Multimed Tools Appl (2016) 75:1223–1241
DOI 10.1007/s11042-014-2365-8

2D Barcodes for visual cryptography

Guangyu Wang · Feng Liu · Wei Qi Yan

Received: 4 March 2014 / Revised: 22 September 2014 / Accepted: 7 November 2014 /
Published online: 29 November 2014

Abstract The basic idea of Visual Cryptography (VC) is to divide a secret image into several partitions which are called VC *shares*. With various categories of VC schemes having been developed to enhance the maturity of VC since its emergence, one of obsessions in current investigations of VC is that each VC share lacks authentication. In this paper, we analyze VC authentication methods using 2D barcodes and embed binary codes into VC shares for authentication purpose. The objective of this paper is to present a method of improving the authentication of traditional VC scheme. Our contribution of this paper is to propose a scheme of embedding 2D barcodes into given VC shares to prevent cheating, we search the best region of a given share where the 2D barcode could be embedded into so as to keep the visual quality of the revealed secret.

Keywords 2D barcode · Visual cryptography · Authentication

1 Introduction

Visual Cryptography (VC) was pioneered by Naor and Shamir in 1994 [30] and it is an effective technique that involves the functions of secret sharing [45]. As equipped with the features of perfect secrecy and easy decryption ways, VC has been treated as a desirable scheme [47]. In VC (http://en.wikipedia.org/wiki/Visual_cryptography), an image is split into several sub-pictures which are commonly generated by using pixels of the original image. The aim of VC research is to provide efficient approaches for image secret sharing [29, 50]. In a secret sharing scheme, there should have a role called *dealer* who clearly knows the content of

G. Wang · W. Q. Yan
School of Computer and Mathematical Sciences, Auckland University of Technology, No. 2-14 Wakefield Street, CBD Auckland 1010, New Zealand

G. Wang
e-mail: qrf3710@aut.ac.nz

F. Liu · W. Q. Yan (✉)
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Room 3217, No. B2 Research Building, No. 89A Minzhuang Road, Haidian District, Beijing, China 100093
e-mail: wyan@aut.ac.nz

F. Liu
e-mail: liufeng@iie.ac.cn

secret while the participants only have the knowledge of their own share. When these shares are superimposed, the secret is able to be obtained directly by Human Visual System (HVS) [24]. It is required that the secret should not be generated correctly if fake shares are used or lack of needed shares for secret revealing, only the authorized shares can be taken for revealing the secret by overlapping the shares. As in VC the original secret is divided into several shares which are parts of the key for revealing the secret image, one of the important VC applications is in security and privacy protection.

Traditionally, basic VC is achieved by image sharing which is a scheme that is similar to that of general secret sharing. Typically, in (*k, n*) scheme, the image that carries the secret is encoded into *n* shares and the decryption process cannot be successful unless at least *k* pieces are collected and superimposed [14]. Specifically, the use of these basic schemes would provide a secure form of 2D barcodes which are employed as a secret carrying mechanism [45]. We take use of pixel value of '1' and '0' representing black and white pixels respectively. The construction of VC shares is noted by a two out of two visual cryptography scheme known as (2, 2)-VCS. The construction of white (C_D) and black (C_1) pixels of VC shares is indicated as below where each pixel from the original image is expanded into four pixels [45].

$$C_D = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,1\,0\,0 \\ 1\,1\,0\,0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,1\,0\,0 \\ 0\,0\,1\,1 \end{bmatrix} \right\}$$

In basic VC scheme, shares are generated by the following rules: pick the pattern of four sub-pixels with the same arrangement for both shares if the pixel of secret image is white; or else if the pixel of the image is black, pick a complementary pair of patterns. An example of overlapped VC shares is shown in Fig. 1 to reveal the visual secret 'Visual Cryptography'.

Another traditional VC is extended VC scheme that allows the construction of visual secret sharing schemes within which the image content of the shares is meaningful [10, 37]. The collections $C_C^{C_1\ C_2}$, where $c, C_1, C_2 \varepsilon \{b, w\}$ of a 2 out of 2 threshold VC scheme (2,2-VCS) are gained by using the following matrices [1].

$$\begin{aligned} S_w^{ww} &= \begin{bmatrix} 1\,0\,0\,1 \\ 1\,0\,1\,0 \end{bmatrix} \text{ and } S_b^{ww} = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{bmatrix} \\ S_w^{bw} &= \begin{bmatrix} 1\,0\,0\,1 \\ 1\,0\,1\,1 \end{bmatrix} \text{ and } S_b^{ww} = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,1 \end{bmatrix} \\ S_w^{bw} &= \begin{bmatrix} 1\,0\,1\,1 \\ 1\,0\,1\,0 \end{bmatrix} \text{ and } S_b^{bw} = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,0 \end{bmatrix} \\ S_w^{bw} &= \begin{bmatrix} 1\,0\,1\,1 \\ 1\,0\,1\,1 \end{bmatrix} \text{ and } S_b^{bb} = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{bmatrix} \end{aligned} \tag{1}$$

Halftone technique has been applied to grayscale and color images in which a continuous tone is simulated by black dots in various ways [2, 43, 52]. The advantage of using halftone

Fig. 1 A visual example of VC

technique is to spread gray-level depth of one pixel into a block of black dots, which increases the random distribution of those dots so as to implement the VCS. Moreover, employing halftone technique in VC has been well investigated [19, 26, 27, 42, 43]. One scheme of using halftone technique can also assert in greatly improving the quality of shares by using contrast enhancement techniques [28].

