A Fragile Associative Watermarking on 2D Barcode for Data Authentication

Jau-Ji Shen[1] and Po-Wei Hsu[2]
(Corresponding author: Jau-Ji Shen)

Department of Management Information Systems, National Chung Hsing University[1]
250, Kuo Kuang Rd., Taichung 402, Taiwan
Institute of Information Management, National Formosa University[2]
Huwei, Yunlin County, Taiwan (Email: jjshen@nchu.edu.tw)

(Received Feb. 7, 2007; revised Apr. 23, 2007; accepted May 7, 2007)

Abstract

Two-dimensional (2D) barcode has improved the information encoded capacity, and it also has enriched the applications of barcode technique. Recently, there are researches dealing with watermark technique on 2D barcode to prevent it from counterfeited or prepensely tampered. The existent methods still have to limit the size of embedded watermark in a relatively small portion. Furthermore, it also needs to utilize original watermark or other auxiliary verification mechanism to achieve the barcode verification. In this paper, we propose a method called associative watermarking which is conducted by the concept of Association Rules (ARs) and the idea of Vector Quantization (VQ). Our method is a kind of blind watermarking, and it also can free the size limitation of an embedded watermark. Performing associative watermarking to 2D barcode can reduce the embedded information amount, and using VQ indexing scheme can easily recall the embedded watermark for the purpose of barcode data authentication. The experiment demonstrates that our method can significantly save the information hiding capacity of 2D barcode and detects a counterfeited or prepensely tampered 2D barcode data correctly.

Keywords: 2D barcode, association rules, associative watermark, authentication, digital watermark, vector quantization

1 Introduction

The appearance of PDF417 2D barcode significantly increases the barcode information hiding capacity [8]. Many important information can be stored into barcode without any extra storage media. The most obviously application is used on identification card. With PDF417 2D barcode, the personal data even photo on ID card can be encoded into a 2D barcode which is then printed on the back of ID card. Then, the identity authentication can be verified automatically by simply scanning the barcode. With the variety of applications, the request of 2D bar-code information hiding capacity becomes critical [7]. Unfortunately, 2D barcode has to be limited in its printed area on ID card. Moreover, ID card usually applies to a lot of key application such as financial transaction, medical transaction and border crossing [4, 10, 11]. So, it is often concerned the problems about counterfeited and prepensely tampered to cause danger of ID card owner. For this severity problem, some experts utilize high in-formation hiding capacity of 2D barcode to design a watermarking technique to make contributions for these problems.

Recently, there are researches dealing with water-mark technique for 2D barcode data authentication [1, 5], but the existent methods have to limit the size of embed-ded watermark. Furthermore, they also need to utilize original watermark or other auxiliary verification mechanism to achieve the barcode verification. In this paper, a blind watermarking technique of 2D barcode based on the concept of Association Rules (ARs) and Vector Quantization (VQ) is proposed. Of course, our method also meets the requirement of keeping the 2D barcode encoded material invariant after watermark em-bedding. Our method is not only capable to hide more complex watermark by utilizing less hiding capacity of 2D barcode, but also reaches the goal of barcode authentication. Our fragile watermark is capable to reflect the anomaly, if the 2D barcode data had been counterfeited or prepensely tampered.

The rest of this paper is organized as follows. Section 2 is Background, we shall briefly introduce the background concepts and techniques upon which the novel method is constructed. Then, in the Section 3, our new watermarking technique is presented in detail. In Section 4, the effectiveness and practicability of our method are demonstrated by experiment. Moreover, the performance comparison of our method and The method proposed by Afzel et. al. [1] is also conducted in this section. Finally, the conclusion is made at the end of this paper.

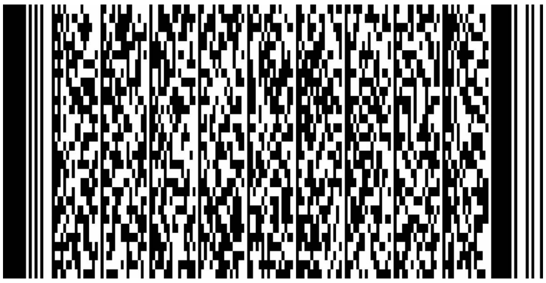


Figure 1: A PDF417 2D barcode structure

2 Background

2.1 PDF417 2D Barcode

PDF417 2D barcode was proposed by T. Pavlidis, et. al. in 1992 [9].and ability to restore the error data. It is applied to a lot of applications such as ID card, driver card and post card. Beside, it can also embed personal information into barcode such as name, phone and address to achieve the goal of copy prevention and assignment of data collection automatically.

In PDF417 [1], the data are consisted by a lot of codewords. Each codeword is consisted by four pairs of alternate bar and space. The width of each bar or space is unique after the codeword being encoded. The minimum width of a bar or a space is called a module, and each codeword is consisted by 17 modules. A PDF417 2D barcode is shown in Figure 1.

