International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.349-360
http://dx.doi.org/10.14257/ijsia.2014.8.5.31

A robust Optimal Zero-Watermarking Technique for Secret Watermark Sharing

Jumana Waleed[1], Huang Dong Jun[1] and Saad Hameed[2]

[1]*School of information Science and Engineering, Central South University, Changsha, 410083, China*
jumana_waleed@yahoo.com, djhuang@csu.edu.cn
[2]*College of Information Science and Engineering, Hunan University, Changsha, China*
saad@hnu.edu.cn

Abstract

In this paper, a robust optimal zero-watermarking technique based on genetic algorithm for secret watermark sharing is proposed for the purpose of copyright protection. It is implemented in discrete cosine transform (DCT) for gray scale images in which the visual secret sharing is used to generate unexpanded master and secret shares for the watermark. The GA based zero watermarking is used to select the perfect positions to extract the robust features. The experimental results indicate that the proposed scheme is highly robust even after different types of attacks being applied, where NC values of each selected attack are considered in the fitness function of the genetic optimization algorithm.

Keywords: *Optimal Zero-Watermarking, Genetic Algorithm, Visual Secret Sharing, Discrete Cosine Transform.*

1. Introduction

Digital watermarking is a powerful technique for copyright protection and digital data ownership. Until the present day, many numbers of watermarking techniques depends of manipulating both spatial and frequency domains which will render the digital data with high distortion, as distortion, as commonly known there is a tradeoff between robustness and imperceptibility. On the other hand, an emerging lossless technique which known as zero watermarking is proposed, this technique relies on extracting specific set of features that could identify the digital data uniquely and could contribute with the construction of the watermark, then registering these features into a third party database for safe keeping. This database is an intellectual properties rights for digital media. Many researchers have gone through this field for the purpose of copyright protection. In [1] two zero watermarks from its host image were generated together, to improve the robustness, where the first is obtained from low-frequency coefficients in the (DWT), and the other is obtained from DWT coefficients of the log-polar mapping to the host image. While [2] constructs the watermark from the low frequency area in BOR multi-wavelet domain to produce a simple while robust zero-watermarking. The scheme creates a relationship inside the sub image with low average, where the center value considered with the mean of the four neighboring coefficients resulting in a strong technique against many attacks. A zero-bit watermarking algorithm

ISSN: 1738-9976 IJSIA

based on the optimized support vector regression (SVR) which presented in [3] to improve the performance of resisting geometric attacks in digital watermarking. [4] Presents a copyright protection zero-watermark scheme based on discrete cosine transformation, in which a normalization process commenced on both embedding and extraction phases to increase the robustness to geometric distortions. Another scheme where presented which fully exploits the characteristics DWT as described in [5]. This novel image zero-watermarking scheme based on DWT-SVD, that achieves multi-resolution decomposition and the SVD, which in turn efficiently represents intrinsic algebraic properties of an image. In [6] the method takes the highly stable invariant centroid as the reference point for geometric correction based on the combination of the image invariant centroid and SIFT feature point. Later it finds out the farthest SIFT point from the invariant centroid, and then finally estimates out geometric parameters by changes of these points' locations.

The visual secret sharing scheme is a visual cryptographic protocol which has the ability for sharing images in secure way, and restores it without the use of computations [7]. In its basic model, a binary image is encrypted into n separated images, which reveals the original image when overlaid. If the user does not have the complete n images then no information about the encrypted image can be retrieved. Some researchers used the concept of visual secret sharing of two participants with the zero-watermarking technique to protect the copyrights of digital images. [8] Embeds a binary watermark in a gray-level image using the concept of expanded visual secret sharing. While [9] and [10] proposed a scheme aims at reducing the size of shares (unexpanded shares).

The key of zero-watermarking is to build a watermark to adapt the feature data of the carrier with the ability to hold a data capable of fully representing the carrier data in addition to its uniqueness, this is done by considering The transform domain of the carrier data as the main structural position selected by most existed zero-watermarking technique. It is always preferable improve the robustness of zero watermarking by exploiting artificial intelligence techniques and Genetic Algorithms (GAs) as optimization algorithms. The zero watermarking problems can be viewed as an optimization problem. Therefore, in this paper the attempt is to provide a solution using genetic algorithms (GAs).

In this paper, an optimal zero-watermarking technique was proposed using the visual secret sharing to generate unexpanded secret and master shares for the watermark, this technique extract the feature bits by utilizing the most important parts in the DCT of the gray image based on genetic algorithm (GA) to get perfect results and obtained a highly robust watermark. The rest of this paper is organized as follows: the visual secret sharing is given in the subsequent section. Section 3 is the explanation of the proposed optimal zero-watermarking technique based on genetic algorithm. In Section 4, we show the presentation of experiments to demonstrate the robustness of the proposed technique. In Section 5 we have the conclusions of our technique and the findings obtained.