In color VC scheme [31], one pixel is transformed into sub-pixels, each of which is also subdivided into color domain. Moreover, multiple secrets sharing in VC has the advantage of being able to hide more than one secret within a set of shares compared to that of single secret [3, 21, 47]. Compared to traditional VC which is use of rectangular shapes on shares, a multiple secrets sharing has been developed by using circular ones that tend to add extra information such as supplementary points, lines or markers [34].

One of authentication methods of VC is to seek the support from 2D barcodes. There are four main benefits of using 2D barcodes in authentication [46]. First, different from using another share for authentication, 2D barcodes are embedded into VC shares, therefore could simplify the authentication process. In addition, cheaters are very hard to get information of the barcodes from secret prediction. Moreover, since the barcodes are able to present long character string using a small size of pattern with black dots, it is able to be applied as a tool to carry the secret. Furthermore, barcodes have the advantage of encoding a large scale of authentication information into a controllable set of shares. Lastly, as a vast majority of applications on mobile devices and personal computers have been developed for scanning barcode, it is convenient for a user to decode the barcodes by directly using the built-in cameras with a cellphone or laptop.

Barcodes are very resilient to errors and changes in an acceptable extent. The threshold of visual angle for scanning a barcode is being increased with the rising resolution of a camera. This strengthens the robustness of barcode utilization when using cameras and software applications developed for cellphones. Especially in the case of embedding 2D barcodes into VC shares which requires high security and recognition ability, information verification needs to be fast and accurate in the process of authentication. As resolution of 2D barcodes could be adaptive to that of the VC shares, the scanning process therefore primarily relies on the information carried by those shares. Using VC shares embedded with 2D barcodes, the process is becoming easy for a dealer to check the correctness of VC authentication. Our contribution of this paper is to authenticate the VC shares using a 2D barcode by embedding it into the similar regions of the VC share, the embedding could not affect the VC secret revealing too much.

In this paper, we will introduce the related work in Section 2, describe the mechanism of 2D barcodes in Section 3. A scheme will be proposed to make an improvement for VC authentication in Section 4. Finally, the experimental analysis and conclusion will be presented in Section 5 and Section 6, respectively.

2 Related work

Even though VC can significantly support secret protection, participants who hold shares could not identify the authenticity of all shares and the secret, given cheaters the opportunity to create unauthorized shares which simulate the valid shares to obtain the hidden secret. Thus cheating prevention approaches are needed in association with VC to block devious practices. Nowadays, various cheating methods have been developed and each of the methods is capable of coaxing VC users. In VC, participants and outsiders are all able to provide counterfeit shares so as to deceive others in various circumstances. Collusive participants are also able to trick

others by showing the fake overlaying results of their shares to other participants (victims). The forged shares from outsiders can be generated by encrypting fake secret into shares with different scales and pixel deployment methods [15]. Chen et al. also developed a cheating preventing method that deals with the cheating immune problem [5]. Practical applications are also developed for VC authentication as shown in [6, 12, 13, 20, 22, 23, 39, 44].

The existing schemes of VC authentication can be classified into two categories. The first is to employ an additional share to check authenticity of the revealed secret [4, 46]. This authentication method enables verification of the shares before the process of secret revealing. The other available authentication method is in use of a blind authentication technique which aims at preventing the prediction of genuine shares. However, as inconvenience of producing additional shares may have, the first type of authentication is hard to be implemented while the second one is always adopted.

A scheme of embedding a 2D barcode into VC shares has been presented in [46]. The selection of VC schemes was recommended to choose XOR or OR operation. Subsequently, two shares were generated for embedding barcodes. The secret image was then decrypted by overlapping the shares. By embedded the 2D barcode into the secret image, the superimposed image was used for VC authentication by verifying the 2D barcode of the secret.

Dissimilar to the basic VC, in the extended VC scheme [46], more authentication processes were developed due to its nature of using meaningful pictures such as 2D barcodes. By applying the extended scheme of secret sharing, two shares were generated which have two selected barcodes visually on the entire shares. The original secret was revealed after superimposed the two VC shares. Authentication process exists in both methods, namely before and after the secret revealing in the extended VC.

Apart from selecting embedding scheme, choosing barcodes is also crucial in authentication of VC shares since a suitable barcode not only decreases the observational difficulties of the secret, but also provides much sufficient and necessary information for VC authentication. The previous approach for using 2D barcode in VC authentication is to embed the barcode into the four corners of VC shares. In this paper, we aim at seeking the best region where the barcode is appropriate for being embedded. The enhancement of utilizing a 2D barcode in VC authentication is emphasized in this paper. Our contribution is to present a new scheme and extend the current existing approach of using 2D barcode in VC authentication.

3 2D barcodes

A barcode is defined as an optical machine-comprehensible representation of certain data, text or other information which has been attached [18]. There are only black printable dots shown in a barcode, hereinafter it is easy to be detected by scanners but hard to be recognized by Human Visual System (HVS) due to its encoding design. Conventionally, the data is stored in one-dimensional barcodes by utilizing parallel lines whose lengths and intervals are varying. With the development of barcode technologies, the adoption of regular 2D patterns, for example, rectangles, dots and hexagons, has now been designed in the construction of 2D barcodes. There exist contributions applied barcodes to VC authentication, the PDF417 barcode has been employed as an original secret which was divided into two VC shares using VCS earlier [49].

Barcodes could be classified into two main types, namely linear barcodes (stacked barcode, one-dimensional barcode) and 2D barcodes (dot matrix barcode). Three examples of 2D barcodes are shown in Fig. 2.