2.2 Association Rules

Association rules is a scheme for data mining used to find out useful information from large amount of data. Based upon the concept of association rules, the relations between data can be established, and the knowledge is then explored among the data. Generally speaking, association rules [2, 3] are defined upon a transaction database, where every product is called an item in the item database I. Each transaction consists of one or more items. Set of transactions is called a transaction database. Upon the transaction database, the association rule is defined as follows. Suppose X and Y are itemsets, where $X \subseteq I, Y \subseteq I, X \cap Y = \Phi$, and $|X| + |Y| = F$. Then, $X \rightarrow Y$ is called the association rule defined upon F-itemset.

Table 1 below is a simple example transaction database:

Table 1: A sample of transaction database

TID	Items
t1	a, e, f
t2	a, c, e, f
t3	b, d, e

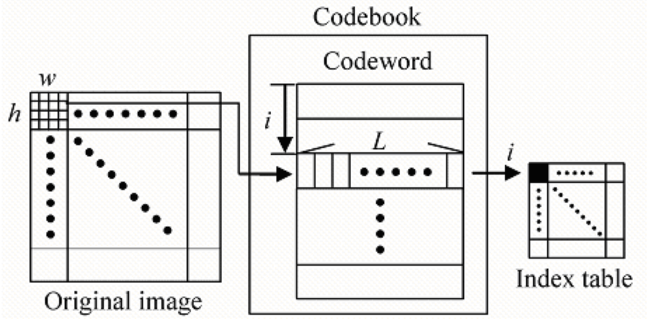


Figure 2: The concept diagram of vector quantization scheme

In the example transaction database in Table 1, the set {a, e, f} is taken as a 3-itemset that appears in both transactions t1 and t2. This association rule may reflect some kind of a trading habit, and that is one of the reasons why association rules are applied in the field of data mining.

2.3 Vector Quantization

Vector Quantization (VQ) was proposed by Gray [6] in 1984 usually applied on image compression. A codebook is built up at first, and the codebook is consisted with a lot of vectors (namely codewords). Then, the original image is cut into blocks with the same size, and all pixels of block are expressed as a vector. The most similar codeword is found out from codebook for each image block vector, and the vector is replaced by this code-word's index in codebook. The decompressing process is simply by replacing each encoded index with its corresponding codeword in codebook. Figure 2 shows the basic concept of VQ in image compression.

3 Proposed Method

To begin with, the notations we will use throughout this paper are defined as follows:

R_B: $\{r_B$: all association rules which are derived from original 2D barcode$\}$,

R_W: $\{r_W$: all association rules which are derived from watermark$\}$,

R'_B: $\{r'_B$: all association rules which are derived from the to-be-verified 2D barcode$\}$.

In this paper, 3-itemset association rules are defined on both the 2D barcode and the watermark. Embedding the watermark into 2D barcode via their ARs may save the embedding capacity of 2D barcode, and using VQ indices can easily to recall the watermark for the purpose of assisting personal data authentication. Four parts in below will introduce the key steps of our purposed method.

3.1 Codewords Preprocessing of the Codebook

Before the detailed steps of Algorithm Codebooking, Figure 3 illustrates the tasks in the codebook preprocessing,

Algorithm Codebooking:

Input: A random key K and a preassigned Codebook C_0 with $M \times N$ codewords (Each codeword has length L which is no smaller than $max\{\lceil lg(M)\rceil, \lceil lg(N)\rceil\}$. Note that the notation "lg" means "log_2".)

Output: Codebook C_1 (It is obtained by embedding a group number and an element number into each codeword of C_0.)

Step 1. Classify all the codewords into M groups such that each group contains N similar codewords. Let $S_M = \{0, 1, 2, \ldots, M-1\}$ and $S_N = \{0, 1, 2, \ldots, N-1\}$ be two integer sets.

Step 2. Assign the M integers in S_M to these M groups, such that each group has a distinct integer as its group number.

Step 3. For each group, every codeword is paired with a distinct integer in S_N by random key K' (initialized by K). Each integer in S_N bound to the codeword is called the codeword's element number.

Step 4. Generate a new key by the key used in Step 3. Let K' be the new key for the next group's codewords.

Step 5. Repeat Step3 and 4, until each codeword of all groups has a group number and an element number.

Step 6. Embed the group number and element number of each codeword into itself as the follows,

For each codeword's group number embedding:

- Translate the codeword's group number G into its binary bits $g_1 g_2 \ldots g\lceil lg(M)\rceil$.
- Select the first $\lceil lg(M)\rceil$ pixel values said $pi, i = 1, \ldots, \lceil lg(M)\rceil$ from the codeword.
- Replace the 2^{nd} LSB(Least Significant Bit) of p_i by bit g_i of G for $i = 1, \ldots, \lceil lg(M)\rceil$.

For each codeword's element number embed-ding:

- Translate the codeword's element number E into its binary bits $e_1 e_2 \ldots e\lceil lg(N)\rceil$.
- Select the first $\lceil lg(N)\rceil$ pixel values said $p_i, i = 1, \ldots, \lceil lg(N)\rceil$ from the codeword.
- Replace the 1^{st} LSB of p_i by bit e_i of E for $i = 1, \ldots, \lceil lg(N)\rceil$.