2. Visual secret sharing scheme

With the emerging of visual cryptography scheme (VCS) or visual secret sharing (VSS) proposed by Naor and Shamir [7], a new non-intrusive watermarking techniques guideline have been introduced as in [11] and [12]. In the original visual secret sharing, any black and white printed material such as text or images etc. are considered as images and can be split into n different share images. By stacking out a set of qualified images k where ($k \epsilon n$) the image can be obtained from this k set of images, knowing

that even k-1 would not reveal the image at all, not even close to the watermark image. No computation is involved in obtaining the watermark image from the k shares.

Recently, 2-out-of-2 visual secret sharing schemes are widely adapted in protecting the copyrights of high precision digital images. In the traditional OR-based (2,2) visual secret sharing scheme, a secret image is encrypted in two random looking images (transparencies), each pixel in the secret image is expanded into four sub-pixels (2×2 binary code-words) in each transparency. The content of the secret image becomes visible by stacking these two transparencies over each other. Knowing that, there is another model of OR-based (2,2) visual secret sharing in which each pixel in the secret image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image as shown in Figure 1. These models increase the size of each share and result in loss of contrast in the recovered image.

In this paper, XOR-based (2,2) visual secret sharing is used without expansion in the secret image pixels. The secret watermark image is split into two unexpanded master and secret shares.

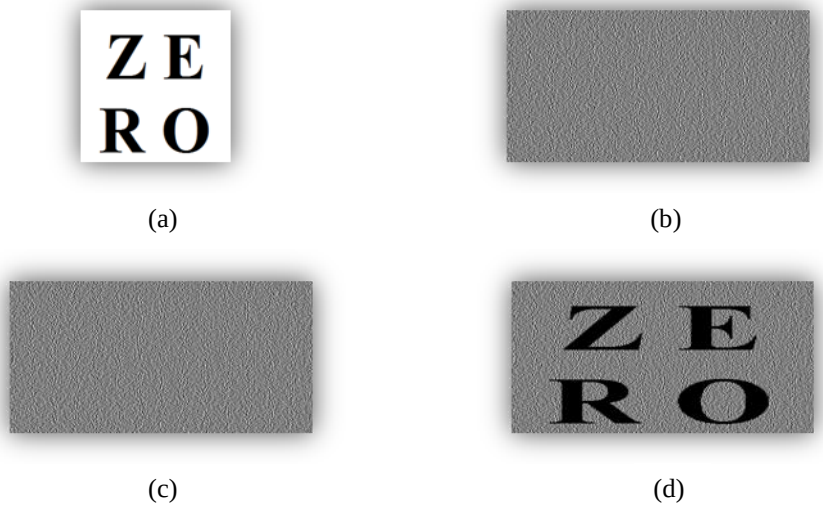


Figure 1. An Example of (2,2) Visual Secret Sharing Scheme, for (a) Secret Image, (b) Share1, (c) Share2, (d) Overlapped Expanded Image

3. The Proposed Optimal Zero-Watermarking Technique based on GA

In this section, we propose a copyright protection technique for improving zero-watermarking using visual secret sharing applied to a binary watermark and optimized using genetic algorithm. The proposed optimal zero watermarking technique can be characterized as follows:

3.1. Embedding Process

To generate the secret share for the watermark, the DCT is performed to the gray image blocks. The DCT block is consisted of several frequency bands; The single direct current (DC) coefficient, the low frequency coefficients of the block (BL), the height frequency band (BH) and the middle frequency coefficients of the block (BM). The most important part (DC)

coefficients are chosen for generating the feature matrix bits. The embedding process can be described as follows; Figure 2 is the representation of the embedding process.