Within the VC, using 2D barcodes has more advantages than that of other types in authentication. First, 2D barcodes can be applied to VC which tackles binary images that

Fig. 2 Examples of various barcode types (each of these barcodes has the same content: AUT)

colors except black and white will not be taken into consideration. Even if binary attributes of 1D barcode can precisely represent the information based on specific protocols, the usages of 1D barcode are still restricted as its limited capacity of information to store. Therefore 2D barcodes, which have advantages such as large capacity with small size, ease to be carried, robustness as well as high security, etc. are more suitable to be applied to VC authentication than 1D barcodes [9, 48]. Ordinarily in VC, participants expect the authentication information to be complicated enough for protecting the shares from being attacked by cheaters. Simultaneously, size of the authentication container is expected as small as that of a share within a controllable scale. Furthermore, VC shares are all depicted in 2D form which is similar to 2D barcodes. Therefore 2D barcodes have the superior advantage of being applied to VC shares for authentication.

According to different encoding designs, 2D barcodes [48] also are grouped into stacked barcodes and dot matrix barcodes. Stacked barcodes present information by incorporating with height adapted 1D barcode. Typical stacked barcodes include Code l6K and PDF417 [11]. Aftermaths, a stacked barcode is not suitable for being embedded into VC shares as it has the similar attributes of 1D barcode. On the other hand, dot matrix barcodes are only organized by an array of printable dots in a regular flat place in order to conveniently deal with the information encoding, the recent developed coding schemes were based upon digital image processing, typical formats of dot matrix 2D barcodes include Aztec Code, Quick Response Code (QR Code), Data Matrix and Maxi Code. Amongst these barcodes, Data Matrix and QR Code are broadly used and supported by the scanner software installed in either personal computers or mobile devices.

A Data Matrix encapsulates three components, namely encoded data, four borders, and quite zone [16]. Each of these components contains black solid squares which is called module. With being translated into mathematical expression, a black module in the barcode represents ‘1’ and a white module is symbolized as ‘0’, or vice versa. To locate the symbols, a Data Matrix Code contains an ‘L’ shape module to define its orientation, boarder and size. All the symbols are bordered by white modules marked as the quite zone. A Data Matrix symbol [17] uses Reed-Solomon Error Correcting Code (ECC) level 200 for error detection and correction.

In QR Code, the encoded message is stored in both horizontal and vertical directions [8, 33, 51]. The modules only represent dark or white elements by a digit 0 or 1. QR Code performs better in data capacity, size scale and scanning speed than that of Aztec Code and Data Matrix. In this paper, our goal of employing 2D barcodes is for authentication purpose since it is possible that an appropriate 2D barcode could find the most similar region from the given VC shares that minimizes visual differences in secret revealing. Therefore, on the basis of similar usability, 2D barcodes, like QR Code, Aztec Code and Data Matrix all could be taken into consideration for authentication purpose in VC. In this paper, we select the 2D barcodes, i.e. QR Code, Data Matrix, and Aztec Code for the authentication of VC shares.

4 Proposed scheme

4.1 Solutions for VC authentication

A 2D barcode has the advantage of only comprising of printable dots and provides security information for authentication, it is therefore reasonable to combine the VC shares and 2D barcodes together for VC authentication, as in traditional VC, the shares are also organized by arrays of only black and white dots.

Even though directly embedding 2D barcodes into the corners of VC shares possibly avoids any visual side-effect of secret revealing when these shares are superimposed. In some cases when VC secret is stored around corners of the VC shares, replacing the corner of shares using 2D barcodes will be harmful for the secret revealing. Much more severely, some useful information at the corners will be substituted by the 2D barcodes. As a result, it appears to be significant to develop other methods which can achieve both goals of authentication and revealing the entire secret.

There are commonly two approaches available to embed a 2D barcode into VC shares. First, searching for the regions which are not occupied by the secret data in the original picture, replacing these regions with 2D barcodes can be an ideal way to preserve the full data of secret and embed 2D barcodes for authentication. However, to achieve this approach which is to discriminate the meaningful regions from other regions of one image is still far from mature, cheaters can probably predict the regions having meaningful information which tends to facilitate their attack process. Furthermore, when the VC share is full of secret information, there will have not available space for barcode embedding.

The other effective method is to find a proper 2D barcode so as to replace certain regions of the VC shares which are similar. This approach is feasible to be applied in practice as the image matching for finding similar regions of 2D barcodes can be easily implemented. Moreover, because of similarity between the 2D barcode and the found regions, the secret can still be revealed somehow even if using the shares embedded with 2D barcodes. The 2D barcodes are required to be similar to the replaced regions in an extent in order to make the superimposed VC shares present the secret, therefore the 2D barcodes and embedded regions of VC shares both dramatically affect the result of secret revealing.

4.2 Embedding 2D barcodes in the basic VC

In order to compare the method of directly embedding a 2D barcode into the corners of shares and that of replacing similar regions of shares using the 2D barcode, we propose an algorithm and conduct experiments to verify the improvements in this paper. Figure 3(a) illustrates the proposed process for embedding a 2D barcode into VC shares, Fig. 3(b) presents an example which is used to explain how the VC region is replaced by the barcode.

In the Fig. 3(a), an image with secret is firstly divided into two VC shares *Share*1 and *Share*2. Then a 2D barcode with the predefined content is constructed. The resolutions of 2D barcode and *Share*2 are adapted before similarity matching so as to find the most suitable regions on *Share*2 that could be replaced by the 2D barcode. The new *Share*2 will be reconstructed after replaced the similar regions with the barcode. Assisted by the new *Share*2, the secret image is then used to produce new *Share*1 by applying VC scheme again. Lastly, the new *Share*2 and newly generated *Share*1 are overlapped to reveal the original secret.

