

An Associative Watermarking based Image Authentication Scheme

Lamiaa M. El Bakrawy¹, Neveen I. Ghali¹, Aboul Ella Hassanien² and Ajith Abraham³,

¹*Faculty of Science, Al-Azhar University, Cairo, Egypt*
Email: lamiaabak, nevgghali@yahoo.com

²*Faculty of Computers and Info., Cairo University, Cairo, Egypt*
Email: aboitcairo@gmail.com

³*Machine Intelligence Research Labs, MIR Labs, USA*
Email: abraham.ajith@gmail.com

Abstract—In this paper, we propose an associative watermarking scheme which is conducted by the concept of Association Mining Rules (AMRs) and the ideas of Vector Quantization (VQ) and Sobel operator. Performing associative watermarking rules to the images will reduce the amount of the embedded data, and using VQ indexing scheme can easily recall the embedded watermark for the purpose of image authentication, and establishing the relation between the association rules on both the original image and the watermark image. The Vector Quantization decoding technique is applied to reconstruct the watermarked image from the watermarked index table. The experimental result shows that the proposed scheme is robust. When the watermarked images suffered from various kinds of image-processing procedures, such as Gaussian noise, brightness, blurring, sharpening, cropping, and JPEG lossy compression can be detected without the original images assistance.

I. INTRODUCTION

In the modern world of information, any kind of data is available to anyone over the Internet. Of all the data transmitted over the Internet, images are the most common means of message conveyance. However, the convenient access to the images on the Internet makes it easy for anyone to download, copy, edit, or distribute images with ease, which of course has a direct and severe impact on the copyright owners (many times the image creators themselves). Therefore, copyright protection for intellectual property on the Internet is an important issue [1], [2], [12]. Digital watermarking techniques have been proposed for the copyright protection of digital images [10]. In digital watermarking techniques, some types of watermarks such as logos, labels, trademark, or random sequence, representing the author's ownership, are embedded into the desired digital image. Generally, a registration to the authentication center is necessary, which helps to solve ownership disputes by identifying the owner of the disputed media. If necessary, the embedded watermark in the digital image can be used to verify ownership [11], [16].

Watermarking techniques have been studied extensively

in the past. By taking account of the domain in which the watermark is embedded. Watermarking techniques can be classified into two broad categories: spatial domain and frequency domain techniques [3], [4]. In spatial domain schemes, the watermark is embedded by directly modifying the pixel values of the host image. On the other hand, watermarking techniques used in the spatial domain directly modify coefficients of images to achieve the purpose for watermarking [5], [16]. The watermarking technique proposed in this paper is based on vector quantization (VQ) [11], [12]. Strictly speaking, VQ cannot be categorized into either of the above types; rather, it is a kind of image compression technique that uses indices of codewords in the codebook to represent the input image and finally refers the index table as the original image.

The remainder of this paper is organized as follows. Brief introduction of vector quantization (VQ), association rule, and edge block detection are respectively introduced in Section (II). The detailed of the proposed scheme is presented in Section (III). Section (IV) shows the experimental results. Conclusions are discussed in Section (V).

II. AN OVERVIEW

A. Vector quantization (VQ)

VQ is a simple data compression technique which was first proposed by Gray [2]. In the beginning, an image is segmented into several blocks with the same size, such as 4×4 . Each block consists of 16 pixels. These pixels, from left to right and top to bottom, can form a vector $v = \{v_1, v_2, \dots, v_k\}$, where k represents number of dimensions. The pixel value of each block is different, so before encoding, representative vectors, called codeword c , should be collected to form a codebook $CB = \{c^i : i = 1, \dots, L-1\}$, where L denotes the codebook size and i denotes the index value. The well-known LBG algorithm [11] can be employed to form the codebook. By clustering code words, it finds a representative codeword from each cluster and uses the representative code words to form a codebook. Through