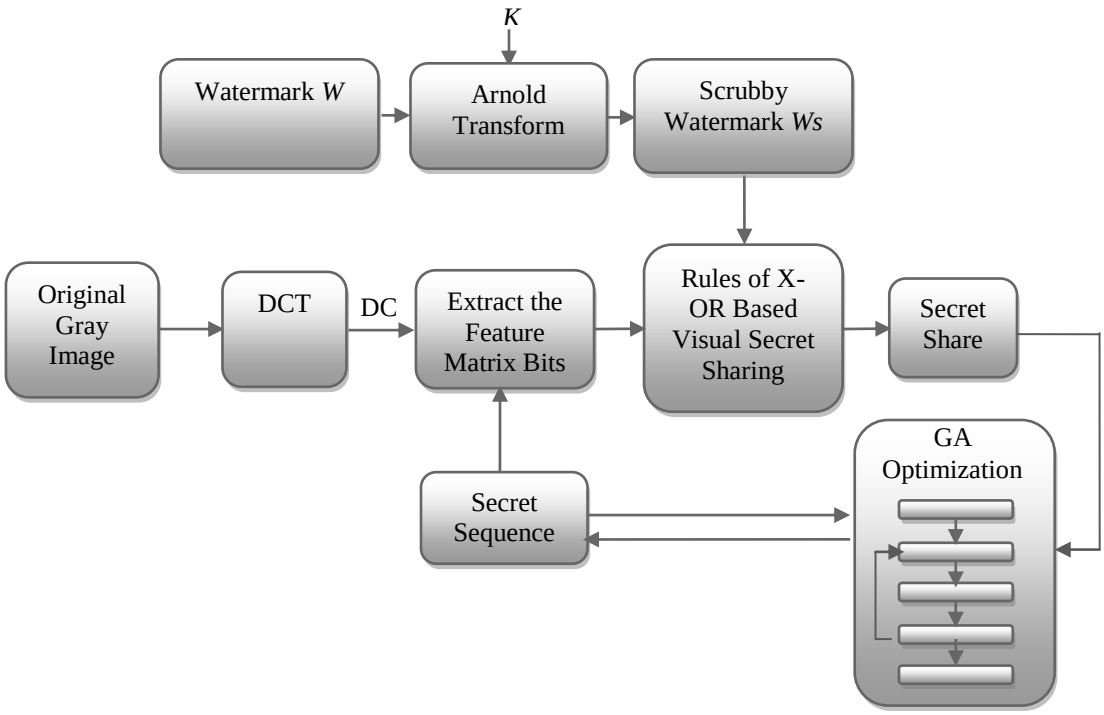


Figure 2. Embedding Process

The proposed embedding process takes place in the following steps, describing in details what the implications in each step:

1. Read the watermark image of size $n \times n$. To reduce the relationship of pixel space in the watermark image, the watermark W is spread out evenly using Arnold transform with scrambling time K. Empirical value of K is 20 which applied on the watermark W to obtain spread out watermark W_s as in Equation (1).

$$W_s(i,j) = W\left(\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} i \\ j \end{bmatrix} mod\ n\right) \quad (1)$$

$$where: W(i,j), W_s(i,j) \in \{0,1\}, 1 \le i,j \le n$$

2. Divide the original gray scale image with size $m \times m$ into 8×8 non overlapping blocks. To extract the feature matrix bits; these blocks are converted into the frequency domain using the two dimensional DCT, $B = \{B_1, B_2, \ldots, B_t\}$, where t is the total number of blocks. Since the number of the watermark bits ($n \times n$) are very less as compare to total number of blocks (t), $2(n \times n)$ blocks need to be selected from B. A random matrix R having dimension $2(n \times n)$ is generated, $R = \{v_1, v_2, \ldots, v_{2(n \times n)}\}$, where v lies in between 1 and t. The blocks whose block number matches with v are separated from B.

3. For the randomly selected blocks, the (DC) coefficients are selected to obtain the two (DC) matrices D_1 and D_2, each of size $(n \times n)$. Then, each element in D_1 will be compared with the corresponding element in D_2. The feature matrix F is constructed by using Equation (2).

$$F(i,j) = \begin{cases} 1, & D_1(i,j) \geq D_2(i,j), \\ 0, & Otherwise \end{cases} \quad (2)$$

$where: F(i,j) \in \{0,1\}, 1 \leq i,j \leq n$

4. Generate the secret share by using the rules given in Table 1. The secret share and the secret sequence are then registered into a third party database for safe keeping. This database is an intellectual properties rights for digital media.

Table 1. Construction Rules of X-OR Based Visual Secret Sharing

Watermark Pixel	White	Black
Bit in Feature Matrix F	0 1	0 1
Master Share Pixel	■ □	■ □
Secret Share Pixel	■ □	□ ■
Master Share X-OR Secret Share	□ □	■ ■

3.2. Extraction process

The inputs to the extraction process are a controversial image and the secret share image. The output is a watermark image *W'*. To extract the features of controversial gray image, the owner uses the same process which is used in the embedding process. Then, the master share is constructed by using the rules given in Table 1. The X-OR logic function is then applied between the secret and master shares to reveal the Scrubby watermark *W's*. Finally, Arnold transform is applied *K* times to *W's* to obtain *W'* which is used to verify the copyright. Note that, the size of the shares and the extracted watermark is exactly same since there is no pixel expansion. Figure 3 represents the extraction process.