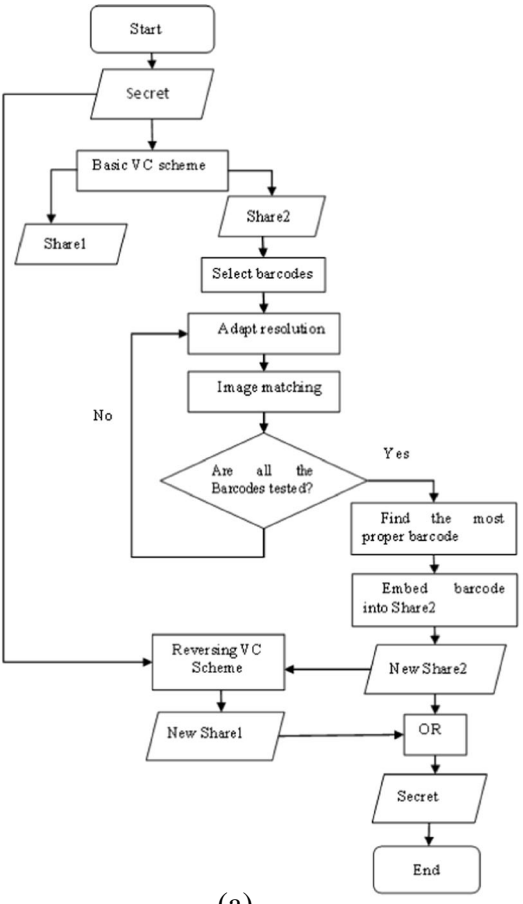


Fig. 3 Replacing the similar regions. (**a**) Flowchart of searching the similar regions on a share. (**b**) Replacing a region using a pixel array of the barcode

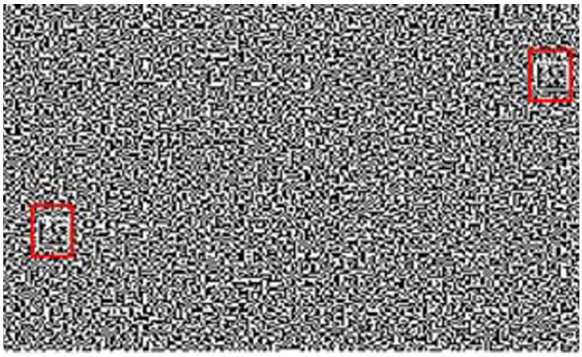
4.3 Resolution adaption

The resolution of a 2D barcode needs to be adjusted so as to match that of the target share for embedding 2D barcode. Specifically, there are three reasons for the necessity of this step. From the view of secret sharing, the employment of 2D barcodes is crucial for authentication of VC

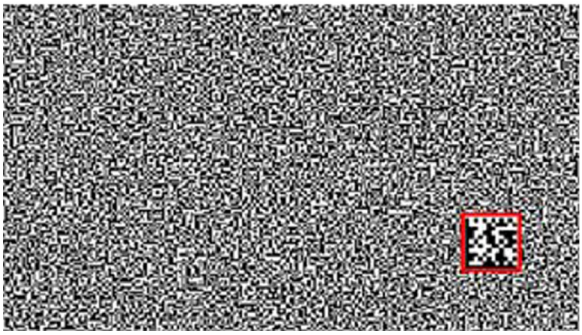
shares. Thus we have to minimize the visual side-effect of 2D barcode on the shares at an acceptable level that the barcodes could be read by a scanner. What is more, the necessity for tackling resolution adaption is to ensure the similarity between a 2D barcode and its similar regions on a share.

If the dots of 2D barcodes are bigger than those of the VC share in size, it will be more difficult to find the regions of the VC share which are similar to the barcode. Besides, a problem lies in visual side-effect of secret revealing due to different sizes of those dots. Figure 4 shows an example of embedding 2D barcodes with different dot size into one VC share.

Algorithm 1: Image adaption
Input: 2D barcode B
Output: Adapted 2D barcode B'
Procedure:
Begin:
```
Set Iw=the width of the barcode B
Set Il=the height of B
Set IW=the width of the VC share D
Set IL=the height of D
Set s=1000 //initialization
```



(a) Embedding barcode (shown in red rectangles) whose resolution is 21×21



(b) Embedding barcode (shown in the red rectangle) whose resolution is 42×42

Fig. 4 The comparison of embedding different sizes of barcodes into a VC share. (**a**) Embedding barcode (shown in red rectangles) whose resolution is 21×21. (**b**) Embedding barcode (shown in the red rectangle) whose resolution is 42×42

```
p=1;
For all height of B (j=1, …, Il)
For all width of B (i=1, …, Iw-1)
       If B (i, j) equals B (i+1, j) then
          p=p +1;
       else if s>p, s=p; p=1;
       end if;
end For;
end For;
For all width of B (i=1, …, Iw)
For all height of B (j=1, …, Il-1)
       If B (i, j) equals B (i, j+1) then
          p=p +1;
       else if s>p, s=p; p=1;
       end if;
end For;
end For;
C=s;
B'=resize B by shrinking its width and height to
     Il/C and Iw/C, respectively;
End.
```

In this paper, we assume the dot size of a VC share is uniform, typically is the size of one pixel, we take the dot size of a 2D barcode into consideration and resize it to match that of the given VC share, our algorithm 1 is provided for this adaption. The dot size of a 2D barcode could be obtained by scanning the 2D image in both horizontal and vertical directions. If a 2D barcode has all dots size with that of S^2 pixels, the dots will be replaced by pixels uniformly.

4.4 Image matching and replacement

After adjusted dot size of the 2D barcode and that of the target VC share, it appears to be crucial to search for the similar regions on the share. Typically, an image can be treated as an array of pixels with various intensities. In both the VC share and the 2D barcode, pixels are clearly distinguished by black and white, thereafter this greatly facilitates the matching process.

