International Journal of Innovative Computing, Information and Control
Volume **3**, Number **3**, June **2007**

ICIC International ©2007 ISSN 1349-4198
pp. **631–640**

A GA-BASED NEARLY OPTIMAL IMAGE AUTHENTICATION APPROACH

Chien-Chang Chen and Cheng-Shian Lin

Department of Computer Science
Hsuan Chuang University
Hsinchu 300, Taiwan
cchen34@hcu.edu.tw

Received February 2006; revised October 2006

Abstract. *In this paper, we present how to find nearly optimal positions for embedding authentication message by Genetic Algorithm (GA), so as to achieve high quality protected image in image authentication problem. Correlations between important DCT coefficients and user defined thresholds constitute the image authentication message. The embedding positions are simulated as chromosomes and we use GA operators, such as reproduction, crossover, and mutation to find nearly optimal embedding positions. Experimental results demonstrate that GA can improve the image quality of protected image effectively.*
Keywords: Genetic algorithm (GA), Image authentication

1. **Introduction.** Recently, massive amounts of data are easily downloaded through the Internet since the rising and flourishing of computer and Internet technology. The convenience of file transmission over networks lets attackers acquire and modify digital content handily. Therefore, the copyright protection has become a very important issue, and this problem can be solved by digital watermark and image authentication techniques.

However, digital watermark differs from image authentication. Digital watermark identifies the legal ownership when a digital watermarked image suffers malicious attacks, but digital watermark cannot detect modification places [3,4,8,11]. Unlike digital watermark, image authentication points out the maliciously altered areas.

The image authentication problem can be classified into watermark-based approach and signature-based approach according to where the signature is located. Both of them extract important features from an image. The watermark-based approach embeds the authentication message into the host image. Thus the embedding quantity must be limited to prevent destroying image quality [1,15]. On the contrary, the signature-based approach stores the authentication message into an extra file and the storage quantity can be much larger than the watermark-based approach [5,14]. However, requiring extra space is a load in signature-based approach.

Besides, in order to reduce image data size, some desirable image compression, such as JPEG, would always be used. Some important works have been proposed to overcome this image compression problem. Extending of Yueng and Mintzer's [17] technique, Wu and Liu [16] proposed schema verification in quantized DCT coefficients via look-up-table. Sun *et al.* [13] discovered that the largest singular value of SVD survives under JPEG

compression and they proposed an SVD-based watermarking strategy that can survive under JPEG compression. Ho and Li [7] computed the feature codes from the relative sign and magnitudes of DCT coefficients. Lin and Chang [10] proposed quantization invariance property that exists during JPEG compression. Chen and Lin [2] further improved Lin and Chang's property [10] to propose two more efficient properties to acquire a watermark-based image authentication strategy.

Although we have proposed an image authentication approach [2] that can detect malicious attack and tolerate JPEG compression efficiently, one possible drawback of our approach [2] is that embedding a lot of authentication message reduces the image quality of protected image. Furthermore, Some researchers utilize the evolutionary computation strategy to acquire nearly optimal solution. Huang and Wu [9] explored the optimal watermark embedding positions by GA, so as to improve quality of the protected image efficiently. Shieh *et al.* [12] examined the correlation between robustness and quality of protected image by GA. Thus, in this paper, we apply GA on our previously proposed framework [2] to improve the image quality of protected image. We simulate the embedding positions as chromosomes in the evolution process. Then we obtain the nearly optimal embedding positions by natural selection and GA operators. Thus, the whole evolution of GA can efficiently achieve high quality protected image.

The rest of this paper is organized as follows. In Section 2, we review our previously proposed JPEG tolerance image authentication approach. Section 3, we briefly depict the GA. Section 4 describes the algorithm that uses GA to improve the image quality of protected image. Section 5 demonstrates the experimental results and discussion of our proposed approach. Finally, conclusion is given in Section 6.

2. Brief Review of Previously Proposed Quantization Properties and Image Authentication Approach.

Our previously proposed JPEG tolerant image authentication approach [2] is briefly reviewed in this section. Section 2.1 shows two important quantization properties QSIP and FQP. Sections 2.2 and 2.3 review previously proposed message embedding and verification approaches, respectively.