Euclidean distance $d(v, c^i)$ shown in Eq. (1), where v_j and c_j^i are respectively the j^{th} elements of the vector v and c^i , we can find code words nearest to the input vector and record the index value of each code word.

$$d(v, c^i) = \sqrt{\sum_{j=0}^{k-1} (v_j - c_j^i)^2} \quad (1)$$

Once the closest codeword for v is found, the index i of the best matching codeword is assigned to the input vector v for the basis of future VQ decoding. VQ facilitates compression by means of transmitting or storing the index of the codeword instead of the codeword itself. In the decoding phase, the decoder also utilizes the same codebook to perform a simple table look-up operation for each index i , so as to obtain the corresponding codeword c_i . Finally, c_i is applied to reconstruct the input vector v [2].

B. Association rules

Association rule mining, which was first proposed by Agrawal et al. [8], is one of the most important topics in the area of data mining, and has many successful applications, especially in the analysis of consumer market-basket data [6], [17]. An association rule is a probabilistic relationship, with the form $X \Rightarrow Y$ between sets of database attributes, where X and Y are sets and termed as itemsets, and $x \cap y = \Phi$. It is inferred empirically from examination of records in the database. Such a rule reveals that transactions in the database containing items in X tend to contain items in Y , and the probability, measured as the fraction of the transactions containing X also containing Y , is called the confidence of the rule. The support of the rule is the fraction of the transactions that contain all items in both X and Y [9].

C. Edge block detection method - the Sobel operator

Edge detection is the task of finding the boundaries between the objects that appear in a digital image [13]. Sobel operator is used to detect image edges by calculating partial derivatives in 3×3 neighborhoods. The reason of using Sobel operator is that it is insensitive to noise and it has relatively small masks than other operator such as Robert operator, two-order Laplacian operator and so on [14]. The detection Equations (2) and (3).

$$G_x = (Z_7 + 2Z_8 + Z_9) + (Z_1 + 2Z_2 + Z_3) \quad (2)$$

$$G_y = (Z_3 + 2Z_6 + Z_9) + (Z_1 + 2Z_4 + Z_7) \quad (3)$$

where Z 's are the gray levels of the pixels inside the mask. The masks are moved pixel by pixel and the procedure is repeated until all possible locations have been computed. Finally, the result generated in the gradient image whose size is the same as the original image. The block under

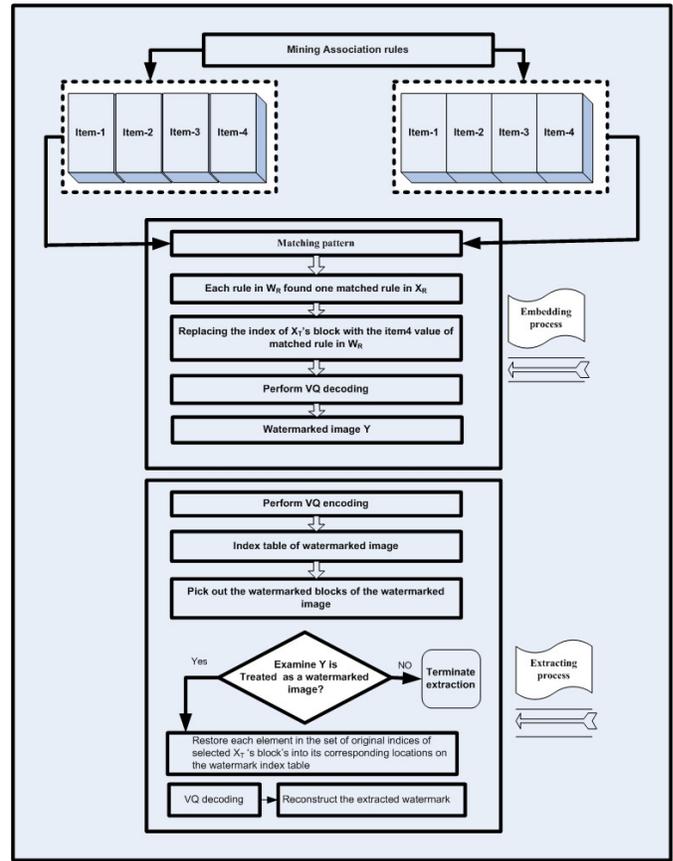


Figure 1 The overview of the proposed algorithm

consideration will be regarded as an edge block if any value of those two computed values is larger than the reselected threshold value [15].