In the case of VC, as there are only black and white pixels in the shares, the number of black and white colors will not be as diverse as that of various colors, thereby are less persuasive to determine the similarity of certain locations. As for the similarity measures of two images, a way of comparing two images by using the discrete metric is considered as the distance of a pair of pixels [38].

$$\delta(A, B) = \begin{cases} 0 & \textit{if pixel } A \textit{ matches pixel } B \\ 1 & \textit{otherwise} \end{cases} \tag{2}$$

As the resolution of a barcode is usually uncertain before the embedding process starts, it is not easy to choose which matching method should be employed. For an example, the standard specification of the QR code resolution varies from 21×21 to 172×172. Moreover, as a VC share has not meaningful features to be extracted for analysis, this method is considered to be improper for VC. Searching every pixel of a 2D barcode and that of a VC share appears needing a long time when the resolutions

are high, the searching workload will be much less when applied it to small pictures or blocks. More importantly, the accuracy of matching the barcode with a region of the VC share is another reason that should be taken into consideration. Therefore, the embedding procedure is to calculate the similarity distance between all pairs of corresponding regions on the share and the 2D barcode.

Algorithm 2: Image matching and replacement
Input: a VC share *D* and a 2D barcode *B*
Output: New share with 2D barcode *D′*
Procedure:

```
Begin:
    Set Iw=the width of barcode B
    Set Il=the height of B
    Set IW=the width of VC share D
    Set IL=the height of D
    Set s=0; //number of the similar pixels
    Set p=0; //number of the pixels in the region
             which is the most similar to barcode B
    For a=1,…, (IW-Iw+1)
        For b=1,…, (IL-Il+1)
            For i=a,…, (a+Iw-1)
                Set s =0;
                For j=b,…, (b+Il-1)
                    If D (i,j) equals B (i-a+1, j-b+1),
                        s=s+1;
                    end if;
                end For;
            end For;
            If s>p,
               p=s;
            end If;
        end For;
    end For;
    D′=D; //initialize the new share D′
    For a=1, …,(IW-Iw+1)
        For b=1, …, (IL-Il+1)
            For i=a, …, (a+Iw-1)
                Set s=0;
                For j=b, …, (b+Il-1)
                    If D (i,j) equals B (i-a+1, j-b+1),
                        s=s+1;
                    end If;
                end for;
            end for;
            If s equals p,
                For i=1,…, Iw
                    For j=1 to Il
                        D′(a+i-1, b+j-1)=B (i, j);
                    End For;
                end For;
```

```
            end If
        end for;
    end for;
End
```

In the matching, the 2D barcode as an image is compared to each same size region of a VC share one by one so as to calculate the similarity distances by using eq. (2). The pixel distance is 0 if these two compared pixels are same, meanwhile the region distance between the region of VC share and 2D barcode is calculated by simply summing up all the different pixels of two regions together. The most matching region is the region with the least distance.

4.5 Barcode selection

Since different 2D barcodes have different coding designs, it is important to choose the most suitable one for replacing regions of the share with the least side-effect on the revealed visual secret. Moreover, since different messages can be stored into these barcodes, these result in the various shapes, selecting proper type of 2D barcodes carrying an appropriate character string turns up to be an important step in embedding a 2D barcode into a basic VC share.

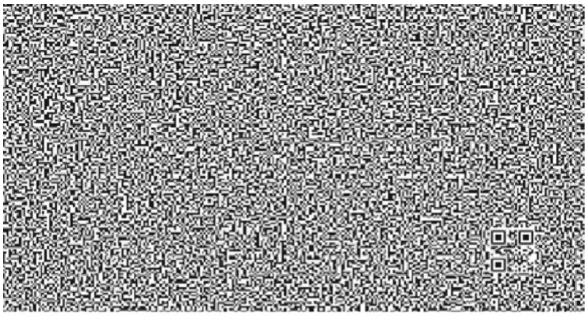
Nowadays, the source of free barcodes generating and downloading is easily to be obtained from public websites. It is not difficult to generate a 2D barcode at all. As a result, an optimized approach of selecting proper barcodes for a share is to find out the most suitable one. However, as it will cost a great deal of time to find out the best one from the given candidates so as to be treated as the embedded barcode.

From our observations, a little change of a barcode will lead to different matching results. Consequently it is important to keep the barcode in the share that can be identified clearly and accurately. Besides, different types of 2D barcodes have obviously distinct shapes due to their encoding design. Thus the candidate barcodes are assumed to be different in both types and contents. Even though it is obvious that using Data Matrix has less side-effect on the revealed secret than using QR Code and Aztec Code shown in Fig. 5, the revealed secrets of using QR Code and Aztec Code respectively are acceptable since the superimposed regions embedded barcodes are visible to the secret. The results of using these three types of 2D barcodes to replace the regions of a VC share are compared in Table 1. Table 1 shows rates of matched pixel number (numerator) to total pixel number of the three types of barcodes (denominator). Apparently the performance of Data Matrix is superior to others in the most similar region searching.

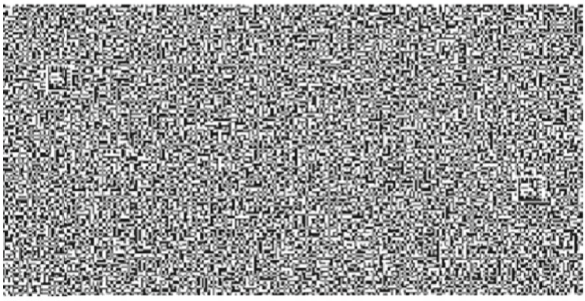
4.6 Secret revealing

Even though the authentication problem of VC could be solved by embedding a 2D barcode into its most similar regions of a VC share, the visual side-effect of the revealed secret still exist. Furthermore, the revealed secret using the new VC share will also be affected. Therefore, it appears crucially to make a change to the other VC share in order to reduce the visual side-effect in secret revealing.