2.1. Two important quantization properties.

2.1.1. *The quantization sum invariant property (QSIP).* The QSIP discusses the correlations between the sum of two coefficients p, q and the quantization step Q. The proposed QSIP is defined as follows. Assume p, q are two DCT coefficients at different blocks with the same position and $\tilde{p}$, $\tilde{q}$ are their JPEG quantization results as $\tilde{p} = \left[\frac{p}{Q}\right] \cdot Q$ and $\tilde{q} = \left[\frac{q}{Q}\right] \cdot Q$, where Q is the quantization step and [] is integer round off. Since JPEG lets user define the quantization table and use the same quantization table to quantize all DCT blocks, we define the QSIP as the following:

(I) if $p + q < k$, then

$$\tilde{p} + \tilde{q} \leq \left(\left[\frac{k}{Q}\right] + 1\right) \cdot Q \tag{1}$$

(II) if $p + q \geq k$, then

$$\tilde{p} + \tilde{q} \geq \left(\left[\frac{k}{Q}\right] - 1\right) \cdot Q \tag{2}$$

where k is a user defined threshold. Several thresholds can be selected to acquire a more precise detection. Important image block's information is acquired using above property as follows. For a predefined parameter k, the correlation of $p+q$ and k decides one bit of the authentication message. For example, if $p+q$ less than threshold k, we store bit 0 as one authentication bit, and we store bit 1 for other conditions. QSIP shows that before and after the quantization process, range of two coefficients' sum is strongly correlated.

2.1.2. *The further quantization property (FQP).* The FQP discusses the correlation between the difference D of two coefficients p, q and the further quantization step T satisfying the condition $T \leq D$. The FQP is defined as follows. Assume p and q are two DCT coefficients at different blocks with the same position. For any further quantization step T satisfying $T \leq D$ as $D = sT + r_2$ with $s = \left\lfloor \frac{D}{T} \right\rfloor \geq 1$ and $T > r_2 \geq 0$, we acquire the following two properties.

(1) If $p - q = D$, then

$$s \cdot T \leq \left[\frac{p}{T}\right] \cdot T - \left[\frac{q}{T}\right] \cdot T \leq (s+1) \cdot T \tag{3}$$

(2) If $p - q \geq 3D$, then

$$(s+1) \cdot T < \left[\frac{p}{T}\right] \cdot T - \left[\frac{q}{T}\right] \cdot T \tag{4}$$

Above FQP shows that when the differences before quantization are D and $3D$, their differences after quantization can be well distinguished. Therefore, we use these two properties to embed information into DCT coefficients.

2.2. **Message embedding approach.** The procedure of message embedding process is introduced as follows.

1. Decompose an image into 8×8 non-overlapping blocks, and then apply all blocks into DCT.
2. Divide all blocks into sets of pairs of DCT blocks by a secret mapping function.
3. For each pair of blocks

3.1 Utilize QSIP to obtain robust image feature code.

3.2 Encrypt the robust image feature code by a private key to acquire authentication message.

3.3 Embed above authentication message into original image via FQP.

4. All blocks perform inverse DCT (IDCT) to obtain the protected image.

2.3. **Message verification approach.** The message verification algorithm follows the message embedding procedure but replaces modification by comparison. The message verification algorithm is introduced as follows.

1. Decompose an image into 8×8 non-overlapping blocks, and then applies all block into DCT.
2. Divide all blocks into sets of pairs of DCT blocks by the same secret mapping function used in message embedding procedure.
3. For each pair of blocks

3.1 Utilize QSIP to obtain the image feature.

3.2 Decrypt the extracted authentication message by the public key.

3.3 Acquire the embedded authentication message via FQP.

3.4 Compare above two results in Steps 3.2 and 3.3 to determine whether these two blocks have been tampered with.

4. The test image is verified by comparing all pairs of DCT blocks in Step 3.4.

The verification approach checks each pair of blocks to figure out whether the decryption result of the extracted authentication message and the correlation of low frequency coefficients as embedded authentication message is consistent. This checking is based on two proposed properties QSIP and FQP. After measuring all pairs of blocks, we can accurately detect whether the tested image is maliciously modified or not.

3. **Overview of Genetic Algorithm.** Genetic Algorithm (GA), first introduced by John Holland in 1975, is a global search method that simulates the natural biological evolution based on Darwin's "survival of the fittest" to solve optimal problems [6].

GA starts with randomly initializing population of possible solutions. Each individual possible solution in the population represents a chromosome. These chromosomes compete with each other under limited environment. Those individuals that survive in the competitive environment have the opportunity to breed the offspring using GA operators, such as reproduction, crossover, and mutation, based on their fitness values from one generation to next. Finally, the survival individuals fit better to the competitive environment than the original individuals, just as in natural adaptation.

