Current Trends in Technology and Science
ISSN : 2279-0535. Volume : II, Issue : VI

The Optimized Image Watermarking Using Genetic Algorithm

Seyed Sahand Mohammadi Ziabari
Master of Science student, Organization :Malek Ashtar university, Email ID : sahandziabari@gmail.com

Reza Ebrahimi Atani
Assistant Professor, Organization : Guilan university, Email: reza.ebrahimi.atani@gmail.com

Kiyan Keyghobad
Assistant Professor, Organization : Malek Ashtar university, Email ID : keyghobad.kiyan@gmail.com

Abdolmajid Riazi
Assistant Professor, Organization : Malek Ashtar university, Email ID : m_riazi@mut.ac.ir

Abstract **- The selection of both the transform domain and the particular algorithm that is used for the embedding of the watermark, depend heavily on the application. One of the most widely used transform domain for watermarking of still digital images is Discrete Cosine Transform domain. The optimized image watermarking using genetic algorithm is presented here. In the previous watermarking algorithms which were used correlation value there is a problem of losses watermarks unintentionally without any malicious attack. We improve the security of the watermarking with some preprocessing operations and we try to remove the implicit error which has been mentioned. And we also decrease the time consuming of genetic algorithm by simplifying the previous algorithms.**

Keywords **- Image, Watermarking, Genetic algorithm, Arnold Transform.**

1. INTRODUCTION

The rapid progress in spreading the digital mediums in World Wide Web addresses during these years, the need of protection of copyright in digital data is increased. There are three main categories for protecting the digital data, namely Encryption, Steganography and Watermarking. The differences between them are represented in [1].

Steganography is the art of trying to keep concealed the very existence of the communication channel. In general, steganography falls under the information hiding root. There are further subdivisions of steganography (Linguistic, Technical) that we are not going to cover.

Digital watermarking is a highly evolving field, which involves the embedding of a certain kind of information under a digital object such as image, video, audio for the purpose of copyright protection. In the watermarking processing, there are three conflicting criteria which have trade off among them: (1) Capacity (The number of bits that can be hidden and then recovered), (2) Robustness to intentional or unintentional attacks such as removal, (3) Imperceptibility [2].

Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the watermark remains in the content in its original form and does not prevent a user from listening to, viewing, examining, or manipulating the content.[3],[4].

The applications of watermarking are well known and can be broadly classified as copyright control such as owner identification, proof of ownership, transaction tracking and copy control, broadcast monitoring and device control.[5]

Watermarking is a method of providing protection of intellectual property in digital media and is divided into two main categories which are spatial domain and transform domain. Watermarking in the spatial domain has lesser disadvantages rather than transform domain. For instance, in the spatial domain in most of the time the robustness against the attacks is much less than transform domain. The transform domain itself is divided into many categories which is depended on the transform function, but the most two famous categories are the Discrete Wavelet transform, Discrete Cosine Transform. Each of them has their own advantages and disadvantages. They are analyzed in [6] separately. The latter one is used in this paper.

The space domain techniques are generally considered more susceptible to the various kinds of attacks. However these techniques were implemented first, and there is still research going in the area, though not as in the transform domains. Space domain techniques can be chosen for low cost schemes requiring low complexity and small computational overhead.

There have been several attempts by the research community to investigate the watermarking performance in different transform domains. The basic benefit from a transform domain is that by choosing a framework that matches the current compression standards, the watermarking algorithm can be designed to avoid embedding in the coefficients that are normally discarded or severely quantized during compression. In [7] the authors propose a spread spectrum technique, which uses the DCT domain as the embedding domain. Its innovation was how communication concepts such as spread spectrum can be applied to watermarking, and that

the watermark can be embedded in the perceptually significant portion of the image.

This paper organized as follows, first we introduce the preprocessing algorithm which is used here, namely Arnold transform, for having much more secure watermarking. Second, we demonstrate the main watermarking algorithm which was presented before. Then we mention the algorithm which has been used to prevent the unintentional removal of watermark after watermarking.

2. PRE-PROCESSING ALGORITHM

Arnold transformation is a technique to increase the security of watermarking. It can disorder the image matrix and make the image illegible [8]-[10]. The Arnold transform is as (**1**).

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N \quad (1)$$

Where X and Y are the original pixel value and X' and Y' are the transformed pixel value by the Arnold transform and N is the number of pixels for one dimension of N*N Image. Figure 1 shows the original and the transformed flower image for 10 iterations.