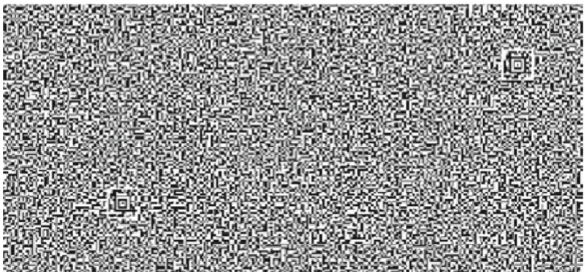
In the final step of the 2D barcode embedding, we have the VC share embedded with 2D barcode (*Share*1) and the secret at our hand, then the new *Share*2 are generated by simply conducting basic VC scheme again using the new *Share*1 and the secret image as shown in Fig. 3(a). Consequently we obtain the new *Share*2. We call this as Reversing VC Scheme. The superimposed result namely revealed secret then is not affected by the embedded 2D barcode anymore.



(a) Secret revealing using QR code (Barcode content: AUT)



(b) Secret revealing using Data matrix (Barcode content: AUT)



(c) Secret revealing using Aztec code (Barcode content: AUT)

Fig. 5 Revealing results with different barcodes. (**a**) Secret revealing using QR code (Barcode content: AUT). (**b**) Secret revealing using Data matrix (Barcode content: AUT). (**c**) Secret revealing using Aztec code (Barcode content: AUT)

5 Experiments and analysis

5.1 Dataset

In order to test the proposed scheme of embedding 2D barcode into VC shares, a dataset of test images has been built up for evaluation purpose. The source of the dataset was collected from the fields like TV test card, Fax test card, digital image compression, watermarking and so on. Figure 6 shows the selected images in the dataset embedded with 2D barcodes according to different categories. A full dataset could be found from [41]. We use the IBM logo to show that all logos as binary images could be used in 2D Barcode based VC authentication, different geometric patterns could tell us how good the VC authentication performs in sharing these types of visual information. The pictures for eyesight test and visual chart show us how the

Table 1 Comparison of similarities amongst three types of 2D barcodes

Samples	QR	Data matrix	Aztec
Sample 1	19/400	22/144	5/400
Sample 2	15/400	13/144	7/400
Sample 3	14/400	14/144	6/400

visual text information could be shared and authenticated by 2D Barcode. The image 'Girl and mom' could show how shapes of human faces could be shared by using VC.

5.2 Experiments

After formation of the dataset, subsequently relevant experiments need to be set up for testing. We collected 10 samples of binary images and split them into shares by using the basic VC scheme.

Comparison of the similarities between the original secret and the secret obtained by stacking new shares is shown in Table 2. There are three findings from the experiments. First, the larger secret image is, the smaller the disparity between the revealed secret and original secret will be. Furthermore, the similarity distance between the original share and the new share is less than that of randomly embedding 2D barcode into these shares. Most importantly, the visual effect of embedding 2D barcodes into VC shares is acceptable.

In the context of embedding 2D barcode into VC shares, messages carrying by 2D barcodes are texts, namely, words, sentences and paragraphs which contain significant authentication messages. Another popular kind of 2D barcode is the URL of a website. Even though the script of web link itself has not meaningful information, the authentication texts can be easily retrieved on the website.

Furthermore, because all the kinds of 2D barcodes mentioned can be decoded and modified by cheaters without being noticed by VC shares holders, methods of one way encryption in which the content is a cipher text that cannot be decoded are needed. Cryptographic Hash function has the premium merits of easily to calculate the Hash values for any input data which are hard to get data from a given Hash, difficult to modify a data without altering the Hash and tough to find two different data generated by the same Hash function, etc. Besides, as cryptographic Hash Functions are used in a large range of areas like Message Authentication, Message Integrity, Digital Signatures, Entity Authentication and Digital Steganography [35], we decide to use a Hash function to encode a 2D barcode.

A Hash function is the algorithm that maps data of arbitrary length to data of a fixed one [32]. The values returned by a Hash function are called Hash values or Hash codes. The definition of Hash function [32] can be a function h: D -> R, where the domain D=R for some n ≥1. Well-known Hash functions include MD4, MD5, SHA-1 and SHA-2. The Hash function MD4 is defined as the iteration of a three rounds compression function [7]. The 128 bits (16 bytes) MD4 Hashes are typically represented as 32 digits hexadecimal numbers. As an updated version of MD4, MD5 is a block related digest algorithm which is computed over the data in phases of 512 bytes blocks organized as 32 bits words. The first block is dealt with an initial seed, resulting in a digest that is used as the seed for the next block. When the last block is calculated, its digest is for the entire computation [40]. In this paper we will use MD5 for encoding 2D barcodes after taking our situation into full consideration.