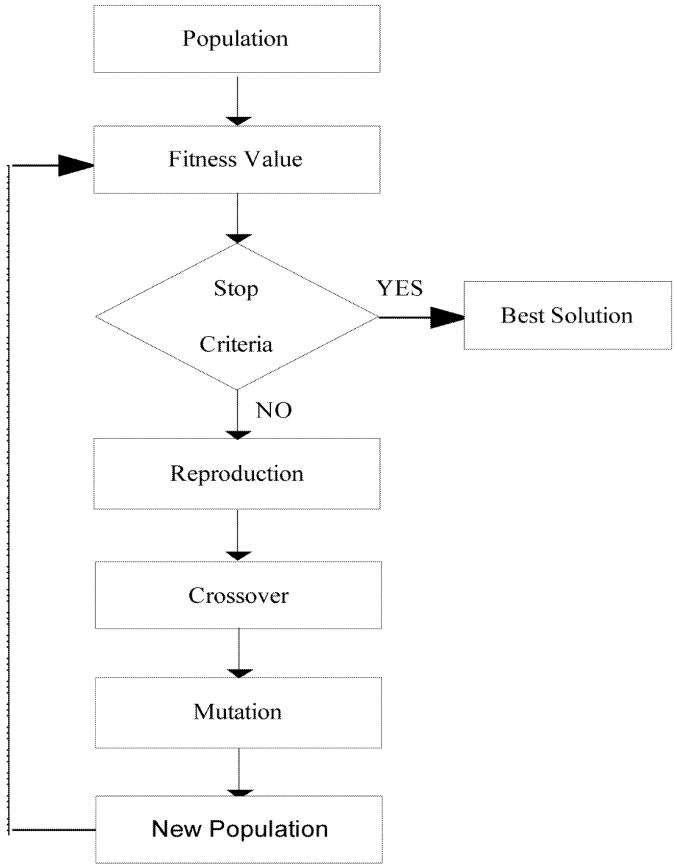


FIGURE 1. The flow chart of a simple GA

Figure 1 shows the flow chart of a simple GA. Five primarily components of GA are depicted as follows:

(1) Chromosome: a binary string representing one possible solution.

(2) Population: a set of chromosomes.

(3) Fitness function: a measurement of how well the chromosome fits the search space.

(4) Genetic operator:

(a) Reproduction: Next generated chromosomes are selected based on the fitness value. The reproduction operator can be classified into two methods: (1) roulette-wheel method and (2) elitism selection method.

(b) Crossover: The chromosomes with higher fitness values generate more offspring. The crossover operator is classified into three methods: (1) one-point crossover, (2) two-point crossover, and (3) uniform crossover.

(c) Mutation: Genes of chromosomes are randomly changed based on predefined mutation rate. The mutation operator is generally classified into two methods: (1) one-point mutation and (2) uniform mutation.

(d) Stop criterion: If a criterion has reached, it would stop searching. Otherwise, carry on the evolution. The stop criterion can be number of generations.

