Hybrid Techniques for Proposed Intelligent Digital Image Watermarking

Bashar S Mahdi .
Computer Science Department,University of technology /Baghdad.
Email:basharsadoon@yahoo.com
Dr. Alia K Abdul Hassan.
Computer Science Department ,University of technology /Baghdad.

Revised on:24/9/2014 & Accepted on: 7/5/2015

Abstract

Digital watermarking provides a solution of the recent problems such as a copyright protection and digital content authentication, as well as the balancing between the copyright protection and authentication requirements are the challenge of the many watermarking methods. In this paper, which is proposed a new intelligent watermarking method to solve that problem by using proposed hybrid techniques.

The proposed method can be describe by three phases, first one is employ the hybrid approach of visual cryptography and one way hash function which providing the security and authenticity to the watermarking system. Second one is concerned with intelligent embedding of watermark data in the cover image data by using three basics techniques which are the genetic algorithm, artificial neural networks and the human visual system model which obtains the effective balancing between the robustness and imperceptibility of the digital image using the middle frequency coefficients. Finally phase is depending on the extracting of the encrypted watermark by using the same operations of embedding stage and by using the overlapping approach in the visual cryptography. Experimental results demonstrates that the proposed method provides a secure adaptive intelligent system which can apply in the different filed of application that need the reliable copyright protection with highly security and authenticity. Moreover, Obtaining a highly balancing among imperceptibility, robustness and security, that are showed by surviving the extracted watermark from different types of malicious and adaptive attacks.

Keywords: Watermarking, DCT,DWT, Genetic Programming, Visual cryptography, Hash function, Neural network, HVS.

تقنيات هجينة لاقتراح علامة مائية ذكية للصورة الرقمية

الخلاصة

تقنية العلامة المائية توفر الحل للمشاكل الحالية المتمثلة بحماية حقوق الملكية والتخويل للمحتويات الرقمية, بالاضافة الى ان التوازن بين متطلبات كل من حماية الملكية والتخويل الرقمي يعتبر من التحديات لكثير من طرق العلامة المائية. في هذا البحث تم اقتراح طريقة جديدة ذكية للعلامة المائية لحل تلك المشاكل باستخدام تقنيات هجينة

https://doi.org/10.30684/etj.33.4B.13
2412-0758/University of Technology-Iraq, Baghdad, Iraq

مقترحة .الطريقة المقترحة يمكن وصفها بثلاثة مراحل, المرحلة الاولى تتم بتوظيف طريقة هجينة لتشفير المرئي وكذلك الدالة التراكمية ذات الاتجاه الواحد والتي توفر بدورها السرية وتخويل لنظام العلامة المائية. المرحلة الثانية تتعلق بطريقة الاخفاء الذكية للعلامة المائية داخل بيانات الصورة الاصلية باستخدام ثلاثة تقنيات رئيسية وهي الخوارزمية الجينية, شبكات العصبية الاصطناعية وكذلك النظام المرئي البشري والتي تحقق التوازن الفعال بين القوة وعدم الادراك للصورة الرقمية باستخدام معاملات الترددات الوسطية. المرحلة الاخيرة تعتمد على استخراج العلامة المائية المشفرة باستخدام نفس التقنيات المستخدمة في مرحلة الاخفاء وكذلك باستخدام تقنية التداخل بواسطة التشفير المرئي. النتائج التجريبية اظهرت بان الطريقة المقترحة توفر نظام ذكي وامني وله قابلية التكيف والذي بالامكان تطبيقة على مجالات تطبيقية مختلفة والتي تحتاج الى حماية ملكية ذات موثوقية وامنية وتخويل بالاضافة الى ان النظام قد حقق التوازن العالي بين المكونات الثلاثة الرئيسية وهي عدم الادراك, القوة,والامنية والتي تظهر بمقاومة ونجاة العلامة المائية المستخرجة من انواع مختلفة من الهجومات الفعالة والخبيثة.