III. THE PROPOSED IMAGE AUTHENTICATION SCHEME

In the proposed method both the original image X with size $A_X \times B_X$ and the watermark W with size $A_W \times B_W$ are divided into non-overlapping blocks with size $k \times k$, and for each block, the codebook C (including Lk^2 -dimensional codewords) is utilized to find the closest codeword so as to obtain the index tables of the original image and watermark, X_T and W_T , respectively. The size of X_T and W_T are $(\frac{A_X}{k} \times \frac{B_X}{k})$ and $(\frac{A_W}{k} \times \frac{B_W}{k})$. Subsequently, association rules defined upon 4-itemset are exploited to mine association rules from X_T and W_T , respectively. Then we embed the association rules generated from the watermark into the original image, the overall description of the proposed system are given in Figure (1).

A. Mining Association rules of the original image and watermark

For each index in the index tables of original and watermark images the 4-itemset association rules can be illus-

trated as $(item1, item2, item3) \Rightarrow (item4)$. The first three items are utilized to find the nearest original image rules for the watermark rules, and by changing the fourth item's value of the rule, which is derived from some selected original image blocks, such that the watermark can be embedded. The four items for each block's rule are defined in Algorithm 1.

Algorithm 1 The four items for each block's rule

Input Parameters: T, S, Imagearray, ImageCells, Normalizedfactor

Phase-I Embedding :

- 1: Calculate the mean of its index and the indices of its neighboring eight blocks
 - 2: **if** the mean value $\geq T_1$ **then**
 - 3: Item1 = 1
 - 4: **else**
 - 5: Item1 = 0
 - 6: **end if**
 - 7: Calculate the variance of its index and the indices of its neighboring eight blocks
 - 8: **if** the variance value $\geq T_2$ **then**
 - 9: Item2 = 1
 - 10: **else**
 - 11: Item2 = 0
 - 12: **end if**
 - 13: Sobel is applied to do convolution on this block to determine whether its corresponding codeword is an edge block or not
 - 14: **if** any value of those two computed values $\geq T_3$ **then**
 - 15: this block is an edge block, and Item3 = 1
 - 16: **else**
 - 17: it is = 0
 - 18: **end if**
 - 19: The item4 value is the corresponding index value indicated in the index table, Where T_1, T_2, T_3 are given threshold.
-

B. Embedding Process

The detailed procedure of hiding association rules W_R in X_R being derived from X_T and W_T is described as follows:

- 1) The first three items play a role as the matching pattern in X_R and W_R . (i.e. if a rule $w_r = \{(1, 0, 1) \Rightarrow 5\}$ in W_R , then the matched rule from X_R will be $\{(1, 0, 1) \Rightarrow *\}$ where $* \in [0, L - 1]$). This matching process is repeated until each rule in W_R has found at least one matched rule in X_R , if there is any rule in W_R unable to find a matched rule in X_R , go to 2; otherwise, go to 3.
- 2) If any rule in W_R has no matched rule in X_R , any of the first three item values of this rule must be changed,

and go to 1. This process is repeated until each non-matched rule in W_R find at least one matched rule in X_R .