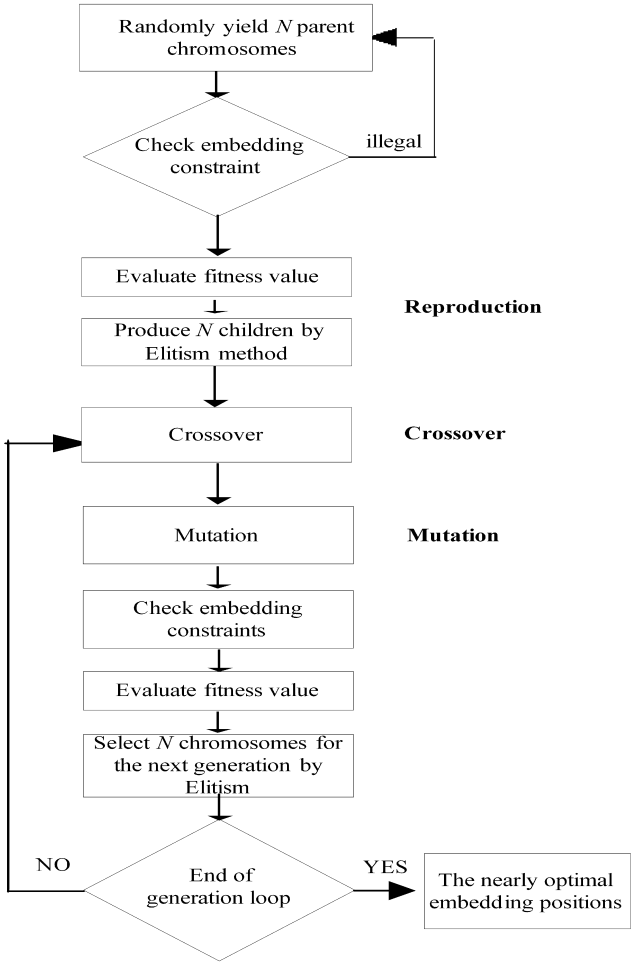


FIGURE 2. The GA-based image authentication algorithm

4. **The Proposed GA-based Image Authentication approach.** This section illustrates our proposed GA-based image authentication approach. Since our previous proposed DCT-based image authentication system [2] embeds authentication message into fixed positions, we then utilize the GA to find nearly optimal embedding positions in each pair of DCT blocks. Figure 2 depicts the GA-based optimization algorithm for each pair DCT block.

4.1. **Chromosome definition.** Before performing the embedding procedure, we need to transform the test image into DCT domain. The coordinates of the embedding position (X, Y) in an 8×8 DCT coefficient block can be defined as Figure 3.

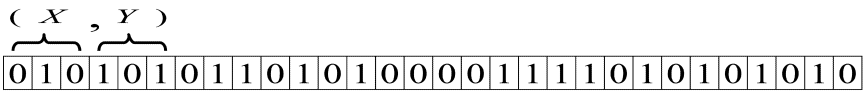


FIGURE 3. Chromosome definition with position $(X = 2, Y = 5)$

Note that, chromosome definition has the following four constraints:

1. DC value cannot be modified in the authentication message embedding process.
2. In each pair of DCT blocks, the positions that have been selected could not be selected again.
3. In each pair of DCT blocks, positions with standard quantization values between 13 and 60 are selected during the GA-based selection process.
4. Difference between two selected DCT coefficients must be smaller than three times of the standard quantization value.

4.2. **Evolution algorithm.** The fitness function and GA operator parameters determine the image quality of protected image. Hence, we explain how they work in evolution process as follows:

(I) Randomly select N chromosomes satisfying above four constrains.

(II) The fitness function measures how good a set of embedding position is. We choose an image quality assessment, Mean Square Error (MSE), to be our fitness function. The MSE is defined as follows:

$$\text{MSE} = \frac{1}{N_X \times N_Y} \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} [g(i,j) - f(i,j)]^2$$

where g is the protected image, f is the original image, and N_X, N_Y are position range in X, Y axes.

(III) GA operators.

(a) Reproduction. After calculating the fitness value of each parent chromosome, we use the elitism method that keeps N chromosomes with higher fitness values to generate children.

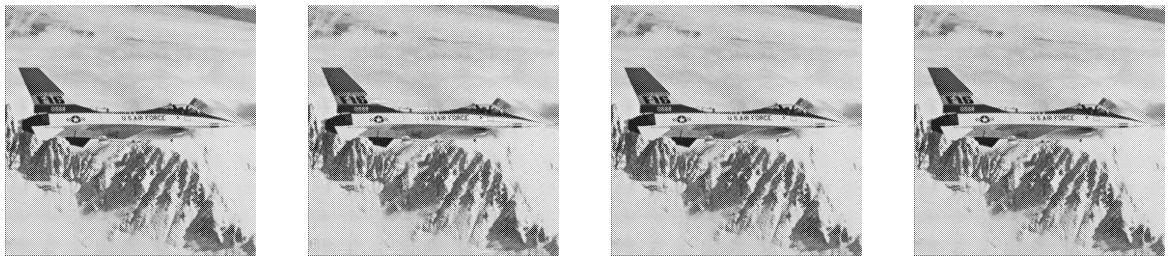
(b) Crossover. After performing reproduction process, we have N parent chromosomes. The newly reproduced chromosomes are randomly mated in a pair of parent chromosomes and then calculate their fitness values. When a new chromosome's fitness value is higher than its parents, the parent chromosomes would be replaced. Our experiment empirically determines the crossover rate being 0.5.

(c) Mutation. We apply one-point mutation with two different mutation rates. We flip each gene of the chromosome with smaller probability than predefine mutation rate in the earlier stage of evolution and flip genes with higher probability in the later stage. These two different mutation rates are empirically determined as 0.01 and 0.08.

(IV) Some children's chromosomes may not satisfy the chromosome constraints. Thus, we examine each chromosome and discard illegal ones to acquire N legal chromosomes for the next generation. At last, we obtain nearly optimal embedding positions for the protected image by repeatedly applying the GA operations to each pair of DCT blocks.