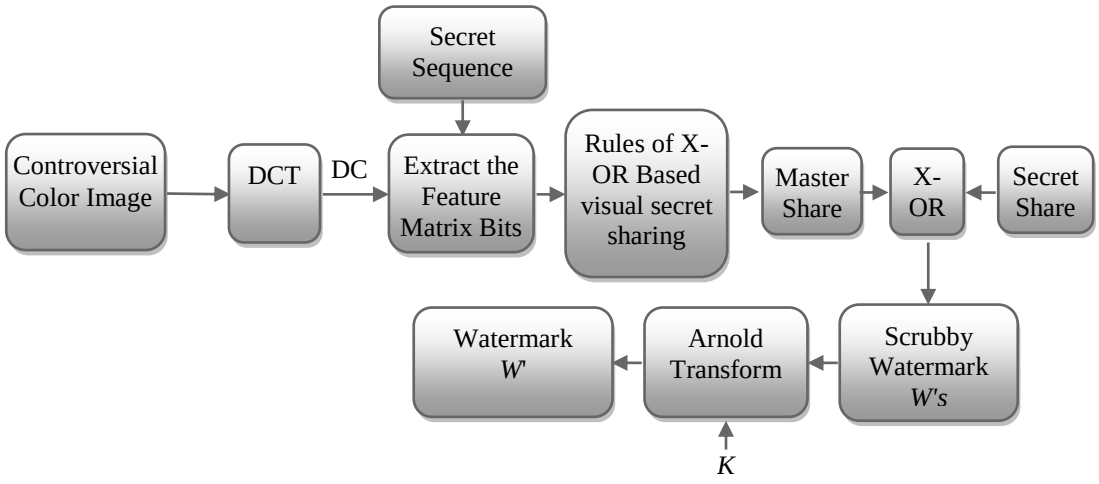


Figure 3. Extraction process

In order to measure the robustness of the zero-watermarking system, the normalized correlation coefficient (NC) of the extracted watermark Wi' is applied in conjunction to the original one Wi; the maximum value of this measure is 1 which determines the best robustness of the watermarking process.

$$NC = \frac{\sum_{i=1}^{N} wi\, wi'}{\sqrt{\sum_{i=1}^{N} wi^2}\sqrt{\sum_{i=1}^{N} wi'^2}} \quad (3)$$

Where: *N* is the size of the original and extracted watermark bits. After obtaining the post attack NC values, we use them to evaluate the fitness of the initial population for the genetic algorithm.

3.3. Genetic algorithm (GA) for optimal positions selection

GA is a nature inspired optimization technique based on evolution and natural selection of individuals. To solve the problem of selecting the best positions to extract a robust features matrix bits, the GA is used considering the following components:

1. Initial population: The chromosomes are randomly generated in the initial population. The length of chromosomes is equal to the double of the size of the watermark i.e. *2(n×n)*. The initial population size contain of 30 chromosomes. The number of generations was considered as 200 times. The best gene is considered as the locations of the best features extraction.
2. Appling attacks: three types of attacks must be applied, JPEG compression with quality factor equal to 10, 15% cropping and adding 5% salt and pepper noise.
3. Fitness function (*FF*): the *FF* can be defined as the function of robustness. For *z* kinds of attack to the zero watermarked image, the *FF* is quantified as follows:

$$FF = \sum_{i=1}^{z} NC_i \quad (4)$$

   The objective is to maximize the fitness function to achieve the optimal robustness for digital image zero-watermarking technique.
4. Perform the crossover and mutation on the selected population to generate the new population. The probability of crossover is set to 0.95, and mutation rate is 0.5.
5. The GA cycle is repeated until the maximum number of generation is reached. The population with the highest fitness value in the final generation is the optimal selected positions.

4. Experimental results

To test the performance of the proposed optimal zero-watermarking technique, the results of the experiments are obtained using MATLAB. The proposed Technique is tested on gray scale images of size 512×512 (Lena, Peppers, Barbara and Boat). The gray image Lena is shown in Figure 4 (a). The binary watermark image of size 32×32 is shown in Figure 4 (b). The resultant Master and Secret Shares for the proposed technique are shown in Figure 4 (c), and (d) respectively. The recovered watermark from an unaltered image is shown in Figure 4 (e), note that the size of all these images is same as the original watermark and looks like a random scatter of black and white pixels.

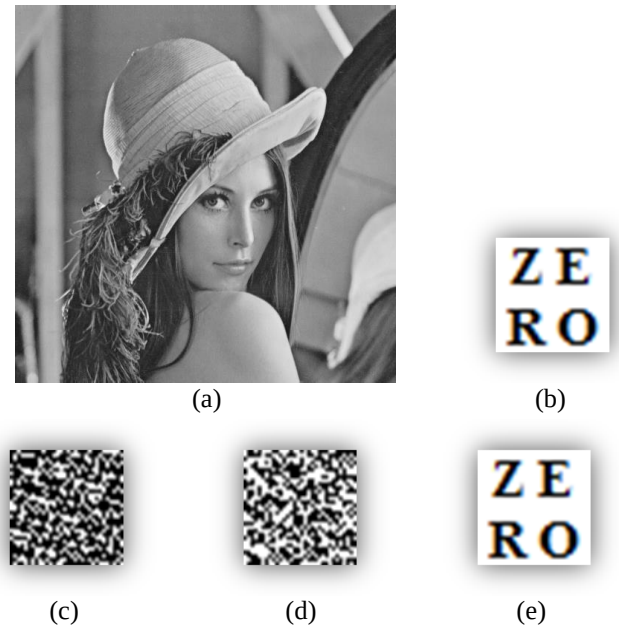


Figure 4. (a) The original gray scale image (Lena), (b) watermark image (32× 32), the resultant images of the zero watermarking technique (c) Master Share, (d) Secret Share and (e) Reconstructed watermark