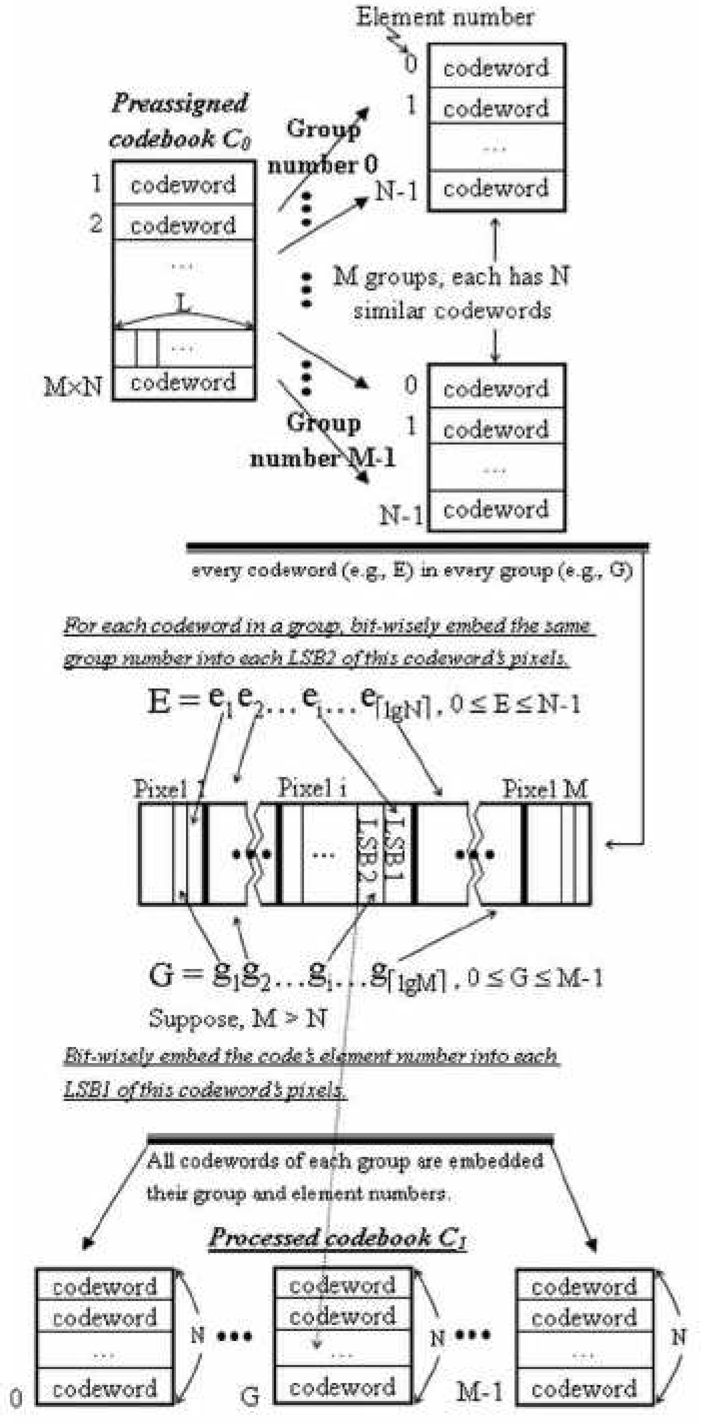

Element number
Preassigned codebook C_0
1 codeword
2 codeword
L
M×N codeword
Group number 0
0 codeword
1 codeword
N-1 codeword
M groups, each has N similar codewords
Group number M-1
0 codeword
1 codeword
N-1 codeword
every codeword (e.g., E) in every group (e.g., G)
For each codeword in a group, bit-wisely embed the same group number into each LSB2 of this codeword's pixels.
$E = e_1 e_2 \ldots e_i \ldots e_{\lceil lgN\rceil}, 0 \le E \le N-1$
Pixel 1
Pixel i
Pixel M
LSB1
LSB2
$G = g_1 g_2 \ldots g_i \ldots g_{\lceil lgM\rceil}, 0 \le G \le M-1$
Suppose, M > N
Bit-wisely embed the code's element number into each LSB1 of this codeword's pixels.
All codewords of each group are embedded their group and element numbers.
Processed codebook C_1
codeword
N
0
G
M-1

Figure 3: The tasks in algorithm codebooking

3.2 Define Association Rules of Image

In order to define the 3-itemset association rules on a 2D barcode and watermark images, the images are partitioned into blocks. Each 2D barcode image is first divided into blocks with $h \times w$ pixels in one block, where $h \times w$ should be no less than L. Each watermark image is divided into blocks with $m \times m$ pixels in one block, where $m \times m$ should equal to L. The association rule with three item values are defined on each image block. Let's define these three item values as follows:

Definition of 1^{st} item value: For each image's block, select the first $\lceil lg(M) \rceil$ pixel values said $p_i, i = 1, \ldots, \lceil lg(M) \rceil$ in row major order. Translate each p_i into its binary bits $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$. Let the decimal value of $(b1_7b2_7 \ldots b\lceil lg(M) \rceil_7$ be the the 1^{st} item value. (Note that it is obtained from all 2^{nd} LSBs).

Definition of 2^{nd} item value: For each image's block, the first L pixel values are selected in row major order to form an L components vector. From codebook C_1, find a codeword which is the most similar one to the vector. The element number of this codeword previously em-bedded by Algorithm Codebooking is now extracted for the 2^{nd} item value.