INTRODUCTION

Personal computers and internet connections made the distribution of digital data (text, sound, and image)and applications easy and fast that leads to appear the problem of copying and transmitting of the digital products illegally without any authentication . The effective way to protect the digital media from the these problems is a digital watermarking, which define as a technique where the secret information was embedded into the host media to provide the host media ownership and decreasing unauthorized copying [1]. There are two types of digital watermark which represents as a visible or invisible watermark that is embedded into the original cover [2]. Current techniques of digital watermarking can be classified into two main classes: spatial and frequency domain watermarking techniques[3,4]. Frequency domain watermarking techniques provides more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms compared with spatial domain [5]. The most popular technique of special domain is the least significant bit (LSB) method [6], However, frequency domain [7] which is used in the digital image watermarking that provides excellent spatial localization and multiresolution characteristics that are same to the human visual system model[8]. Further performance improvements in DWT-based digital image watermarking algorithms could be obtained by combining DWT with DCT[9]. In the related work Chin-Chen Chang et al [10] also suggested spatial- domain image hiding schemes to hide a binary watermarking into two shares. Embedding images can be superimposed to decode the hidden messages [11]. Zhang [12] proposed a RBF neural network to achieve maximum-strength watermark according to the frequency component of the cover image. Liu [13] also proposed a watermarking scheme based on RBF neural network. In this paper, One of the problem which deal with watermark security and authentically is solved by using hybrid techniques of the proposed method. The rest of the paper is organized as follows. The proposed methods in three phases : phase one related with hybrid visual cryptographic and one-way hash function. Intelligent embedding techniques are presented in phase two. Watermark extracting which is explained in phase three. Section 3 explains the evaluation functions of system. Then, experimental results are described in Section 4. Finally, in Section 5 which is showed the paper conclusions.

The Proposed Method

The proposed method general architecture which including three phases: The first one described the generating of two public and secret image from the watermark image, second phase is showed the intelligent embedding for the watermark, final phase is depended on the extracting of the watermark from the watermarked image.

Phase 1: Hybrid Visual Cryptographic and One-way Hash Function:
Visual cryptography is a type of encryption methods which can coding every pixel of binary image i to two shares [14]. Typically, visual cryptography decomposes every pixel in a secret image into a (2×2) block in the two images share according to the rules in Figure 1.

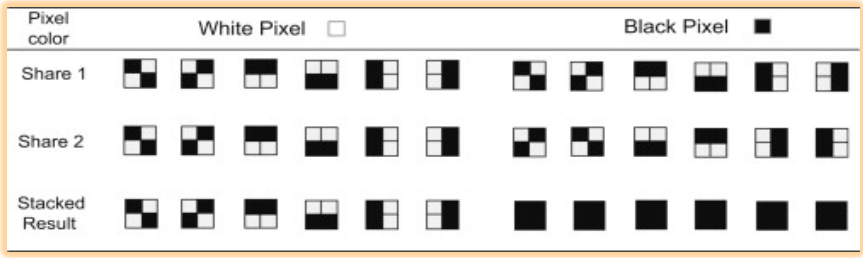

Figure (1): Visual cryptography sharing and stacking of pixels

In the first phase, visual cryptography encryption will be carried out. It consists of generation of shares using the hybrid techniques. In our scheme, VC share creation is performed. Every pixel in watermarked image is broken into four sub pixels, by using this scheme which are encrypted each pixel of the image. Any single share is highly secure and is chosen by using keyed hashing (SHA1) function that shown in Figure 2.
A one-way hash function which depends on secret key is called Message Authentication Code [15]. There are two functions which are used in the proposed system and depend on SHA1 function.

- $Hash1(P,K) = H(K\&(P\&H(K)))$ (1)

- $M = Hash1(P,K) \bmod NS$ (2)

Where
a secret key known only to the owner is represented by K, concatenation operation is represented by &, P is a pixel position, NS is number of share and M is index of selected share.