- 3) If any rule w_r in W_R has more than one matched rules, say s rules $x_{r1}, x_{r2}, \dots, x_{rs}$, the selected rule x_r is so-called the most similar rule to w_r . The similarity is defined as follows:

$$Similarity = \frac{1}{MSE - T_M} \quad (4)$$

$$MSE = \frac{1}{k \times k} \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} ((c_{w_r}(i, j) - c_{x_{rt}}))^2 \quad (5)$$

Where $1 \leq t \leq s$, T_M is a given threshold, c_{w_r} is the codeword denoted by the index taken from the item4 value of w_r , and $c_{x_{rt}}$ is the codeword denoted by the index taken from the item-4 value of rule x_{rt} which represents each rule of $x_{r1}, x_{r2}, \dots, x_{rs}$.

- 4) For any rule x_r in $\{x_{r1}, x_{r2}, \dots, x_{rs}\}$. If there are more than one X_T 's block which derived the same rule x_r , then one of these x_r 's relevant blocks is randomly selected for the watermark information. Subsequently, by replacing the index of this block with the item4 value of w_r , the purpose for watermarking is successfully achieved.
- 5) VQ decoding is performed on the watermarked index table, which has been embedded with all the rules in W_R , to reconstruct the watermarked image.

C. Extracting Process

For extracting the watermark from the watermarked image Y . Four keys should be recorded.

- 1) key1: the set of all selected X_T 's block's locations.
- 2) key2: the set of original indices of these blocks.
- 3) key3: the MSE values between the codewords of original indices of these blocks, and the codewords of indices of these blocks after embedding.
- 4) key4: for each element of key2, record all of its corresponding blocks in W_T

Then the detailed process is described as follows:

- 1) Perform VQ encoding on the test image Y to obtain the index table Y_T .
- 2) Use key_1 to pick out the watermarked blocks Y_{TW} from Y_T .
- 3) Calculate the MSE values between the code words indexed by all the elements in Y_{TW} and key_2 .

$$mse(1) = MSE(c_{Y_{TW}}(1) - C_{Key_1}(1)) \quad (6)$$

Let Q be the set comprised of all the $\{mse(l)\}$, l is the l^{th} element in Y_{TW} and key_2 , $c_{Y_{TW}}(l)$ and $c_{key_2}(l)$ stand for the codewords with indices $Y_{TW}(l)$ and

$key_2(l)$, respectively; and $MSE(c_{YTW}(l), c_{key_2}(l))$ is the MSE value calculated from these two codewords.

4) Given a threshold T_R and key_3 , Set

$$R = \{mse(l) | mse(l) \leq key_3(l) \times T_R\} \quad (7)$$

and calculate

$$P = \frac{|R|}{|Q|} \quad (8)$$

Where $|R|$ and $|Q|$ denote the total quantities of elements in R and Q

- 5) Given a threshold T_S . If $P \geq T_S$. Y is treated as a watermarked image and goes to 6, Otherwise, Y is not watermarked, and the extraction is terminated.
- 6) According to key_4 , restore each element in key into its corresponding locations on the watermark index table.
- 7) Do VQ decoding with the above results to reconstruct the extracted watermark

IV. EXPERIMENTAL RESULTS

In this paper we compare our experimental results with the method proposed by Shen and Ren [11]. This is because that the authors utilized the concepts of vector quantization (VQ) and association rules in data mining to propose a robust watermarking technique. The 4×4 masks are used to detect edge block and each mask stands for different direction occurring in the edge block. Afterwards, those masks are applied to do convolution on the 4×4 image block.

In this research, PSNR (Peak Signal-to-Noise Ratio) is used to evaluate the difference between the watermarked image and the original image; NC (Normalized Correlation) is applied to determine the degree of similarity between the original watermark and the extracted watermark. Here, A_X and B_X represent the height and width of the original image X , respectively. A_W and B_W are the height and width of watermark W . X_W and X_W separately denotes the watermarked image and the extracted watermark.

The original image and the watermark are divided into non-overlapping blocks with size 3×3 . The codebook used in this study adopts the traditional LBG method [18] to train a grayscale Lena image with size 512×512 , and the threshold for the termination of training is set as 0.05. There are 256 codewords in this codebook, and the size of each codeword is 3×3 pixels. Sobel operator is used to detect edge block since Sobel operator is insensitive to noise and it has relatively small masks than other operators such as Robert's operator, two-order Laplacian operator and so on. The original image used in the experiments is a grayscale Lena image with size 512×512 .