Definition of 3^{rd} item value: For each image's block, select the first $\lceil lg(N) \rceil$ pixel values said $p_i, i = 1, \ldots, \lceil lg(N) \rceil$ in row major order. Translate each p_i into its binary bits $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$. Let the decimal value of $(b1_8b2_8 \ldots b\lceil lg(N) \rceil_8)$ be the 3^{rd} item value. (Note that it is obtained from all 1^{st} LSBs).

The item values of an association rule have been clearly defined now. Each image block should generate an association rule, no matter what it is a 2D barcode image block (the pixel values of 2D barcode have to be binarized into 0 or 255 first.) or a watermark image block.

3.3 Watermark Embedding

Figure 4 shows the steps of our embedding algorithm:

The so-called associative watermarking is conducted by making association between rules in R_W and R_B. Therefore, the key K is applied again for randomly pairing together each rule in R_W with a rule in R_B. In other words, each r_W should get a certain r_B as its partner. For each (r_B, r_W) pair, Algorithm Rule Embedding is used to achieve the goal of establishing associations between r_B and r_W.

Algorithm Rule Embedding:

Input: Codebook C1, the original 2D barcode and watermark.

Each rule pair (r_B, r_W) - Suppose that r_B is de-fined by a block B in 2D barcode, and r_W is defined by a block W in watermark.

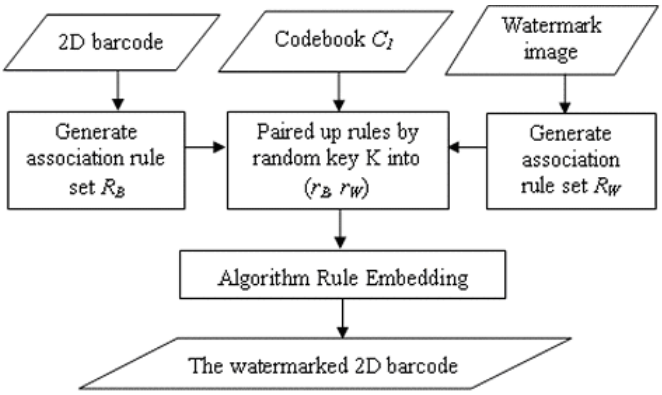

2D barcode
Codebook C_1
Watermark image
Generate association rule set R_B
Paired up rules by random key K into (r_B r_W)
Generate association rule set R_W
Algorithm Rule Embedding
The watermarked 2D barcode

Figure 4: Flowchart of associative watermark embedding procedure

Output: The watermarked 2D barcode.

Step 1. Check Block W's first L pixels in row major (which are the pixels used to generate r_W) to find its most similar codeword from Codebook C_1. Collect all codewords in the same group with this most similar codeword. From these codewords in the group, an arbitrary codeword c whose em-bedded element number equals to the 2^{nd} item value of r_B is selected. Let the selected codeword c be the representative of W. Regenerate r_W by codeword c.

/*Consequently, both of the 1^{st} and 2^{nd} items of r_W are the group number of c, and the 3^{rd} item is the element number of c.*/

Step 2. Pick up Block B's first $\lceil lg(N) \rceil$ pixel values said $p_i, i = 1, \ldots, \lceil lg(N) \rceil$ in row major order. Translate each pi into its binary bits $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$. Let $x_1x_2 \ldots x_{\lceil lg(N) \rceil}$ be the binary form of 3^{rd} item value of r_W. Replace $(b1_8b2_8 \ldots b\lceil lg(N) \rceil_8)$ by $(x_1x_2Kx_\lceil lg(N) \rceil)$ in sequence.

/*On the other word, each p_i's value should be changed from $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$ to $bi_1bi_2bi_3bi_4bi_5bi_6bi_7x_i$. Note that: after above two steps, both of the 2^{nd} and 3^{rd} item values of r_B equal to the element number of codeword c.*/

Step 3. Pick up Block B's first $\lceil lg(M) \rceil$ pixel values said $p_i, i = 1, \ldots, \lceil lg(M) \rceil$ in row major order. Translate each pi into its binary bits $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$. Let $x_1x_2 \ldots x_{\lceil lg(M) \rceil}$ be the binary form of 1^{st} item value of r_W. Replace $(b1_7b2_7 \ldots b\lceil lg(M) \rceil_7)$ by $(x_1x_2Kx_\lceil lg(M) \rceil)$ in sequence.

/*On the other word, each pi's value should be changed from $bi_1bi_2bi_3bi_4bi_5bi_6bi_7bi_8$ to $bi_1bi_2bi_3bi_4bi_5bi_6\ x_i\ bi_8$. Note that, after this step, the 1^{st} item value of r_B is changed to the group number of codeword c. All the modifications of r_B's item values are accomplished by changing pixel values of each 2D barcode block ac-cording to the definition of item values, thus the 2D barcode is said to be watermarked after process of this algorithm*/

After **Algorithm Rule Embedding**, the element number of the W's similar codeword c are now assigned to the 2^{nd} and 3^{rd} item values of r_B, and r_B's 1^{st} item value is now changed into the group number of c. Since r_B and r_W are associated by random pairing, thus the association can be traced from a watermarked 2D barcode's block said B by generating its association rule r_B, then r_B's 1^{st} item can be used to find the right codeword group. In this group, r_B's 2^{nd} item value denotes the element number of codeword c which can be selected to reconstruct block W for the embedded watermark. Moreover, by the r_B's 2^{nd} and 3^{rd} item values' equality which is made during rule embed-ding, this equality relation provides the sensitivity measure for checking any possible altering on the water-marked 2D barcode.