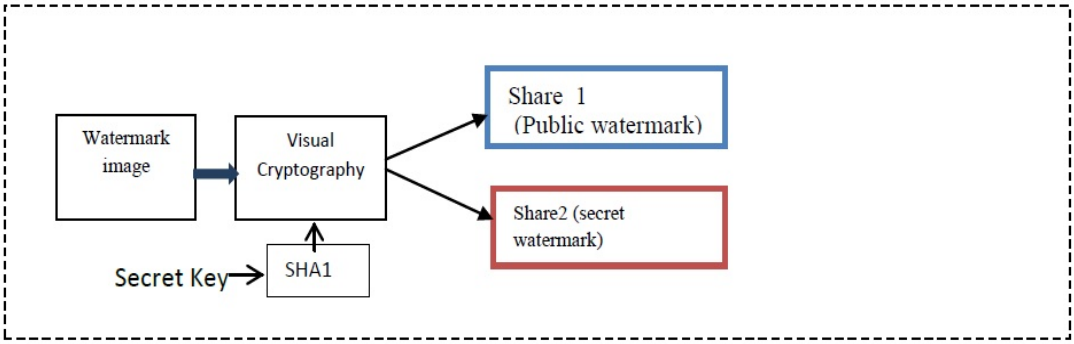

Figure (2): Hybrid visual cryptography and hashing

Phase2:Intelligent Embedding Techniques

The phase two of proposed method aimed to providing the adaptive intelligent embedding by using hybrid of three techniques are human visual system, genetic algorithm and artificial neural network which described in the following points with general proposed embedding algorithm:

Human Visual System Model

There are three main properties of HVS model in DCT domain are: luminance ,frequency sensitivity and masking effects. Where the luminance sensitivity is measures the threshold detectibility of constant background noise. The frequency sensitivity is the human's eye sensitivity to different spatial frequencies. Masking regarded as the effect of visibility decreasing of one signal to another signal called masker[16]. In the proposed method will focus on the brightness, texture and entropy sensitivity. The luminance sensitivity(LS) is compute by using Eq.(3)

$$LSt = \left(LDC,t \,/\, \overline{LDC,t} \right)^{\Upsilon} \quad (3)$$

where

LDC,t represents the DC coefficient of the t^{th} block of DCT blocks and LDC,t is regards as the mean value DC coefficients for all blocks of an image, and Υ is used to control of luminance sensitivity degree.

As will known the image divided into three types of blocks are: smooth blocks, textured blocks, and edge blocks[17]. The texture sensitivity can be calculated by the Eqs.(4,5):

$$G = (Yt(i,j) \,/ Q(i,j)) \quad (4)$$

$$TSt = \sum_{i,j=0}^{7} Round\,(G) \quad (5)$$

Where

$Yt(i,j)$ is represented the t^{th} block of DCT coefficients and Round (G) takes the rounded value of G and returns '1' if the value is not equal to zero, '0' otherwise.

The amount of the information in the block represents the entropy value of image blocks which employ to sorting image blocks according to value of entropy. The entropy value is various from block to other. The entropy sensitivity is calculated by Eq.(6) :-

$$ESt=\sum_{i,j=0}^{7} Pt(i,j).\log\frac{1}{Pt(i,j)} \quad (6)$$

$$Pt\ (i,j) = \frac{Yt(i,j)}{\sum_{i,j=0}^{7} Yt(i,j)} \quad (7)$$

Where
$Yt(i,j)$ represented to the t^{th} block of DCT coefficients of the position (i,j).

Genetic Algorithm and Neural Network

GA is algorithm of stochastic seeking which is depended on the natural genetic mechanism, and is extremely proficient in searching of optimum solutions.

ANNs are effective apparatuses that provide an perfect selection and classification procedure with high-speed computation [18].

ANN may be applied here to detect the desired adaptive embedding weight of the watermarking system, based on the feature of the HVS model . The embedding process is formulated as follows:

$$\tilde{A}i,j,k=Ai,j,k(1+\alpha i,j,k * Wi,j,k) \quad (8)$$

Where
A *i,j,k,* denotes the DCT coefficient of the position (i, j) of the Kth block, and $\alpha i,j,k$ is the adaptive weight of watermark W *i,j,k,* in the position (i, j) of the Kth blocks.
In Figure 3 represent the architecture of applied ANN where C is HVS feature vector = (c1,c2 ,c3,) The c1 , c2 *and* c3 represent the sensitivity value of luminance, texture, and entropy of respectively as input layer.

In Figure 4 the flowchart for GA and ANN based watermark embedding is shown.