To check the robustness of the proposed technique, some common image processing attacks were performed on the original images. Noise addition to the image is obtained by adding 1% and 5% salt and pepper noise to the original image. Gaussian noise is obtained with mean=0 and variance=0.0005. Median filtering is performed with window size 3×3. And, Gaussian low pass filtering of the image was done with a window of size 2×2. Gamma Correction 1.5, Intensity Adjustment ([0 0.8], [0 1]), and histogram equalization are applied to the original image. The JPEG compression attack is performed by compressing the image with quality factors 15 and 10. The scaling of an image is done by first reducing the original host image size from 512×512 pixels to 256×256 pixels, and then zoomed to its original size by means of pixel replication. The cropped image is obtained by cropping 15% of the original image.

To evaluate the proposed scheme fidelity, we measure the similarity between the original and attacked images by using Peak Signal to Noise Ratio.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{5}$$

Where, the MSE is the mean squared error (MSE) between the original and the distorted one, is defined as Equation (6).

$$MSE = \frac{1}{m \times m} \sum_{i=1}^{m} \sum_{j=1}^{m} [I(i,j) - I'(i,j)]^2 \tag{6}$$

Where: $m \times m$ is the size of the image, and $I(i, j)$, $I'(i, j)$ are the pixel values of the host and the attacked images. Figure 5 demonstrates the values of PSNR for the gray scale images. Figure 6 shows the NC values of the reconstructed watermark with random positions

selection for the proposed zero-watermarking (without optimization) under different types of attack, while Figure 7 shows the NC values with the proposed optimization technique.