Another issue in authorization of VC shares is how to use a 2D barcode to differentiate the correct share from the unauthorized ones. As for the case of VC share, its recognizable features are size and pixel characteristics. The advantage of using the Hash code of these features is that

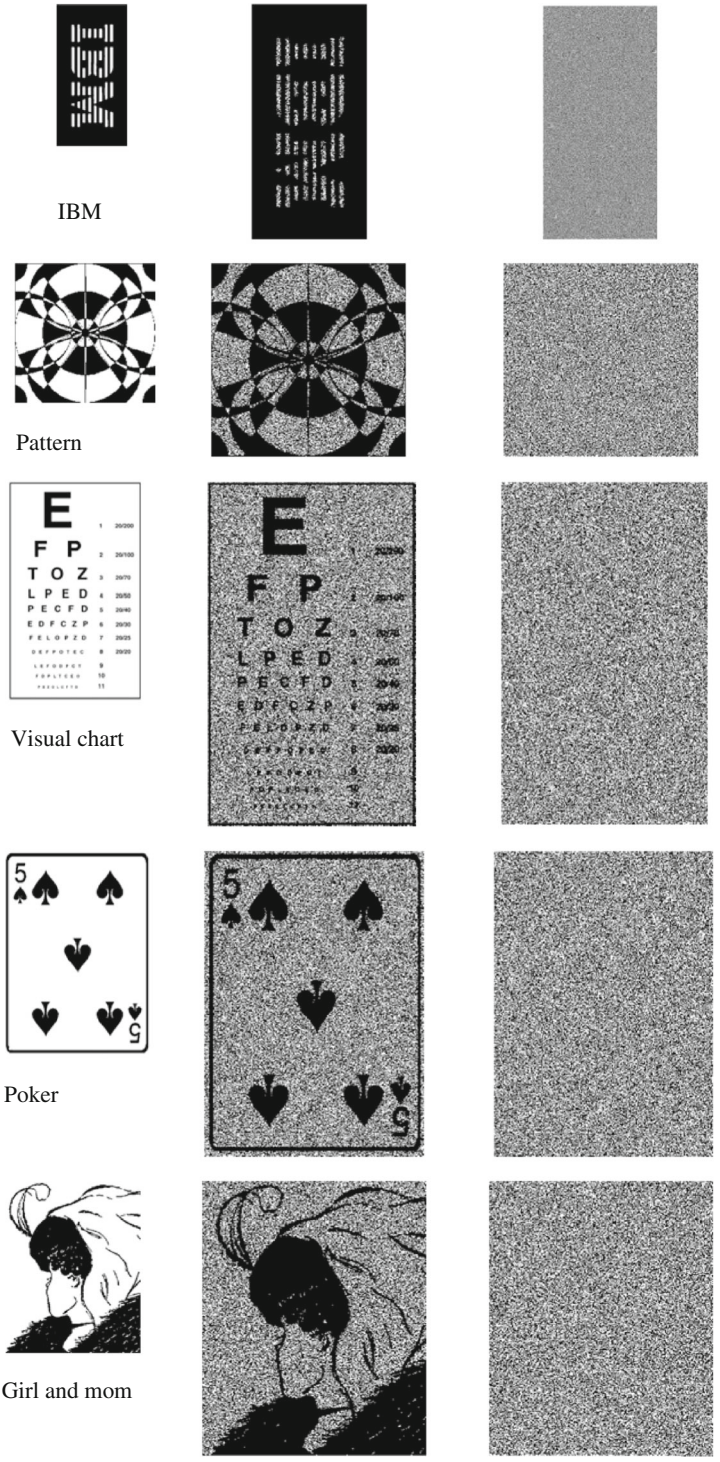


Fig. 6 Dataset for testing VC share embedded 2D barcodes

Table 2 Similarities between original and new secret images

Sample	The effects of 2D barcodes on a share
IBM	13/886×432 (0.003 %)
Visual chart	13/936×1186 (0.001 %)
Pattern	14/722×720 (0.002 %)
Poker	13/624×872 (0.002 %))
Girl and mom	13/600×738 (0.0006 %))
Human face and vase	13/474×636 (0.004 %))

modified shares can be prevented in the authentication process. Moreover, as modified shares can hardly be used to reveal the true secret, hints of secret can also be included as a significant content in a barcode. Thus we decide to use the Hash code of VC shares such as width, length, the number of black and white pixels in the share as well as related information of secret. All the meta-data information of a 2D barcode can also be copied and kept by the dealer who is subsequently able to verify the correctness of authentication information stored in the 2D barcode of the VC shares by using a barcode scanner and a decoder. Figure 7 illustrates the VC shares which are embedded by 2D barcodes with different types of messages.

5.3 Analysis

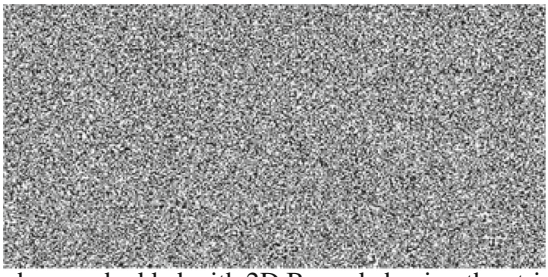
The proposed scheme of embedding 2D barcode is primarily for the security purpose. Embedding the 2D barcode into the most similar regions of VC share can effectively hide the 2D barcode. In the scenario when a VC share holder attempts to cheat by modifying the share embedded with 2D barcodes, VC dealers are able to prevent this hoax promptly by verifying the information included in the 2D barcode. Similarly, it appears to be practical for the VC dealer to resist cheatings from attackers. The Confidentiality, Integrity and Availability (CIA) [36] are commonly accepted security standards. As with the nature of information hiding, the security level of VC components is able to be evaluated by the standard of CIA.

Confidentiality prevents the security compromising by unauthorized individuals while ensuring that the real participants are able to acquire it. To make sure the authorized access, highly secure information of VC secret, such as significant account number and routing number of banking vault, is tremendously close to the stability of the society.