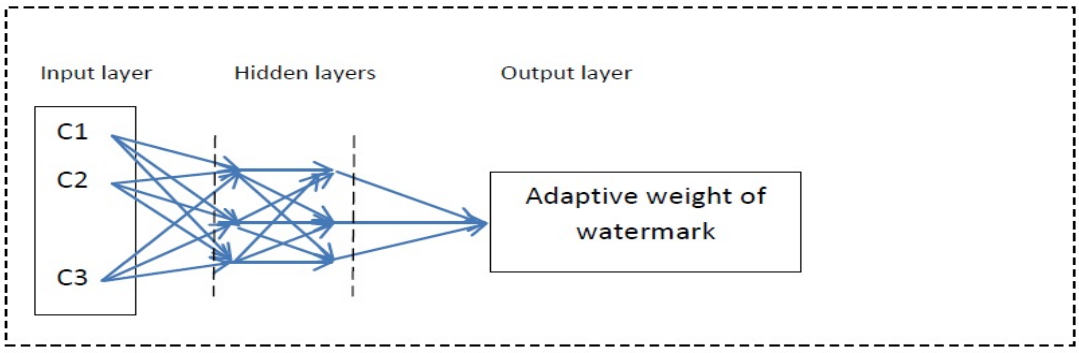

Figure (3):Architecture of applied ANN

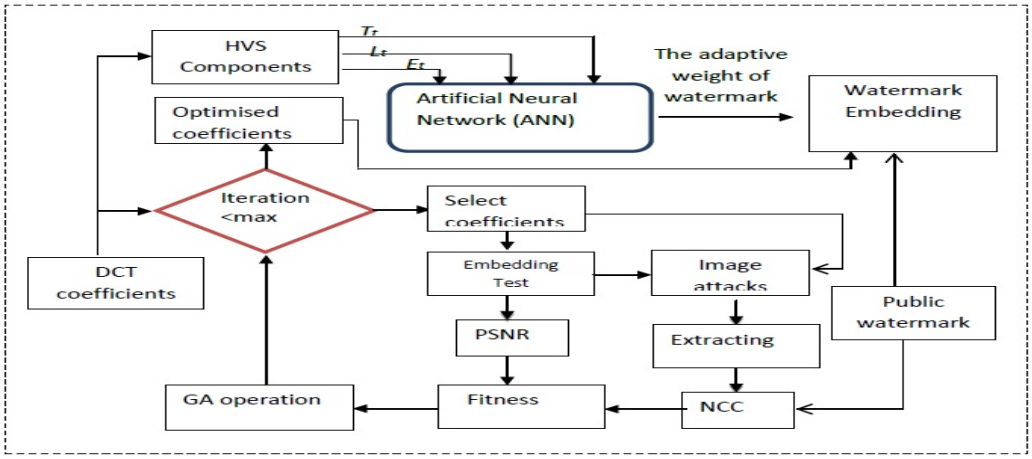

Figure (4): Proposed scheme using GA and ANN

Proposed Embedding Algorithm

The embedding of the generated public share from phase one which showed in Figure 5 ,where each steps of this figure which explained in the section A and B after that applied the embedding process in steps of algorithm .