Since in [11], the watermark is binary, in order to make the comparison of different methods objectively, binary watermark is applied. Here, watermarks with

different sizes are considered in the experiments. Also the parameters in this paper are the same in [11]. First, for convenience, the thresholds T_1 and T_2 are set as the half of the codebook size which is 128. The threshold T_3 applied to determine whether an image block is an "edge block" is set to 70, and $T_M = 80$ is selected since it ensures the better PSNR value, threshold T_R and T_S for the judgment of whether an image is embedded with a watermark or not are set as 0.1 and 0.35, respectively.



(a) Watermarked with PSNR = 31.9998(dB)



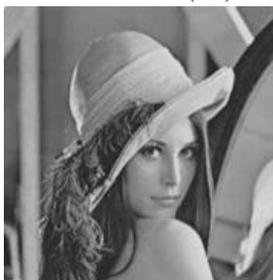
(b) Extracted watermark (64 × 64) with NC = 0.9928



(c) Watermarked with PSNR = 31.8379(dB)



(d) Extracted watermark (128 × 128) with NC = 0.9871



(e) Watermarked with PSNR = 31.8379 (dB)



(f) Extracted watermark (256 × 128) with NC = 0.9875

Figure 2 Watermarking image and its watermark extraction

The image pixel of the binary watermark in our method is either 0 or 255. In order to minimize the distortion of the extracted watermark in this approach, the codeword with all values only 0 (c0) and the codeword with all values only 255 (c255) will be produced, and then replace these two codewords nearest to c0 and c255, respectively. MSE (Mean-Square Error) as mentioned above is utilized

to decide two codewords will be modified to c_0 or c_{255} . Thus, the codeword with the minimum MSE value between c_0 and the codeword itself will be changed to c_0 . Similarly, the codeword with the minimum MSE value between c_{255} and the codeword itself will be changed to c_{255} . Besides, since the codebook applied in our method is grayscale, the extracted watermark will be in grayscale form. However, in order to make objective comparisons between our approach and [11], the extracted grayscale watermark will be polarized. That is, the pixels with values larger than or equivalent to 128 will be reset to 255, and the pixels with values smaller than 128 will be reset to 0, respectively. Fig. 2 shows watermarked images and the corresponding extracted watermarks of the proposed method.

Table (I) shows that the value of PSNR of watermarked images with different sizes of watermarks in the proposed method is greater than the value of PSNR of watermarked images in Shen and Ren method. It means that the watermarked image of our proposed method have better image quality. Since NC value can be anywhere between 0 and 1. The closer the NC value is to 1, the higher the accuracy is for the extracted watermark [14]. So the extracted watermark of our proposed method is more accuracy than the extracted watermark of Shen and Ren's method.

Also the well-known image processing software, Photoshop, is applied to perform 32 image attacks (including JPEG lossy compression (quality level 0, 1, 2, ..., 12), sharpening (1-3 times), adding in Gaussian noise ($\sigma = 2, 4, 6, 8, 10, 15$ and 20), blurring (1-3 times) and 6 kinds of cropping methods) on the watermark images. Then NC is used to compare the difference between the original watermark and the extracted watermark. After applying 6 kinds of cropping attacks, JPEG lossy compression (quality level = 0), sharpening three times, adding in Gaussian noise ($\sigma = 20$) and blurring three times to watermarked images of the proposed method and Shen and Ren's method, we can obtain the corresponding extracted watermarks. Table II shows that no matter which kinds of attacks the watermarked images suffer from, extracted watermarks are still similar with the watermark extracted from non-attacked watermarked image. Moreover, NC values calculated from extracted watermarks using the proposed method outperform Shen and Ren's method especially in case of Gaussian noise and blurring.