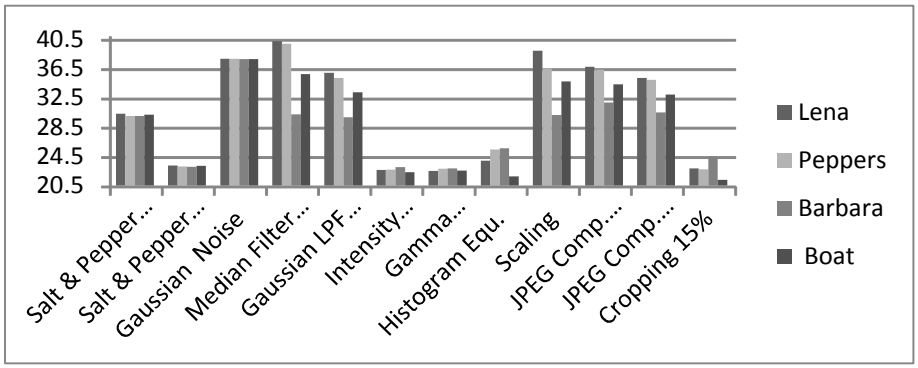


Figure 5. The effect of attacks on PSNR values

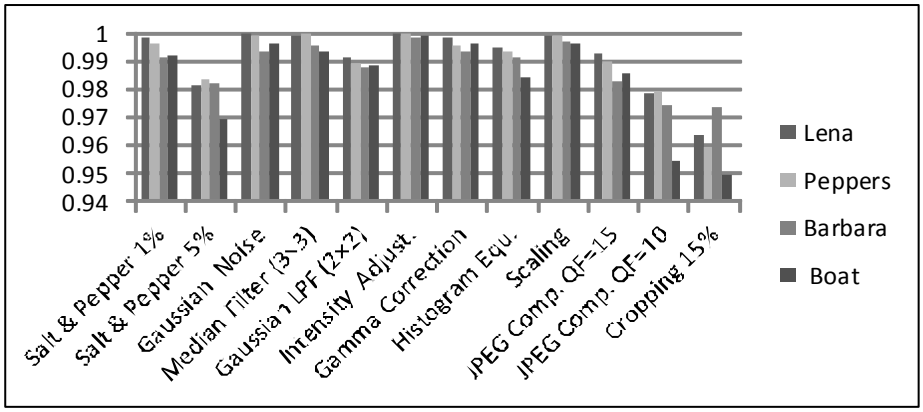


Figure 6. The effect of attacks on NC values without optimization

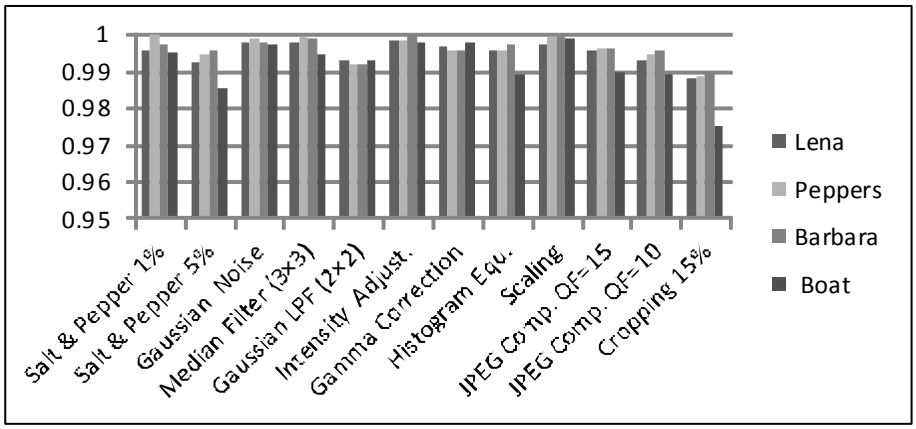


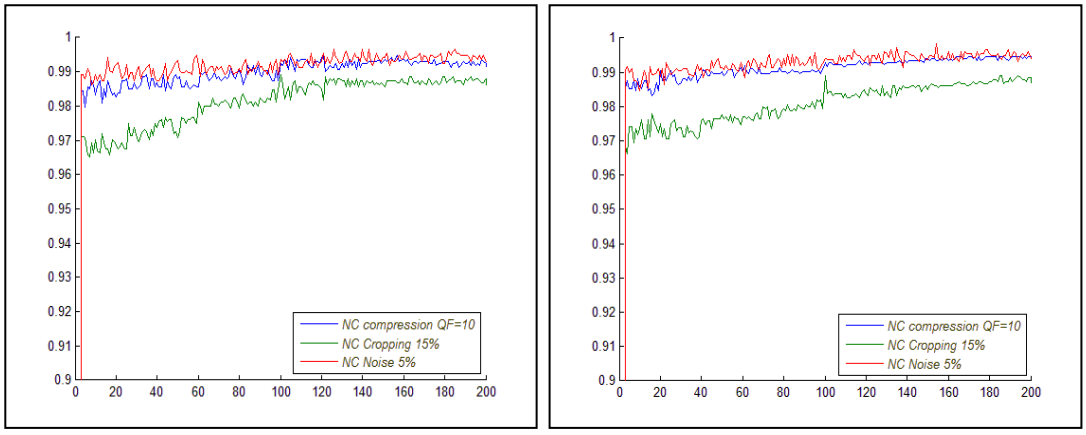
Figure 7. The effect of attacks on NC values with proposed optimization technique

Table 2 lists comparison results of NC values between the optimized and non optimized zero-watermarking techniques. Table 2 shows the values of all NC obtained by each attack through the passing generations of the GA algorithm in contrast to NC values of a zero watermarking technique lacking the GA optimization ability.

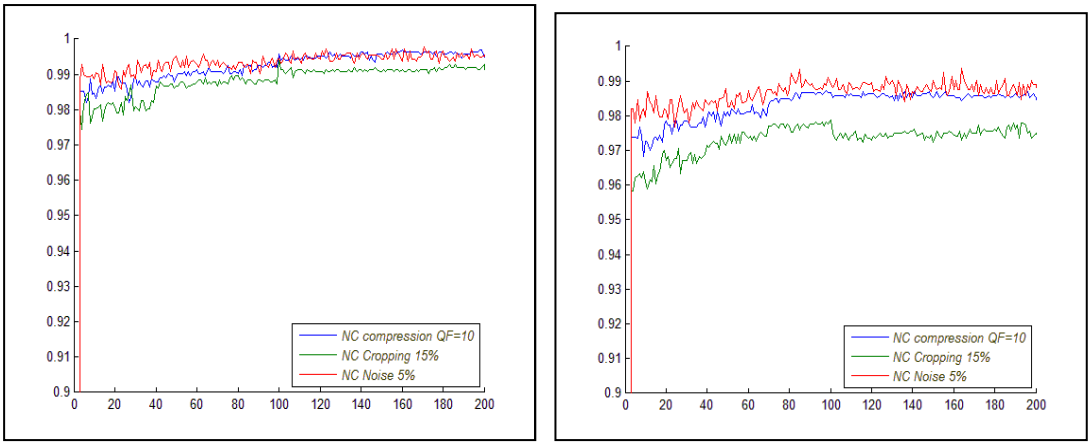
As in Figure 8, the values of NC are shown for all 4 test images suffering from three different attacks and showing how these values are improved across the progression of generations in the GA algorithm, on the other hand, Figure 9 shows the impact of the mentioned NC values improvement on the calculated fitness function, resulting a fitness values showing a clear climbing curve towards optimum results. The exact digital values of maximum fitness for the test images are 2.9733, 2.9775, 2.9806 and 2.9489 for Lena, Peppers, Barbara and Boat respectively.