3.4 Watermark Extraction and Verification Method

Figure 5 shows the detailed process for tracing back the watermark:

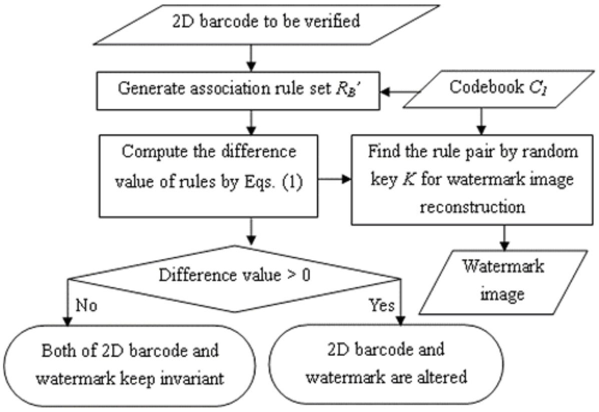
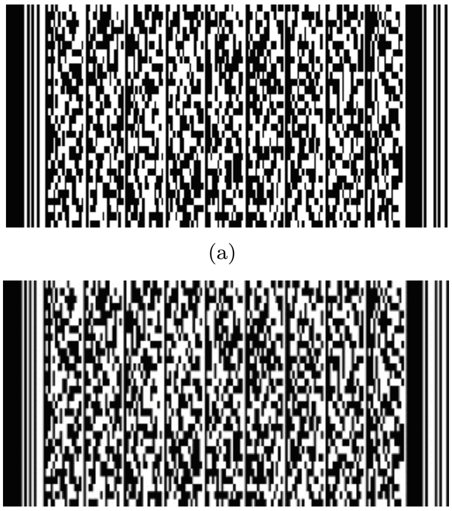

2D barcode to be verified
Generate association rule set R_B'
Codebook C_l
Compute the difference value of rules by Eqs. (1)
Find the rule pair by random key K for watermark image reconstruction
Watermark image
Difference value > 0
No
Yes
Both of 2D barcode and watermark keep invariant
2D barcode and watermark are altered

Figure 5: Flowchart of watermark extraction and verification

In our method, the first step of watermark recalling is the extraction process of the association rules set r_B' from the watermarked 2D barcode. According to Algorithm Rule Embedding, if the to-be-verified 2D bar-code is watermarked, the 1^{st} and 2^{nd} item values of any rule r_B' in the association rules set r_B' has been assigned as the group and element number of a codeword which is the representative of a watermark block which has rule r_W. Nevertheless, (r_B', r_W) is randomly paired by the key K such as the same way in pairing (r_B, r_W). Based on these associations, the watermark image can be properly reconstructed. However, if the extracted association rule r_B' is proven to be false, that is its 2^{nd} item value different from it's 3^{rd} item value. This case contradicts to the result of rule embedding, thus those pixel values of the relevant watermark image block were set by 0.


(a)

(b)

Figure 6: (a) 2D barcode image, (b) watermarked 2D barcode image

For the verification, the 2^{nd} item value and 3^{rd} item value of r_B' that has paired with r_W, are checked to see whether they are equal or not. If the answer is yes, the association rule is correct; otherwise it may have been counterfeited or tampered. In addition, a Difference Value is calculated by Equation (1). If the Difference Value is greater than 0, the 2D barcode may have been counterfeited or tampered, and the extracted watermark is altered. Otherwise, both the 2D barcode and the extracted watermark are correct.

$$\begin{aligned} &Difference\ Value \\ &= \sum r'_{B\_check}\ for\ each\ ruler'_B\ in\ R_B, \end{aligned} \qquad (1)$$

$$r'_{B\_check} = \begin{cases} 0, & \text{if } 2^{nd} \text{ item value for } r'_B = 3^{rd} \text{ item value of } r'_B \\ 1, & \text{if } 2^{nd} \text{ item value for } r'_B \neq 3^{rd} \text{ item value of } r'_B \end{cases}$$

4 Experimental Results

Afzel et al. [1] proposed the watermark embedding technique, which can reach the goal of using the extra information embedding capacity of 2D barcode to assist personal data authentication by embedding watermark into a 2D barcode. The experiment is conducted to prove that our method can also achieve the same goals but saving more capacity of a 2D barcode. On the other words, our method can embed a more complex watermark. The results will be figured and tabled in this section to demonstrate our points. The 2D barcode used in this experiment is a 900×1782 gray scale image shown in Figure 6(a). The watermark image used here is 480×360 gray scale ID picture shown in Figure 7(a). The parameters were set as follows: $L = 9, |C_0| = 256, M = 64, N = 4, m = 3, h = 3$

Table 2: PSNR values of extracted watermark images under various parameter setups

	$m = 2$	$m = 3$	$m = 4$
N = 4	-	31.62	29.59
N = 8	-	31.08	29.13
N = 16	31.04	29.49	28.06