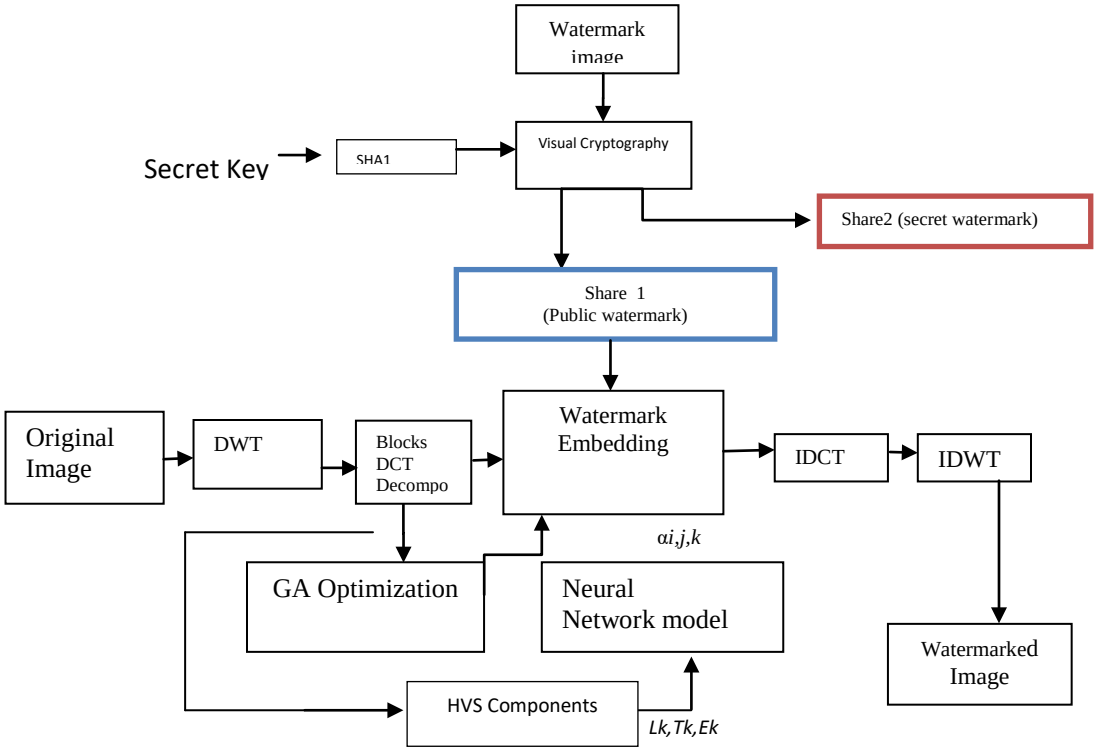

Figure (5):The proposed watermarking embedding scheme

Algorithm 1:Embedding Process
Input : public share, cover image.
Output: Watermarked image.
Step 1: Perform visual Cryptography (VC) by using keyed hash on watermark image to decompose two shares image one is public that used in embedding process and second is secret that is used in extraction process.
Step 2: Divide the cover image by using DWT into four non-overlapping sub-bands: LL1, HL1, LH1, and HH1.and then select only LH1, HL1, and decompose LL1 into four non-overlapping sub-bands LL2, HL2, LH2, HH2, and select LH2, HL2.
Step 3: Each sub-band HL1, LH 1, HL2, HL2 which divides into 8x8blocks.
Step 4: Perform DCT to each block.
Step 5: Select middle band coefficients of DCT by using GA optimization.
Step 6: Compute HVS components from selected coefficients (L,T,E) luminance, texture, and entropy sensitivity.
Step 7: Applied artificial network (BPNN) by using HVS components the output is the adaptive weight of watermark embedding.
Step8: Embed share 1 into selected coefficients with adaptive weight.
Step 9: Inverse DCT is applied on each 8x8 block.
Step 10: Inverse DWT is performed to produce the watermarked image.

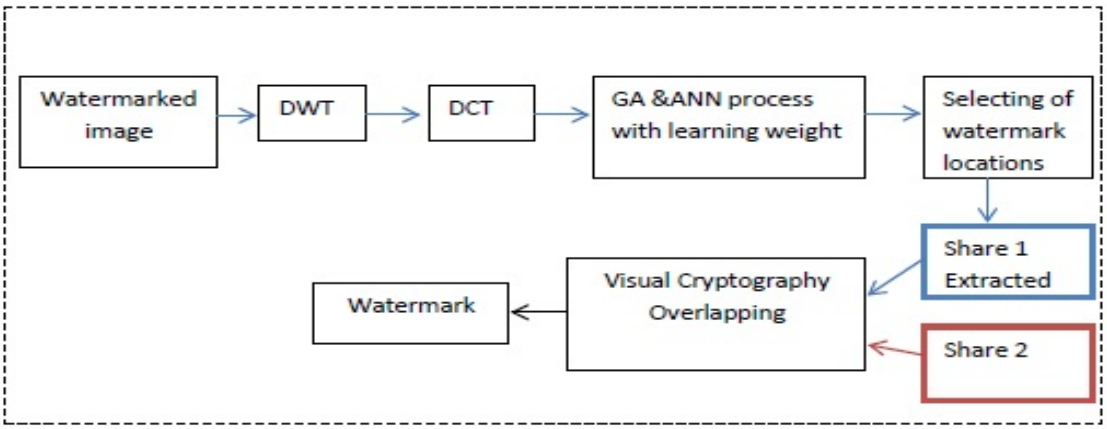

Figure (6):Block diagram of proposed watermarking extraction

Phase 3: Watermarking Extraction
In this phase the watermark is perform the proposed extracting procedure to extract the embedded watermark from the watermarked image, the watermarking extraction procedure is represented in Figure 6, followed by a step by step explanation as follows:

Algorithm2: Extracting Process
Step 1: The watermarked image which decompose it into four non-overlapping sub-bands by using DWT : LL1,HL1, LH1, and HH1.and then select only LH1, HL1, and

decompose LL1 into four non-overlapping sub-bands LL2, HL2, LH2,HH2,and select LH2,HL2.

Step 2: Each sub-band HL1, LH 1,HL2,HL2 divides into 8x8blocks.

Step 3: Perform DCT to each block.

Step 4: Select middle band coefficients of DCT by using GA optimization and by using ANN to select learning weight.

Step 5: Extract share 1 from selected coefficients.

Step 6: Perform Visual Cryptography VC and overlapped extracted share1 with secret share2, the result of overlapping will be a watermarked image.

Evaluation Function

The major function for evaluating the image imperceptibility are :Mean Square Error (MSE) and the Peak-Signal to Noise Ratio (PSNR) which shows in Eqs. (9,10) respectively.

$$\mathrm{MSE}(\mathbf{X}, \mathbf{X}') = \frac{\mathrm{ED}(\mathbf{X}, \mathbf{X}')}{M \times N}. \tag{9}$$

$$\mathrm{PSNR}(\mathbf{X}, \mathbf{X}') = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}(\mathbf{X}, \mathbf{X}')}. \tag{10}$$

where

X and X′ denote the original image and the watermarked image, the width and height of the images are represented by M and N, and the pixel at position (i, j) of X and X′ are represented by X(i, j) and X′(i,j) respectively[19].

The main function for evaluating the robustness is a Normalized Correction (NC) between the original and extracted watermark which is shows in in Eq.(11).

$$\mathrm{NC}(\mathbf{X}, \mathbf{X}') = \frac{\sum_i^M \sum_j^N (X(i,j) \times X'(i,j))}{\sum_i^M \sum_j^N (X(i,j)^2}. \tag{11}$$

Where

X and X′ denote the original watermark and the extracted watermark , the width and height of the images are represented by M and N, and the pixel at position (i, j) of X and X′ are represented by X(i, j) and X′(i,j) respectively[19].

Experimental Results

In our proposed work three important properties are evaluated . First is imperceptibility, second robustness and third security of watermark. The imperceptibility is employed by using genetic algorithm for optimizing and obtain the maximize Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross Correlation (NCC) of the extracted watermark. Security of watermark by using proposed visual cryptography by using hash function that mean split the watermark image into two share any single share was highly secure and by hashing chosen of two black and two white sub pixels.

The watermarking scheme has been tested on two images with size of 512x512 pixels. The watermark image is binary logo image32×32 by using MATLAB R2012b and visual basic.net to generate hashing value for each pixel of watermark image with secret key

and with position of it to select high secure and high randomly chosen one of many combinations for white and black pixels.

ANN with GA used to select perfects coefficients of DCT and weight for embedding the watermarked as shown in Figure 4. As mentioned above, various attacks that were shown in Figures 10, 11, 12,13 and 14 are used to test the imperceptibility, robustness and security of the watermarking of the proposed scheme.

The tested image is compressed using JPEG in different quality factors. Figure 7 shows the watermarked image under JPEG compression attack with quality factor 30% to 90%. As mentioned, the proposed algorithm robust against JPEG compression attack.

