

References

[1]- Hai Tao, Li Chongmin, Jasni Mohamad Zain, Ahmed N. Abdalla , "Robust Image Watermarking Theories and Techniques",A Review" Journal of Applied Research and Technology, Vol. 12, pp 122-138, 2014.

[2]- Rafael C. Gonzalez , Richard Wood , "Digital Image Processing", Third Edition, Pearson Education, 2011 .

[3]-Sudhanshu Suhas Gonge, Ashok Ghatol, "A Robust and Secure DWTSVD Digital Image Watermarking Using Encrypted Watermark for Copyright Protection of Cheque Image", Springer International Publishing Switzerland, pp 290-303, 2015.

[4]- Seyed Sahand, Reza Ebrahimi, Kiyan Keyghobad, Abdolmajid Riazi, " The Optimized Image Watermarking Using Genetic Algorithm", Current Trends in Technology and Science ,ISSN : 2279-0535. Volume (II),Issue VI,pp 359-363,2013.

[5]- Sachin Goyal, Roopam Gupta, Ashish Bansal," Application of Genetic Algorithm to Optimize Robustness and Fidelity of Watermarked Images", /International Journal on Computer Science and Engineering Vol.1(3),239-242,2009.

[6]- Memon et al , N. D. Memon , P.W. Wong "A buyer-seller watermarking protocol". IEEE Trans. Image Process., pp. 643–649, 2001.

[7]-Cauvery N K, "Water Marking on Digital Image using Genetic Algorithm", IJCSI International Journal on Computer Science Issues Vol 8, Issue 6, No 2, Nov 2011, pp. 323-331, ISSN(online):1694-0814.

[8]-Venkatesan and K. Kannan and S. Raja Balachandar," optimizatuon of fidelity in digital image watermarking using a new genetic algorithm ",2012,Vol. 6, ,No.73,pp. 3607-3614.

[9]-T. Sridevi and S. Semeen Fatima," Watermarking Algorithm using Genetic Algorithm and HVS", International Journal of Computer Applications ,2013, Vol.74, No.13,pp.26-30.

[10]-N. Mohananthini and G. Yamuna. "Comparison of multiple watermarking techniques using genetic algorithms." Journal of Electrical Systems and Information Technology (2016).

[11]- AbdulAmeer I. and Malallah S., " Copyright Protection Service for Mobile Images " , Eng. and Tech. Journal, Vol.34,Part (B), No.4, 2016.

[12]- Sastry, Kumara, David E. Goldberg, and Graham Kendall. "Genetic algorithms: Search methodologies" Springer US, 2014. pp. 93-117.

[13]-Tanya Abdul Sattar, "Security approach for information exchange", university of technology ,department of computer science, thesis 2016.

اقتراح تقنية العلامة المائية لحماية الصورة باستخدام الخوارزمية الجينية

أ.م.د. اسراء عبد الامير عبد الجبار ولاء ضياء عبد الغفور

المستخلص

هذا البحث يقترح تقنية العلامة المائية لحماية الصور من التلاعب بها من باستخدام الخوارزمية الجينية. هذه التقنية تتكون من ثلاث مراحل: توليد النمط، تضمين العلامة المائية واسترجاعها. في هذا البحث تم اقتراح نمطين (أولي وثانوي) من بعض خصائص الصورة التي سيتم استخدامها كعلامة مائية ثم يتم تطبيق الخوارزمية الجينية للحصول على أنماط عشوائية، فريدة وقوية، سوف يتم تضمين النمط الأولي الناتج في القطر الرئيسي من صورة الغلاف. بالإضافة إلى توليد نمط ثانوي يضاف في القطر الثانوي من صورة الغلاف، والغرض من النمط الثانوي هو لضمان تأمين اتصال آمن بين المرسل والمستلم. عندما يرسل المرسل الصورة المضاف اليها العلامة المائية يقوم المتلقي في استرجاع النمط الثانوي أولا فإذا تطابق هذا النمط مع النمط المتفق عليه بينهما مسبقا ، هذا يعني ان الصورة لم يتم التلاعب بها من قبل المهاجمين والمستلم يمكنه استرجاع النمط الأساسي , اما إذا كان النمط الثانوي غير متطابق فان المستلم يرسل إشعار إلى المرسل ليخبره بإعادة إرسال الصورة مرة أخرى. التقنية المقترحة أعطت نتائج جيدة عند تطبيقها على صور مختلفة وذلك لان العلامة المائية المضافة غير مرئية وقوية بما يكفي لكشف التلاعب.

* الجامعة التكنولوجية