Table I
PSNR OF WATERMARKING IMAGE AND NC OF ITS WATERMARK EXTRACTION

| watermark Size | PSNR proposed method | NC proposed method | PSNR Shen & Ren method | NC Shen & Ren method |
|------------------|----------------------|--------------------|------------------------|----------------------|
| 64×64 | 31.9998 | 0.9928 | 30.8683 | 0.9872 |
| 128×128 | 31.8379 | 0.9871 | 30.7539 | 0.9772 |
| 256×128 | 31.8379 | 0.9875 | 30.7493 | 0.9843 |

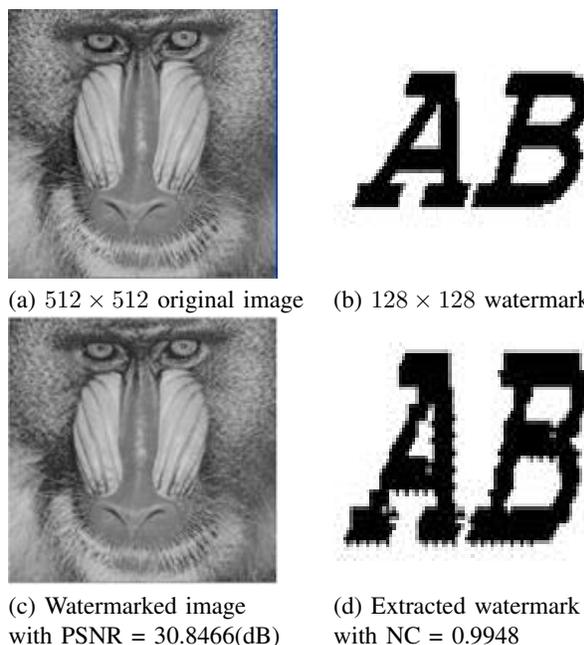


Figure 3 Watermarking image and its watermark extraction

Finally, we use another 512×512 image, Mandril and another watermark to emphasis that the proposed method can be easily applied in different kinds of protected images. Figs. 3(a) and 3(b) are the original images, 128×128 watermark. Figs. 3(c) is the corresponding watermarked image. It is noticed that PSNR values of the watermarked image is smaller than watermarked image, Lena, since the codebook was trained using Lena only. Figs. 3(d) shows the extracted watermark. Then, we also apply the same image processings, JPEG lossy compression (quality level = 0), sharpening three times, adding in Gaussian noise ($\sigma = 20$) and blurring three times, to the watermarked image, we obtain the corresponding extracted watermarks and there NC values are shown in table (III).

V. CONCLUSIONS

In this paper, a robust watermarking technique is proposed using vector quantization (VQ) and association rules

Table II
COMPARISON BETWEEN THE NC VALUES OF WATERMARKS EXTRACTED FROM ATTACKED WATERMARKED IMAGES OF PROPOSED METHOD AND SHEN AND REN'S METHOD

| Experiments | The proposed method | Shen & Ren method |
|--|---------------------|-------------------|
| Quarter-cropped | 0.9584 | 0.9509 |
| Quarter-cropped and filled with pixels valued | 0.9629 | 0.9618 |
| Quarter-cropped and replaced with the original image | 0.9600 | 0.9566 |
| Half-cropped | 0.9593 | 0.9566 |
| Half-cropped and filled with pixels valued | 0.9415 | 0.9344 |
| Half-cropped and replaced with the original image | 0.9516 | 0.9433 |
| JPEG lossy compression (quality level = 0) | 0.9578 | 0.9452 |
| sharpening three times | 0.9608 | 0.9519 |
| adding in Gaussian noise ($\alpha = 20$) | 0.9734 | 0.9314 |
| blurring three times | 0.9707 | 0.9457 |