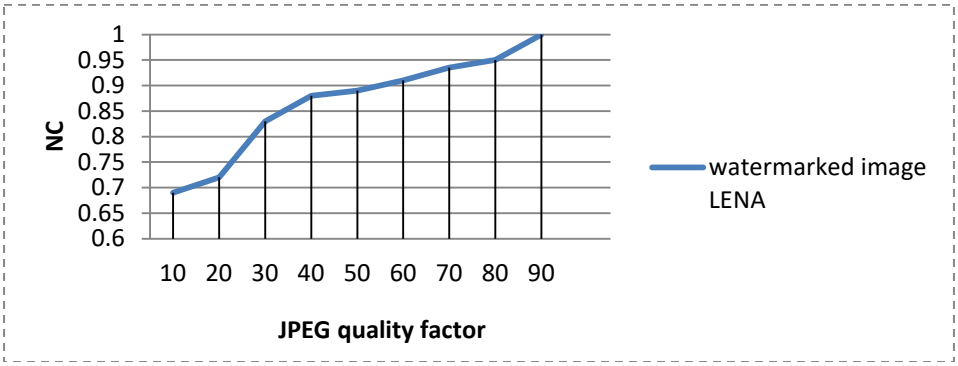

Figure (7):JPEG compression attack results

The proposed scheme in this paper is robust and secure against many attacks that depend on the final result of NCC that show in Table1.

Table (1) : The NCC parameter value for watermarked image under attacks

Different attacks	NCC=
Medianfilter(3x3)	0.9920
Rotation 90°	0.9901
Gaussian filter	0.9905
Image sharpening	0.9616
Scaling 30%	0.8852
Salt & pepper noise 0.025	0.9905
Cropping 0.25	0.9806

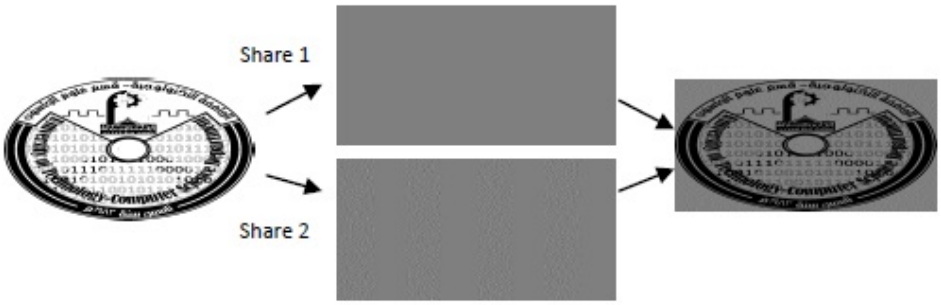

Figure (8): Visual Cryptography for watermark image

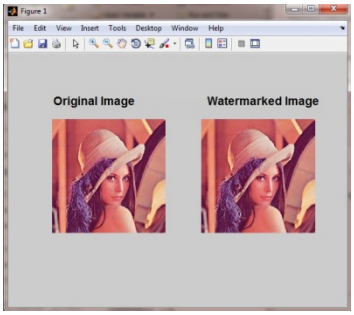

Figure (9): Original image and watermarked

(a) (b) (c)

Figure (10):(a) Watermarked image, (b) original watermark,(c)are the watermarking extraction without attacks NCC=1.

(a) (b)

Figure (11):(a) watermarked image, (b) the watermark extracting under attacks

(a) (b)

Figure 12:(a) watermarked Image, (b) watermark extracting under crop attacks

(a) (b)

Figure (13): (a) watermarked image,(b) watermark extracting Under Rotation attacks

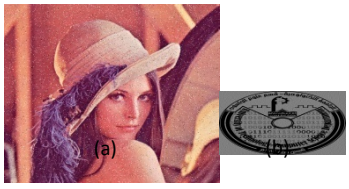

Figure (14):(a) watermarked Image, (b) watermark extracting under Salt & pepper noise attacks

Conclusions

Using a hybrid methods to obtain the effective balancing between robustness and imperceptibility of watermarked image which is enhanced during the process of watermark embedding by using genetic algorithm and artificial neural network. As well as improve the performance of conventional watermarking techniques by using characteristics of HVS which makes the watermark invisible and embedded adaptively. Providing a secure invisible watermark with authentically used based on Visual Cryptography and MAC , which uses only one share (public image) for imbedding and other shares (secret image) for extraction. The proposed method which obtains the high imperceptibility and robustness to the watermarked image while preserving the robustness with high security against various attacks such as low pass filtering, median filtering and JPEG compression, rotation , Scaling, Cropping, Salt & pepper noise and image sharpening .