Figure 1.Original and transformed images (Iterations=10)

If the watermark is scrambled in the stage of pre-processing, it should be recovered fleetly in the stage of back processing. The idea of periodicity algorithm is that if the watermark reaches one scrambled state by taking m steps of Arnold transformation, it needs to take T-m steps to recover. T is the periodicity of the corresponding Arnold transformation [10]. For example, if the size of watermark is 32*32 (T=24), it takes five steps to reach one scrambles state through Arnold transformation, then it needs to take ninety-one steps to recover.

3. THE WATERMARKING ALGORITHM

The embedding takes place in the DCT domain, which is also used by the JPEG standard, and allows for the exploitation of the particular characteristics of domains and the achievement of watermark transparency. In this paper, the watermarking algorithm which has been used in [11]-[13] with a little change according to [14], is used. The main algorithm is as follows.

Firstly, both the watermark and the image are DCT transformed. For the cover image of size $M_1 \times M_2$ the non-overlapping DCT transform with size of 8×8 is used. Therefore there are blocks which is shown with U and V whereby $C=\{C_{uv} \ |u=1,2,\ldots,U, \ v=1,2,\ldots,V\}$, $U=\text{floor}[M_1/8]$ and $V=\text{floor}[M_2/8]$. The correlation value is computed as (2).

$$R(i,j) = \frac{1}{U \times V} \sum_{u=1}^{U} \sum_{v=1}^{V} C_{UV}(i,j) / C_{UV}(0,0)$$

Where $C_{uv}(0,0)$ is the DC coefficient of the i^{th} row and j^{th} blocks and $C_{uv}(i,j)$ is the AC coefficients of blocks. The embedding structure is as **Error! Reference source not found.**,**Error! Reference source not found.**.

$$C'_{UV} = \begin{cases} C_{UV}(0,0)R(i,j) + \alpha, \ if \ P = W = 0 \quad or \quad P = W = 1 \\ C_{UV}(0,0)R(i,j) - \alpha, \ if \ (P = 0 \& W = 1) \ or (P = 1 \& W = 0) \\ C_{UV}(i,j), \quad if \quad else \end{cases} \quad \ldots(3)$$

$$P_{UV}(i,j) = \begin{cases} 1, & if\,(C_{UV}(i,j) \geq C_{UV}(0,0)) \\ 0, & \text{otherwise} \end{cases} \quad \ldots(4)$$

Where α is the embedding strength in the range of {0, 1} and W is the watermark bit and P is calculated as **Error! Reference source not found.**. Since maximal value of α is equal to 1. It is claimed in [14] that this method loses the watermark even without attack. Thus, just with changing in the watermarking algorithm. First, losing watermarks without any attacks. Second the processing time is greatly decreased because of simplifying the algorithm. It is claimed that the consumption time will be reduced to 2/3 of the whole time for watermarking.

For solving these problems, means losing watermarks without any malicious attacks and high time consumption, the watermarking algorithm is changed into the [14] as **Error! Reference source not found.**.

$$C'_{UV}(i,j) = \begin{cases} C_{UV}(i,j), & if \ P = W = 0 \ or \ P = W = 1 \\ (-\lambda)C_{UV}(i,j), if & (P = 0 \& W = 1) \ or \ (P = 1 \& W = 1) \\ (+\lambda)C_{UV}(i,j), & if \quad else \end{cases} \quad \ldots(5)$$

Where $P_{uv}(i,j)$ is defined as **Error! Reference source not found.**.

$$P_{UV}(i,j) = \begin{cases} 1, & if \quad C_{UV}(0,0) \geq 0 \\ 0, & Otherwise \end{cases} \quad \ldots(6)$$

As it is shown in [14] they did not use the correlation in the watermarking algorithm, thus the speed of algorithm will be increased. The extraction process is really simple, first the periodicity anti-Arnold transform is performed into the watermarked image and then as **Error! Reference source not found.** the watermark will be extracted.

$$W_{UV}(i,j) = \begin{cases} 1, & if \quad C'_{UV} \geq 0 \\ 0, & Otherwise \end{cases} \quad (2)$$

$$\ldots(7)$$

4. GENETIC ALGORITHM

During these years using optimization algorithms for watermarking because of their ability to find the better solution is incredibly increased. One of the most important of these algorithms is Genetic algorithm [15].
Genetic algorithm is used in many problems of watermarking optimization and different watermarking domains [16]-[20]. The structure of genetic algorithm in [13] is used here.
The cover image is divided into the 8*8 blocks and DCT applied into these blocks to get the coefficients values. For each block the number of block and the number of each coefficient in that block and also the embedding strength are digitized into 32 binary bits. Table 1 is shown this bit dedication for block $C_{uv}(i,j)$ for building the chromosomes of Genetic algorithm. (u,v) are the number of the block and (i,j) are the number of the DCT coefficients.