Table 2. Performance comparison between the proposed non-optimized and optimized zero-watermarking techniques

Attack types	Without optimization				With optimization based on GA				
	Lena	Peppers	Barbara	Boat	No. of gen.	Lena	Peppers	Barbara	Boat
Salt & Pepper Noise 5%	0.9815	0.9833	0.9821	0.9694	10	0.9833	0.9857	0.9845	0.9725
					50	0.9923	0.9947	0.9953	0.9851
					100	0.9923	0.9927	0.9957	0.9867
					150	0.9929	0.9941	0.9959	0.9851
					200	0.9923	0.9947	0.9953	0.9851
JPEG Comp. QF=10	0.9785	0.9791	0.9742	0.9541	10	0.9893	0.9845	0.9887	0.9797
					50	0.9935	0.9915	0.9951	0.9825
					100	0.9937	0.9941	0.9947	0.9893
					150	0.9943	0.9937	0.9943	0.9901
					200	0.9931	0.9943	0.9955	0.9889
Cropping 15%	0.9633	0.9591	0.9737	0.9491	10	0.9701	0.9737	0.9803	0.9608
					50	0.9879	0.9885	0.9927	0.9749
					100	0.9843	0.9889	0.9903	0.9789
					150	0.9861	0.9849	0.9869	0.9724
					200	0.9879	0.9885	0.9898	0.9749

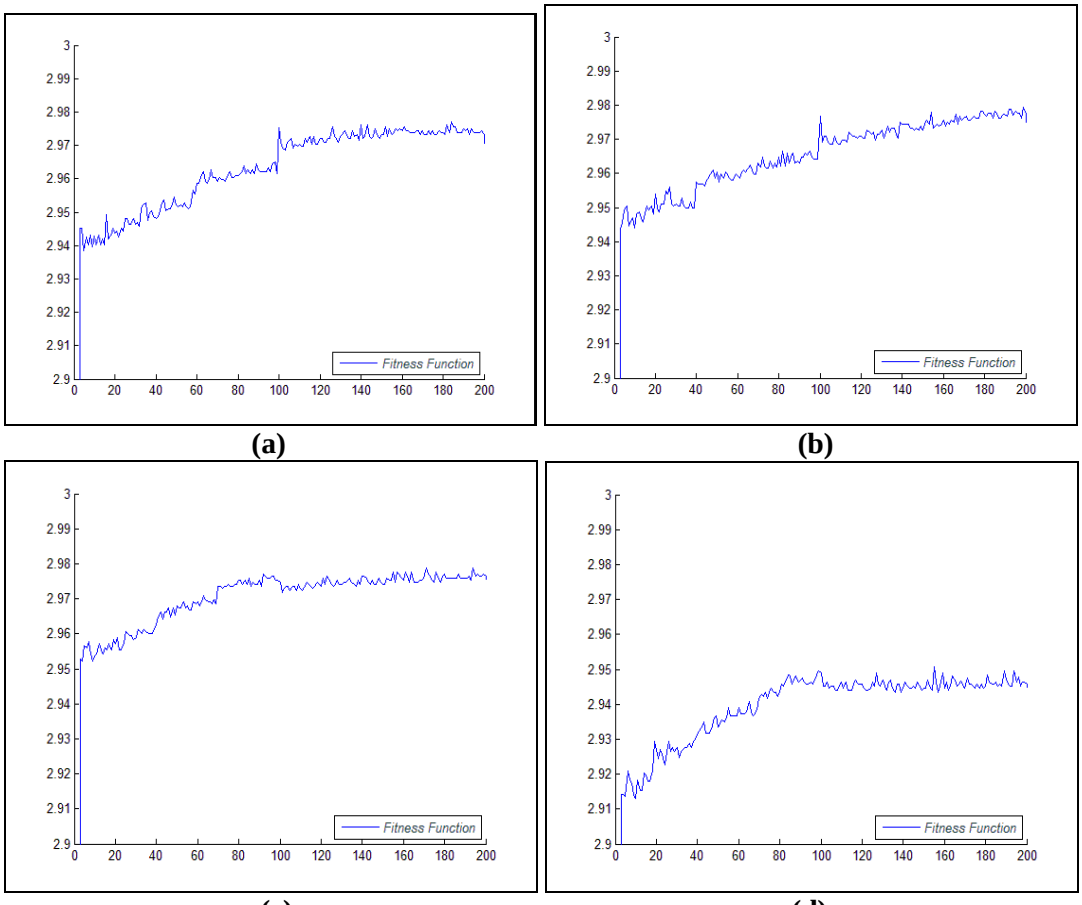


(a) **(b)**



(c) **(d)**

Figure 8. The NC values for JPEG compression with quality factor equal to 10, 15% cropping and adding 5% salt and pepper noise versus GA generations for (a) Lena , (b) Peppers, (c) Barbara and (d) Boat test images.