5. **Experimental Results and Discussion.** We demonstrate the experimental results of two test images "LENA" and "F16" with size 256×256. The population size N is 6. The authentication message is composed of extracting 5 bits from each pair of DCT blocks. In each pair of blocks, comparing the lowest DCT coefficient at position (0,0) with thresholds 263, 1051, 2983 acquires 3 bits and comparing two DCT coefficients at positions (1,0) and (0,1) with threshold 263 acquires 2 bits. These 5 bits form the authentication message. Note that a DCT block is positioned from (0, 0) to (7, 7) and thresholds 263, 1051, 2983 are empirically selected. Then we apply the proposed GA-based approach to search for nearly optimal embedding positions.

The experimental results of previously proposed algorithm [2] demonstrate in Figure 4(b) and 5(b) with PSNRs 35.20dB and 36.29dB. The GA-based algorithm successfully finds nearly optimal embedding positions to improve the image quality of protected image as Figure 4 (c), (d) and Figure 5 (c), (d) with generations 60, 120. Figure 6 plots the correlations between different generation numbers and their corresponding PSNRs. The image quality of protected image is improved when the number of generations increases. Figure 7 demonstrates the correlations between generation number and computation time. We obviously figure out that large generation number causes heavy computation load. The simulation is programmed in MATLAB. Thus, we conclude that the proposed GA-based image authentication approach can improve the image quality of protected image efficiently, though more computation time is needed.



(a) (b) (c) (d)

FIGURE 4. (a) The original test image F16 with size 256×256, (b) experimental result of previous proposed algorithm with PSNR=35.20dB, (c) embedding authentication message by 60 generations evolution with PSNR=41.71dB, (d) embedding authentication message by 120 generations evolution with PSNR=42.21dB.

(a) (b) (c) (d)

FIGURE 5. (a) The original test image LENA with size 256×256, (b) experimental result of previous proposed algorithm with PSNR= 36.29 dB, (c) embedding authentication message by 60 generations evolution with PSNR= 42.13 dB, (d) embedding authentication message via 120 generations evolution PSNR= 42.45 dB.

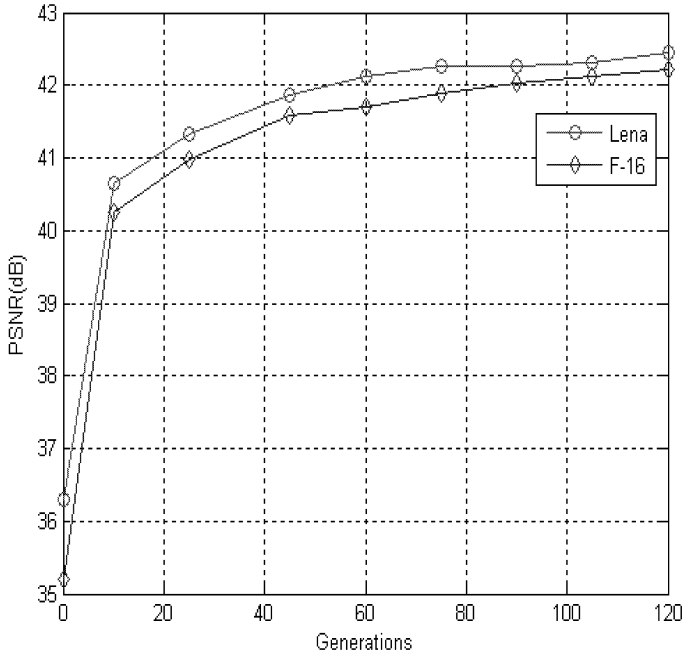


FIGURE 6. Generations vs. PSNR

6. **Conclusion.** We propose a GA-based image authentication approach to improve the image quality of a protected image. In the evolution process, the embedding positions are simulated as chromosomes. The nearly optimal embedding positions are then obtained by natural selection that employs Mean Square Error and GA operators. Finally, the experimental results demonstrate that the quality of the protected image can be significantly improved when the generation number is large enough though more computation time is required. How to reduce the computation time merits future study.