Table III
NC VALUES OF WATERMARKS EXTRACTED FROM ATTACKED WATERMARKED IMAGES OF PROPOSED METHOD

| Experiments | NC |
|--|--------|
| JPEG lossy compression (quality level = 0) | 0.9918 |
| sharpening three times | 0.9908 |
| adding in Gaussian noise ($\sigma = 20$) | 0.9943 |
| blurring three times | 0.9933 |

depending on Sobel operator to detect edge of image. The reason of using Sobel operator was insensitive to noise and it has relatively small masks than other operator such as Robert's operator and two-order Laplacian operator. The experimental result shows that the proposed scheme achieves more effective resistance against several images processing such as blurring, sharpening, adding in Gaussian noise, cropping, and JPEG lossy compression especially in case of Gaussian noise and blurring.

REFERENCES

- [1] Shen, J., Hsu, P., A robust associative watermarking technique based on similarity diagrams, Pattern Recognition Society, vol.40, pp.1355 - 1367, 2007.
- [2] Yang, C., Shen, J., Recover the tampered image based on VQ indexing, Signal Processing, Vol.90, pp.331-343, 2010.
- [3] Yen, E., Lin, L., Rubik's cube watermark technology for grayscale images, Expert Systems with Applications, Vol.37, pp.4033-4039, 2010.
- [4] Shen, R., Fu, Y., Lu, H., A novel image watermarking scheme based on support vector regression, The Journal of Systems and Software, Vol.78, pp.1-8, 2005.
- [5] Aslantas, V., An optimal robust digital image watermarking based on SVD using differential evolution algorithm, Optics Communications, Vol.282, pp.769-777, 2009.
- [6] Shen, B., Yao, M., Wu, Z., Gao, Y., Mining dynamic association rules with comments, Knowl Inf Syst, Vol.23, pp.73-98, 2010.
- [7] Ma, W., Wang, K., Liu, Z., Mining potentially more interesting association rules with fuzzy interest measure, Soft Computing, Vol.10, pp. 1-10, 2010.
- [8] Agrawal, R., Imielinski, T., Swami, A., Mining association rules between sets of items in large Databases, Proceedings of the ACM SIGMOD conference on management of data, pp.207-216, 1993.
- [9] Linde, Y., Buzo, A., Gray, RM., An algorithm for vector quantization design, IEEE Transactions on Communications, Vol.28, pp.84-95, 1980.
- [10] Wang, Y., Doherty, J., Dyck, R., A wavelet-based watermarking algorithm for ownership verification of digital images, IEEE Transactions on Image Processing, Vol.11, pp.1-11, 2002.
- [11] Shen, J., Ren, J., A robust associative watermarking technique based on vector Quantization, Digital Signal Processing, Vol.10, pp.1- 16, 2009.
- [12] Wu, H., and Chang, C., A novel digital image watermarking scheme based on the vector quantization technique, Computers & Security , Vol.24, pp.460 - 471, 2005.
- [13] Meinhardt, E., Zacur, E., Frangi, A., Caselles, V., 3D Edge Detection by Selection of Level Surface Patches, Journal of Mathematical Imaging and Vision, Vol.34, pp.1-16, 2009.
- [14] Dong, Q., Song, C., Ben, C., Quan, L., A fast subpixel edge detection method using Sobel-Zernike moments operator, Image and Vision Computing, Vol.23, pp.11-17, 2005.
- [15] Fan, K., Kan, K., Chang, J., Edge preservice and block effect reduction by block coefficient diffusion method, Signal Processing, Vol.61, pp.171-180, 1997.
- [16] Tsai, P., Hu, Y., Chang, C., A color image watermarking scheme based on color quantization, Signal Processing, Vol.84, pp.95 - 106, 2004.
- [17] Weng, C., Chen, Y., Mining fuzzy association rules from uncertain data, Knowledge and Information Systems, Vol.9, pp.24, 2009.
- [18] Chang, C., Tsou, C., Chou, Y., A remediable image authentication scheme based on feature extraction and clustered VQ, Lecture Notes in Computer Science, Vol.4810, pp.446-449, 2007.