Table 1.Example of chromosomes.

U(for instance= 31)	V(for instance= 20)	I(for instance =5)	J(for instance= 12)	Embedding strength α(=0.3)
Convert to 8 bits	Convert to 8 bits	Convert to 4 bits	Convert to 4 bits	Convert to 8bit
00011111	00010100	0101	0111	10011001

So the chromosome representation in Genetic algorithm is 32bit representation.

5. EXPERIMENTAL RESULTS

Matlab R2011b [21,22] is used for Implementing the embedding algorithm. Here we used the Cameraman image of size 256*256 for cover image and the Flower image of size 32*32 stands for watermark image.
Genetic algorithm parameters are as follows; Cross-over rate =0.7, mutation rate=0.001, Initial population=20, Iteration =3, Cross-over is two point crossover and the fitness function is as (1).

$$F = PSNR + \lambda.(1-BER) \quad (1)$$

As it can see the fitness function includes two criteria in perceptual and robustness evaluation. PSNR for measuring how the embedding is imperceptible and BER to measure how the embedding is robust against the difference attacks.
The algorithm is performed into the cameraman picture with size of 256*256 as a cover image and the flower image with size of 32*32 as a watermark image.


Figure 2.Cover and watermark images.


Figure 3.Watermarked and extracted images.


(a)


(b)


(c)


(d)

Figure 4. Experimental results.
a) After Median filter attack.

b) after Histogram equalization attack.
c) After Sharpening attack.
d) After Cropping attack.

Notice that before embedding the Arnold transform is used to scramble the watermark image. Table 2 and 3 show the watermarking results after two attacks which are performed into the watermarked image separately.

Table 2.Watermarking results

	Without attack
PSNR	49.7
BER	0.22

Table 3.Comparing presented algorithm with Wang [12]

	Algorithm Presented		[12] Wang	
	PSNR	1-BER	PSNR	1-BER
Salt & Pepper	29.89	0.66	26.57	0.68
Median filter	27.34	0.54	21.13	0.54
Sharpening	26.42	0.43	20.53	0.43
Motioning	27.65	0.56	25.72	0.40
Blurring	25.72	0.52	25.81	0.46
Histogram Equalization	28.32	0.41	27.11	0.22
Scaling (30%)	35.14	0.32	34.11	0.27
Cropping	17.29	0.44	16.31	0.39

6. CONCLUSION

In this paper we showed that by not using the correlation in the watermarking algorithm, the speed of the embedding will be increased and also the unintentional removal of watermarks after embedding is diminished. For having more security in the watermarking we used preprocessing operation, Arnold transform, to scramble the watermark. The fitness function includes two criteria in perceptual and robustness evaluation. PSNR for measuring how the embedding is imperceptible and BER to measure how the embedding is robust against the different attacks.

REFERENCE

[1] J. Cox, L. Miller, A. Bloom, J. Fridrich, T. Kalker, “Digital watermarking and Steganography”,Morgan Kaufmann publisher, 2th edition, 2008.

[2] J.R. Smith, B.O. Comiskey, "Modulation and information hiding in images", In proceeding of the first information hiding workshop, Cambridge U.K, Vol.1174, 1996.

[3] C.I. Podilchuk, E.J. Delp, "Digital watermarking: algorithms and application", IEEE signal processing magazine, pp.33-46, 2001.

[4] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE transaction on image processing, Vol.6, pp.1673-1678, 1997.

[5] I.J. Cox, M.L. Miller, "The first 50 years of electronic watermarking", Journal of applied signal processing, vol2, pp.126-132, 2002.

[6] A.K. Singh, N. Sharma, M. Dave, A. Mohan, "A novel technique for digital image watermarking in spatial domain", 2nd IEEE international conference on parallel, Distributed and Grid computing(PDGC), pp.497-501, Solan, 2012.