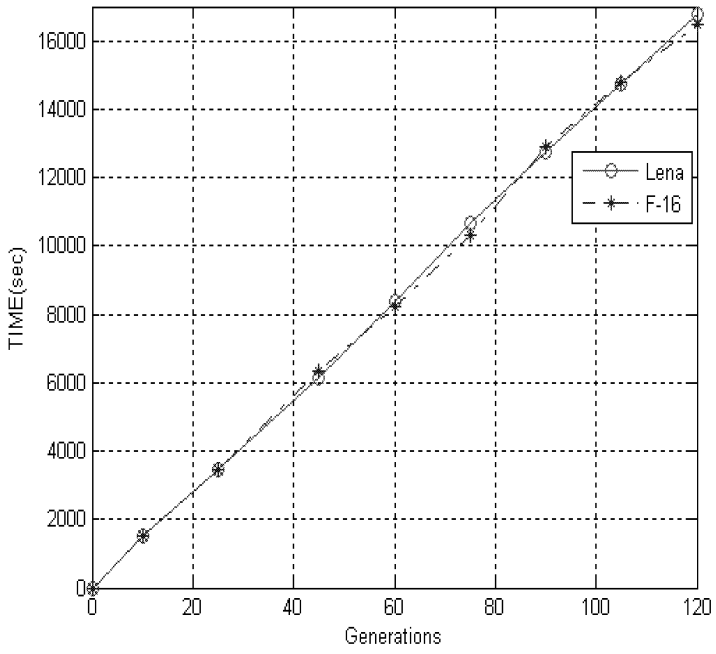


FIGURE 7. Generations vs. calculation cost

Acknowledgment. The authors would like to thank the two reviewers for their valuable comments.

REFERENCES

[1] Barreto, P. S. L. M., H. Y. Kim and V. Rijmen, Toward a secure public-key blockwise fragile authentication watermarking, *IEE Proceedings - Vision, Image and Signal Processing*, vol.149, no.2, pp.57-62, 2002.

[2] Chen, C. C. and C. S. Lin, Toward a robust image authentication method surviving JPEG lossy compression, *Journal of Information Science and Engineering*, vol.23, no.2, pp.511-524, 2007.

[3] Chu, W. C., DCT-based image watermarking using subsampling, *IEEE Transactions on Multimedia*, vol.5, pp.34-38, 2003

[4] Cox, I., M. Miller and J. Bloom, *Digital Watermarking*, Morgan Kaufman Publishers, 2002.

[5] Garg, G., P. K. Sharma and S. Chaudhury, Image based document authentication using DCT, *Pattern Recognition Letters*, vol.22, pp.725-729, 2001.

[6] Goldberg, D. E., *Genetic Algorithm in Search, Optimization & Machine Learning*, Addison-Wesley, 1989.

[7] Ho, K. and C. T. Li, Semi-fragile watermarking scheme for authentication of JPEG Images, *Proc. of the IEEE International Conference on Information Technology: Coding and Computing*, vol.1, pp.7-11, 2004.

[8] Hsu, C. T. and J. L. Wu, Hidden digital watermarks in images, *IEEE Transactions on Image Processing*, vol.8, no.1, pp.58-68, 1999.

[9] Huang, C. H. and J. L. Wu, A watermark optimization technique based on genetic algorithms, *SPIE-Visual Communications and Image Processing*, 2000.

[10] Lin, C. Y. and S. F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, *IEEE Transactions on Circuits and Systems of Video Technology*, vol.11, pp.153-168, 2001.

[11] Lin, S. D. and C. F. Chen, A robust DCT-based watermarking for copyright protection, *IEEE Transactions on Consumer Electronics*, vol.46, no.3, pp.415-421, 2000.
[12] Shieh, C. S., H. C. Huang, F. H. Wang and J. S. Pan, Genetic Watermarking based on transform-domain techniques, *Pattern Recognition*, vol.37, no.3, pp.555-565, 2004.
[13] Sun, R., H. Sun and T. Yao, A SVD and quantization based semi-fragile watermarking technique for image authentication, *Proc. of the IEEE International Conference on Signal Processing*, vol.2, pp.1592-1595, 2002.
[14] Tsai, P., Y. C. Hu and C. C. Chang, Using set partitioning in hierarchical trees to authenticate digital images, *Signal Processing: Image Communication*, vol.18, pp.813-822, 2003.
[15] Wong, P. W. and N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, *IEEE Transactions on Image Processing*, vol.10, pp.1593-1601, 2001.
[16] Wu, M. and B. Liu, Watermarking for image authentication, *Proc. of the IEEE International Conference on Image Processing*, vol.2, pp.437-441, 1998.
[17] Yueng, M. and F. Mintzer, An invisible watermarking technique for image verification, *Proc. of the IEEE International Conference on Image Processing*, vol.2, pp.680-683, 1997.