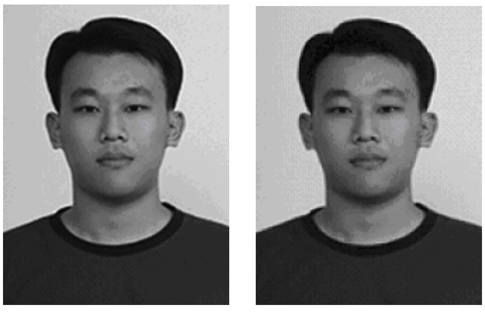

(a) (b)

Figure 7: (a) watermark image, (b) extracted watermark image ($PSNR = 31.62$)

and $w = 3$. Among the parameters, h and w have to do with the number of association rules obtained from the 2D bar-code image. The smaller h or w will get more association rules, and then more watermark association rules are embedded into the 2D barcode. The parameters h and w are set according to the size of watermark image to be embedded. As for m (relevant to the size of watermark blocks), it decides the number of rules that can be extracted from the watermark image. A greater m means a smaller number of association rules to be extracted, and a smaller m leads to a larger number of association rules to be extracted. However, if the m is too large, the quality of the watermark image can be severely distorted. The possible range of 2^{nd} item value and 3^{rd} item value of the association rule may be affected by N. A bigger N leads to a bigger possible range that will increase the complexity of the association rule. But, a too big N can also distort the image quality of the extracted watermark. Therefore, m and N were set according to the image quality of the extracted watermarks shown in Table 2. The watermarked 2D barcode image is shown in Figure 6(b). After the process of PDF417 Decoder, the encoded data could still be correctly extracted from the water-marked 2D barcode. Figure 7(b) shows the extracted watermark image. The PSNR (Peak Signal-to-Noise Ratio) value of the extracted watermark image was computed by using Equation (2) as follows:

$$MSE = \frac{1}{pq}\sum_{i=1}^{p}\sum_{j=1}^{q}((f(i,j) - \hat{f}(i,j))^2). \qquad (2)$$

In Equation (2), p and q stand for the height and width of the original watermark image, respectively, f stands for the pixel value of the original watermark image, and stands for the pixel value of the extracted watermark image. In this experiment, the tested 2D barcode image and watermark image for Afzel et al.'s Method are the same as our method.

As for the embedding capacity of the 2D barcode image, the ratios of the space occupied for our method and Afzel et al.'s method are listed in Table 3. In the same watermark image, our method obviously needs less space, and the capacity enhanced is increased threefold better than Afzel et al.'s method.

Table 3: The usage of 2D barcode information embedding capacity comparison, where the percentages of our method are derived by (number of association rules embedded / number of association rules embeddable), while those for Afzel et al.'s method are (number of pixels used / number of pixels available)

	$m = 2$	$m = 3$	$m = 4$
Our method	43200 / 178200 (24.24%)	19200 / 178200 (10.77%)	10800 / 178200 (6.1%)
Afzel et al.'s method	518400 / 855150 (60.62%)		

Table 4: Comparison results between our method and Afzel et al.'s method

Image process	**Our method**		**Afzel et al.'s method**
	Difference Value	Tamper?	Tamper? (compared with the original watermark image)
Attack-free	0	No	No
Blurring	12737	Yes	Yes
Sharpening	10531	Yes	Yes
Brightness (+1 pixel)	19061	Yes	Yes
Brightness (+20 pixel)	7906	Yes	No (Error)
Dark (-1 pixel)	19200	Yes	Yes
Dark (-20 pixel)	10299	Yes	Yes
Gaussion noise (1%)	15193	Yes	Yes
Rescaling	13982	Yes	Yes
Alter	58	Yes	Yes
Scan	14388	Yes	Yes