References

[1] A. Khan, A. M. Mirza and A. Majid, "Optimizing Perceptual shaping of a digital watermark using
Genetic Programming", in Iranian Journal of Electrical and Computer Engineering (IJECE), vol. 3,
No. 2, pp 1251-1260, 2004

[2] A. Khan, A. M. Mirza and A. Majid, "Intelligent perceptual shaping of a digital watermark: exploit-
ing characteristics of human visual system", in International Journal of Knowledge-based Intelligent
Engineering Systems, (KES), vol. 9, pp. 1-11, 2005.
[3] B. Sikander, M. Ishtiaq, M. A. J, A. M. Mirza, "Adaptive digital image watermarking using
Genetic Algorithm" IEEE International Conference on Information Science and Applications (ICISA
2010), Seoul, Korea, April, 2010.
[4] Muhammad Ishtiaq, M. Arfan J., Muhammad A. Khan, Zahoor Jan, Anwar M. Mirza, Robust
and imperceptible watermarking of video streams for low power devices, Signal Processing, Image
Processing and Pattern Recognition (SIP), Springer, Dec, 2009.
[5] Bassim Abdulbaki Jumaa* & Arwa Aladdin ImageWatermarking Using DWT_DCT, Eng.& Tech. Journal, Vol.28, No.23, 2010.
[6] MeiJiansheng, Li Sukang and Tan Xiaomei ”A Digital Watermarking Algorithm Based OnDCT and DWT”International Symposium on Web Information Systems and Applications ,China, May 22-24, pp. 104-107, 2009.
[7] Vetterli, M. and J. Kova_evi, Wavelets and Subband Coding. Prentice Hall, USA, 1995.
[8] Wolfgang, R., C. Podilchuk and E. Delp, "Perceptual Watermarks for Digital Images and
Video," Proc. of the IEEE, vol. 87, no. 7,pp: 1108-1126, 1999
[9] Rao, K. and P. Yip. Discrete Cosine Transform: algorithms, advantages, applications. Academic
Press, USA, 1990.
[10] Tsai Hung-Hsu, Jhuang Yu-Jie, Lai Yen-Shou. An SVD based image watermarking in wavelet domain using SVR and PSO. Applied Soft Computing, 12(8): 2442-2453, 2012.
[11] M. Naor, and A. Shamir, “Visual Cryptography”, Advances in Cryptology – Eurocrypt’94
Proceeding, LNCS Vol. 950, Springer-Verlag, pp. 1-12, 1995.
[12] Zhi-Ming, Z.; Rong-Yan, L.; Lei, W.: Adaptive Watermark Scheme with RBF Neural Networks. In Proc. International Conf Neural Networks and Signal Processing, vol. 2, pp. 1517-1520, 2003.
[13] Quan, L.; Jiang, X.: Design and Realization of a Meaningful Digital Watermarking Algorithm Based on RBF Neural Network. Proceedings of the Sixth World Congress on Intelligent Control and Automation, WCICA. vol. 1, pp. 2878-2881, 2006.
[14]Musaab R. Abdulrazzaq ,Visual Cryptography Vs Bit Level Secret Sharing For Image Encryption, Eng.& Tech. Journal, Vol.28, No.07, 2010.

[15] William stalling, " Cryptography and Network Security Principles and Practice", 5th Edition, 2012.
[16] Mathon, B., Patrick, B, Cayre, F, " Practical Performance Analysis of Secure Modulations for WOA Spread-Spectrum Based Image Watermarking", Multimedia and Security workshop, Dallas, Texas, USA, 2007.
[17] Miladi, B., Sayadi, M., Fnaiech F., " Textures Synthesis Methods", International Conference on Electrical Systems and Automatic control, Tunisia, 2010.
[18] Qianhui, Yi. and K. Wang,An Improved Watermarking Method Based on Neural Network for Color Image. International Conference on Mechatronics and Automation. Changchun, pp: 3113-311, 2009.
[19] Jana D., David M., Andreas L., " Theoretical Framework for a Practical Evaluation and Comparison of Audio Watermarking Schemes in the Triangle of Robustness, Transparency and Capacity" , Springer ,Volume 4300, pp. 1-4,2006.