(a) **(b)**

(c) **(d)**

Figure 9. The Fitness Function values versus GA generations for (a) Lena , (b) Peppers, (c) Barbara and (d) Boat test images

5. Conclusions

In this paper, we have proposed an optimal zero-watermarking technique that extracts the feature bits from the most important parts in the host gray image instead of embedding watermark into that image to protect the copyright information in a robust way. Its high robustness is due to the exploitation of GA for the evaluated selection of the positions to extract the feature bits. The feature bits are used to split the watermark into unexpanded master and secret shares. The proposed technique generates a secret share to the watermark from host image during the embedding procedure, which is constructed from that the DC coefficient in discrete cosine transform domain of the host image. The secret share and the optimal secret sequence are then registered in a third-party database for copyright protection. The master share is constructed from the controversial gray image during the extracting procedure. According to the obtained results of NC values that shows the proposed technique is robust against different kinds of attack, such as: noise addition, Median filtering, Gaussian low pass filtering, intensity adjustment, gamma correction, histogram equalization, scaling, JPEG compression, and cropping.

Acknowledgements

This work was supposed by the project of National Science Fund of China (No. 60873188).

References

[1] L. Jing and F. Liu, "Double Zero-Watermarks Scheme Utilizing Scale Invariant Feature Transform and Log-Polar Mapping", IEEE International Conf. on Multimedia and Expo, Beijing, China, **(2007)** July 2-5, pp. 2118-2121.
[2] X. Tang, J. Wang, C. Zhang, H. Zhu and Y. Fu, "A Fast and Low Complexity Zero-Watermarking Based on Average Subimage in Multiwavelet Domain", In Proc. of IEEE 2nd International Conf. on Future Computer and Communication (ICFCC), Wuhan, China, vol. 2, **(2010)** May 21-24, pp. 178-182.
[3] G. G. Yong and J. G. Ping, "Zero-bit watermarking resisting geometric attacks based on composite-chaos optimized SVR model", The Journal of China Universities of Posts and Telecommunications, vol. 18, no. 2, **(2011)**, pp. 94-101.
[4] M. Shakeri and M. Jamzad, "A Robust Copyright Protection Scheme Based on Discrete Cosine Transform And Image Normalization", In Proc. of IEEE 7th Iranian Machine Vision and Image Processing (MVIP), Tehran, Iran, **(2011)** November 16-17, pp. 1-6.
[5] Y. Zhou and W. Jin, "A Novel Image Zero-watermarking Scheme Based on DWT-SVD", In Proc. of IEEE International Conf. on Multimedia Technology (ICMT), Hangzhou, China, **(2011)** July 26-28, pp. 2873-2876.
[6] L. Peili and T. Yuehui, "Robust Zero-watermarking Algorithm Based on Invariant Centroid", IEEE Fifth International Conference on Computational and Information Sciences (ICCIS), Shiyang, China, **(2013)** June 21-23, pp. 758-761.
[7] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptography Eurocrypt'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 950, **(1995)**, pp. 1-12.
[8] S. Punitha, S. Thompson and N. S. R. Lingam, "Binary Watermarking Technique based on Visual Cryptography", IEEE International Conference on Communication Control and Computing Technologies (ICCCCT), Ramanathapuram, India, **(2010)** October 7-9, pp. 232-235.
[9] F. Liu and C.-K. Wu, "Robust visual cryptography-based watermarking scheme for multiple images and multiple owners", Information Security, IET, vol.5, no 2, **(2011)**, pp. 121-128.
[10] B. Surekha and G. Swamy, "A Semi-blind Image Watermarking based on Discrete Wavelet Transform and Secret Sharing", IEEE International conf. on Communication, Information & Computing Technology (ICCICT), Mumbai, India, **(2012)** October 19-20, pp. 1-5.
[11] B. Surekha and D. G. Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications, vol. 5, no. 1, **(2011)** January, pp. 1-12.
[12] P. V. Jithi and A. T. Nair, "Progressive visual cryptography with watermarking for meaningful shares", International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing, Kottayam, India, **(2013)** March 22-23, pp. 394-401.

Authors

Jumana Waleed is a Ph.D. student in the School of information science and Engineering at Central South University, Changsha, China. Her research activity focuses on image processing, and information security working on digital watermarking. She received the B.S. degree in computers sciences from the Al-Yarmouk University College, Iraq, in 2004, and the M.S. degree in Computer Science/Data Security from the University of Technology, Baghdad, Iraq, in 2009.

Dr. Huang Dong Jun is a professor at Central South University. He received his PHD degree in computer science and technology from the Central South University, China, in 2004. He worked as a visiting academic to University of Glasgow, UK, from 2007 to 2008. Currently, he is the director of the Department of Computer Engineering, Central South University and the member of the IOT Education Expert Group of the Ministry of Education, China. His research interests include computer networks, multimedia technology, image and video processing, video conferencing system and video surveillance techniques.

Saad Hameed was born in Baghdad – Iraq in 7 June 1979, he received his B.Sc. Degree in computer science at AL-Mansour University College 2001, and Masters Degree in computer Sciences, Iraqi committee for computer and informatics in 2004, he continued working in academic teaching in AL-Mansour University College for 11 years, through that time all of his research was self-funded and concentrated in automation and control, he has been promoted from assistant Lecturer to Lecturer in 2011, he is now a Ph.D. degree student at Hunan University in P.R. China.