In the watermark image recalling and 2D barcode de-

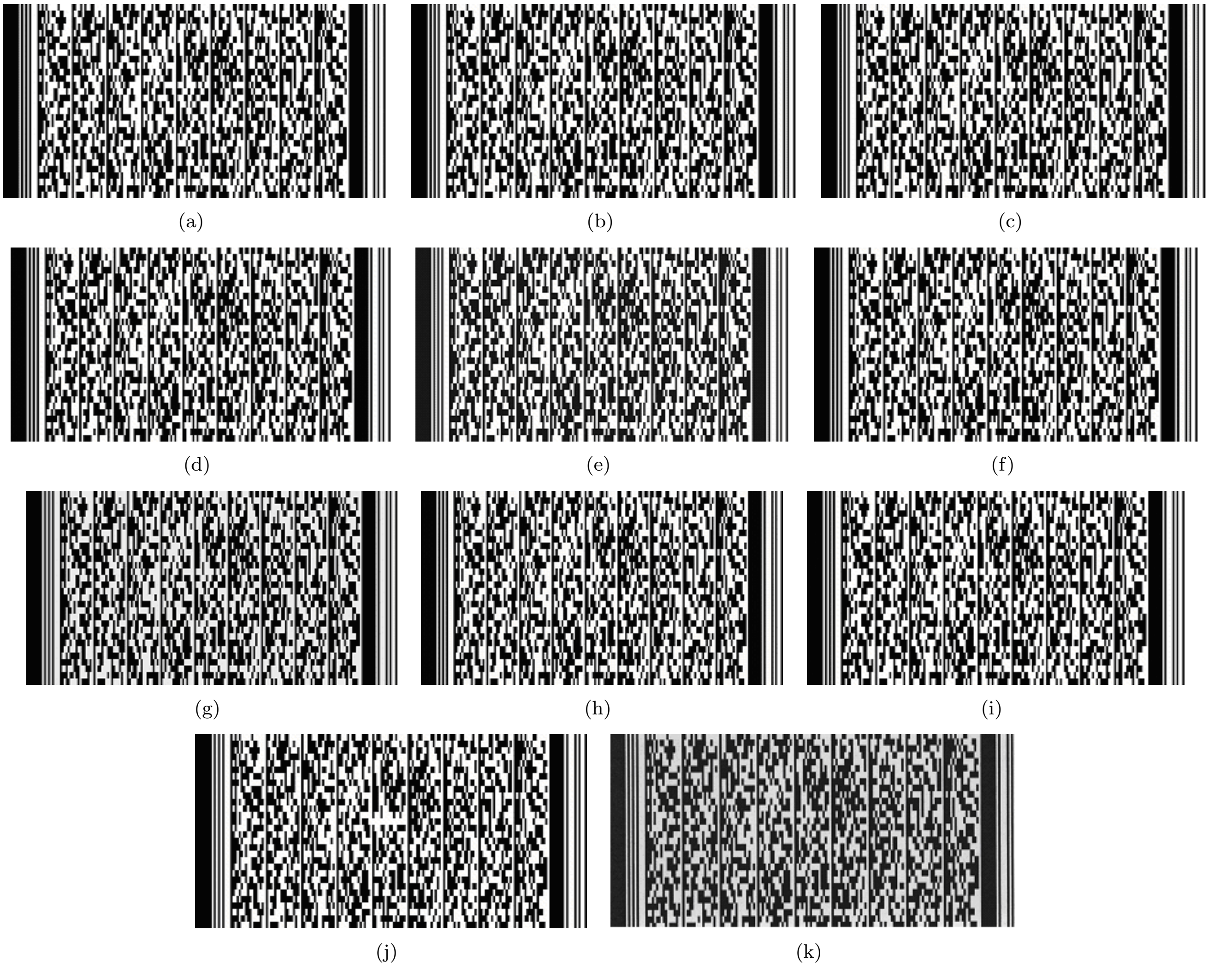

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k)

Figure 8: Wtermarked 2D barcode attacked by (a) attack-free, (b) blurring, (c) sharpening, (d) brightness (+1 pixel), (e) brightness (+20 pixel), (f) dark (-1 pixel), (g) dark (-20 pixel), (h) Gaussion noise (1%), (i) rescaling, (j) alter, (k) scan (600 dpi)

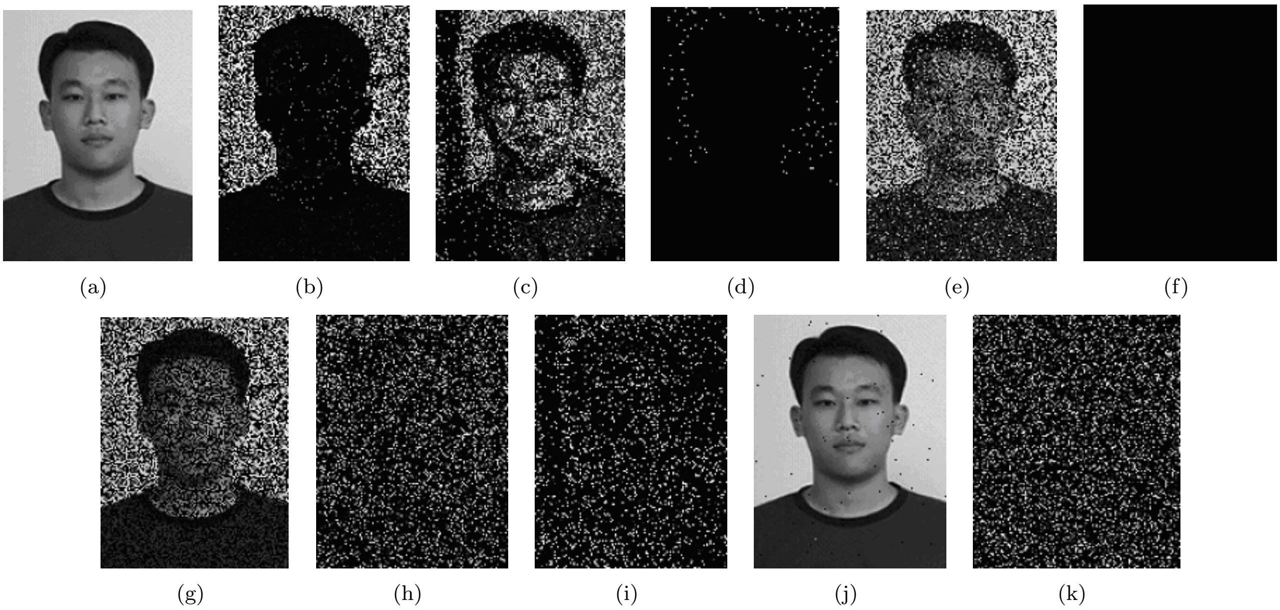


Figure 9: Extracted watermark images from attacked 2D barcode images (a) attack-free, (b) blurring, (c) sharpening, (d) brightness (+1 pixel), (e) brightness (+20 pixel), (f) dark (-1 pixel), (g) dark (-20 pixel), (h) Gaussion noise (1%), (i) rescaling, (j) alter, (k) scan (600 dpi)