[7] S. Pereira, J.J.J.O. Rouanaidh, F. Deguillaume, G. Csurka, T. Pun, "Template-based recovery of Fourier-based watermarks using Log-polar and Log-log maps", Proceedings IEEE in multimedia system 99, International conference in multimedia computing and systems, Florence, Italy, 1999.

[8] Z. Jia, Z. Ting, "The research and design of invisible digital watermarking based on DCT and Matlab", International conference on computer science and network technology, pp.825-828, Harbin, 2011.

[9] J. Yang, "Algorithm of image information hiding based on new anti-Arnold transform and blending DCT domain", 12th IEEE international conference on communication technology (ICCT), pp.312-315, Nanjing, 2010.

[10] L. Fang, W. Yukai, "Restoring of the watermarking image in Arnold scrambling", 2nd International conference on signal processing system(ICSPS),vol.1,pp.771-774, Dalian, 2010.

[11] C.S. Shieh, H.C. Huang, F.H. Wang, J.S. Pan, "Genetic watermarking based on transform domain techniques", Pattern recognition 37(3), pp.555-565, 2004.

[12] F.M. Meng, H. Peng, Z. Pei, J. Wang, "A novel blind image watermarking scheme based on support vector machine in DCT domain", International conference on computational intelligence and security, vol.2, pp.16-20, Suzhou, 2008.

[13] J. Wang, H. Peng, P. Shi, "An optimal image watermarking approach based on a multi-objective genetic algorithm ", Information science 181, pp.5501-5514, 2011.

[14] Z. Wei, J. Dai, J. Li, "Genetic watermarking based on DCT domain techniques", Canadian Conference on electrical and computer engineering (CCECE), pp.2365-2368, Ottawa, 2006.

[15] K. Deb, "Multi-objective optimization using evolutionary algorithms", Wiley, New York, 2003.

[16] C. H. Huang, "A watermark optimization technique based on genetic algorithms", In security and watermarking of multimedia contents II, Vol.3971, pp.516-523, 2000.

[17] B. Sikander, M. Ishtiaq, M.A. Jaffar, M. Tariq, A.M. Mirza, "Adaptive digital watermarking of images using Genetic algorithm", digital watermarking of images using Genetic algorithm", International conference on Information science and applications(ICSA),pp.1-8, Seoul,2010.
[18] C.C. Lai, C.H. Yeh, C.H. Ko, C.Y. Chiang, "Image watermarking scheme using Genetic algorithm", Sixth international conference on Genetic and evolutionary computing, pp.476-479, Kitakushu, 2012.
[19] M. Khodaei, K. Faez, "Image hiding using Genetic algorithm and LSB substitution", Image and signal processing lecture in computer science,vol.6134, pp.404-411,2010.
[20] J.S. Pan, H.C. Huang, L.C. Jain, "Intelligent watermarking techniques", Series on innovative intelligence,World scientific, Vol.7, 2004.
[21] http://www.matlabsite.com
[22] U. Qidwai, C.H. Chen "Digital image processing: an algorithm approach with Matlab ", CRC press, Tailor and Francis group,2010.

AUTHOR'S PROFILE

Seyed Sahand Mohammadi Ziabari was born in Rasht, Iran. He studied Electronics Engineering at the University of Lahidjan in Guilan, Iran. He got his B.Sc degree in 2011 and at the same year he was accepted to follow his master study at Malek Ashtar University of Technology in Tehran, Iran. He received the M.sc degree in Cryptology in 2013. His research interests include Cryptology, Image and Speech Processing and watermarking, Fingerprint recognition.

Reza Ebrahimi Atani was born in Arak, Iran. He graduated from Razi high school of Rasht in 1998; he studied Electronics Engineering at the University of Guilan in Rasht, Iran. He got his B.Sc degree in 2002 and at the same year he was accepted to follow his masters study at Iran University of Science & Technology (IUST) in Tehran, Iran. He joined the Electronics Research Center of IUST and received the M.Sc degree in Electronics-VLSI design in 2004 and again at the same year he was accepted to pursue his studies as a full-time PhD student under supervision of Prof. Sattar Mirzakuchaki and Prof. Shahabaddin Ebrahimi Atani. He received the Ph.D. degree in 2010 where he worked on "Design and implementation of a stream cipher for mobile communications" as his PhD dissertation. He has an assistant professor position in Department of Computer Engineering at the University of Guilan. His research interests include Cryptology, Cryptographic Hardware and Embedded Systems (CHES), Computer and Network security, Information Hiding, Semi-Ring Theory and Semi-Module Theory.