tecting, PhotoShop 8.0 is applied, and the watermarked 2D barcode image is changed by doing "blurring," "sharpening," "brightening (+1 pixel)," "brightening (+20 pixels)," "darkening (-1 pixel)," "darkening (-20 pixels)," "Gaussion Noise (1%)," "rescaling (down sampling by 2 and up sampling by interpolation)," "alter," and "reproduced by scan (600dpi)." After the above image processing, the resultants of watermarked 2D barcode images are shown in Figures 8(b)-8(k). By using our watermark reconstruction method to extract the watermark images on the attacked 2D barcodes, these extracted watermarks are shown in Figures 9(a)-9(k). It shows that the proposed associative watermarking technique is sensitive enough to reflect any slightly changed on a watermarked 2D barcode. Finally, the results of comparison with Afzel et al.'s method are shown in Table 4. The correctness of the 2D barcode and the extracted watermark can be correctly determined by the computation of Difference Value even though they have been changed under image processing.

5 Conclusions

In this paper, we offer a new watermarking technique which is conducted by the concepts of association rules and the vector quantization. The main application field of our new technique is to assist 2D barcode in application of personal data authentication. Our method can reach the goal of embedding the watermark rules into the 2D barcode by establishing the relation between the association rules on both the 2D barcode image and the watermark image. Besides, the correctness of both the watermark image and the 2D barcode image can be verified by checking the association rules. One of our new technique's strong point is that can save the information em-bedding capacity of the 2D barcode. Moreover, the pro-posed associative watermarking can embed more complex watermarks in order to rise up the security level. Furthermore, our verification procedure does not utilize original watermark or other auxiliary verification mechanism, so it is a blind watermarking technique. The correctness of 2D barcode can be correctly determined by the Difference Value. Finally, the random key K ap-plied in rule's pairing and watermark embedding processes can be treated as a personal password.

References

[1] N. Afzel, T. Nikhil, and M. H. Max, "Embedding biometric identifiers in 2D barcodes for improved security," *Computers & Security*, pp. 679-686, 2004.

[2] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between sets of items in large databases," *Proceedings of ACM Special In-terest Group on Management of Data, ACM SIGMOD'93*, 1993.

[3] R. Agrawal, and R. Srikant, "Fast algorithms for mining association rules," *Proceedings of the 20th International Conference on Very Large Data Bases, VLDB'94*, 1994.

[4] S. Chow, N. Serinken, and S. Shlien, "Forgery and tamper-proof identity document," *Proceedings of IEEE International Carnahan Conference on Security Technology*, pp. 11-14, 1993.

[5] J. Dittmann, L. C. Ferri, and C. Vielhauer, "Holo-gram watermarks for document authentications," *IEEE International Conference on Information Technology: Coding and Computing*, pp. 60-64, 2001.

[6] R. M. Gray, "Vector quantization," *IEEE ASSP Magazine*, pp. 4-29, 1984.

[7] L. O'Gorman, and T. Pavlidis, "Auto ID technology: From barcodes to biometrics," *IEEE Robotics and Automation Magazine*, vol. 6, pp. 4-6, 1999.

[8] T. Pavlidis, "A new paper/computer interface: two-dimensional symbologies," in *IEEE International Conference on Pattern Recognition*, pp. 145-151, Barcelona, Spain, 2000.

[9] T. Pavlidis, J. Swartz, and Y. P. Wang, "Information encoding with two dimensional bar codes," *Computer*, vol. 25, no.6, pp. 18-28, 1992.

[10] D. Ross, "Back on the cards," *IEE Review*, vol. 49, pp. 22-23, 2003.

[11] A. W. Vaidya, "Keeping card data secure at low cost," *European Convention on Security and Detection*, pp. 212-215, May, 1995.

Jau-Ji Shen received the B. S. in Mathematics from Fu-Jen University, Taipei county, Taiwan, Republic of China, in 1982. Two years after, he received M.S. in information science program of Applied Mathematics from National Chung-Hsing University, Taichung, Taiwan. In 1988, he received Ph. D. in Information Engineering and Computer Science from National Taiwan University, Taipei, Taiwan. From 1988 to 1994, he was the leader of software group in Institute of Aeronautic, Chung-Sung Institute of Science and Technology, ROC. He is currently a professor of the Department of Management Information Systems, National Chung-Hsing University, Taiwan, ROC. His current research interests include digital images, data mining and database techniques.

Po-Wei Hsu received the B. S. in Department of Electrical Engineering from National Formosa University, Yunlin county, Taiwan, Republic of China, in 2004; the M. S. in Institute of Information Management from National Formosa University, in 2006. His research interests include cryptography, digital right management and software engineering.