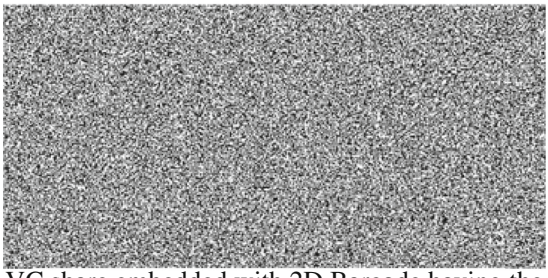
Ensuring the integrity means that only authorities might make changes to the assets [36]. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps have to be taken to ensure that data cannot be altered by authorities (e.g. in a breach of confidentiality). In addition, integrity also means responsively detecting any changes in data might cause a result of authentication failure. Thus the cheating activities can be noticed and then prevented before the VC secret revealing.

Ensuring the availability refers that the assets are absolutely available to authorized users when required. By adding authentication process in VC, all the participants should have the chance to read the secret [36]. VC shares can distribute the secret while embedding 2D barcode can improve identifying the real shares from the unauthorized ones.

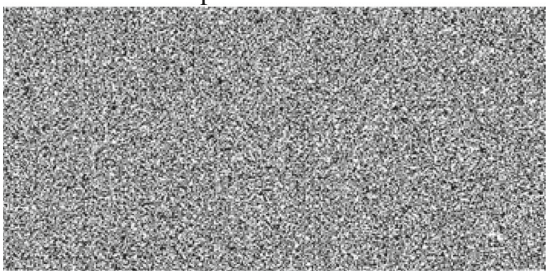
Another important security assess criterion is Authentication, Authorization, Auditing and Accounting (AAA) [25]. A 2D barcode can perform as a key of access to the VC shares and the authentication of VC shares thus should be ensured as the information stored in 2D barcodes only are read by a scanner. The AAA authentication of VC shares can compare a user's authentication credentials (data in 2D barcodes) with others. The user is granted access to the VC secret revealing process only if the information is right. If the credentials are different, the request of access would be denied and the authentication fails.



(a) A VC share embedded with 2D Barcode having the string "AUT"



(b) A VC share embedded with 2D Barcode having the URL 'http://www.aut.ac.nz'



(c) A VC share embedded with 2D Barcode having the Hash code of "Height: 432 Width: 886 Blackpixels: 18563 Hints of secret: ibm"

Fig. 7 Examples of VC shares embedded with Data Matrix barcodes. (**a**) A VC share embedded with 2D Barcode having the string "AUT". (**b**) A VC share embedded with 2D Barcode having the URL 'http://www.aut.ac.nz' (**c**) A VC share embedded with 2D Barcode having the Hash code of "Height: 432 Width: 886 Blackpixels: 18563 Hints of secret: ibm"

Accounting offers the approaches for collecting information about the end users resource consumption, which can then be processed for billing, auditing, and capacity planning purposes [36]. Auditing functionality permits to verify the correctness of procedures carried out based on accounting data. The information stored in 2D barcodes of VC shares needs to be verified and the process of secret revealing is conducted based on the result of data matching. In this paper, we concentrate on the authentication aspect of this protocol so as to protect the security of the property from being obtained by cheaters.

Even though embedding 2D barcode into VC shares for the authentication can be evaluated by both CIA and AAA, there exist drawbacks of this approach of authenticating VC shares. Firstly, despite the replaced regions of the VC share is the most similar one, cheaters are able to find the 2D barcode on VC share in some occasions. Therefore it is expected to improve the

barcode embedding so as to make the authentication process more effectively. Besides, our algorithm of embedding 2D barcode is only applied to (2, 2) -VCS. More cases of (k, n)-VCS are expected to be investigated.

6 Conclusion

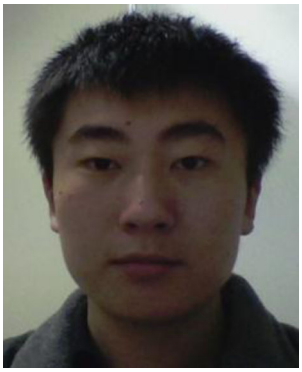
This paper investigated the authentication problem of VC and justified one of its solutions which are to seek the aid from using 2D barcodes. On the basis of previous work of VC and advantages of various barcodes, we implemented a scheme of embedding a 2D barcode into a VC share by searching for the most similar region which is used to replace the corresponding regions of the share afterwards. Our contribution is to implement the VC authentication and minimize the side-effect on the revealed secret by using the given 2D barcode.

Although there are a broad range of benefits of using 2D barcodes in VC authentication, the improvement presented by this paper has practical significance. Our future work will focus on embedding a 2D barcode into shares of other VC schemes such as that of multiple secrets VC, etc.

References

1. Ateniese G, Blundo C, Santis AD, Stinson DR (2001) Extended capabilities for visual cryptography. Theor Comput Sci 250:143–161
2. Campbell A (2000) The designer's lexicon. Chronicle Books, San Francisco
3. Chen Y-F, Chan Y-K, Huang C-C, Tsai M-H, Chu Y-P (2007) A multiple-level visual secret-sharing scheme without image size expansion. Inf Sci 177:4696–4710
4. Chen, S.-Q. A Corner Matching Algorithm Based on Harris Operator. In: Information Engineering and Computer Science (ICIECS), 2010 2nd International Conference on, pp. 1–2 (2010)
5. Chen Y-C, Tsai D-S, Horng G (2012) Comment on "cheating prevention in visual cryptography". IEEE Trans Image Process 21:3319–3323
6. Chen Y-C, Tsai D-S, Horng G (2012) A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography. J Vis Commun Image Represent 23:1225–1233
7. Dobbertin H (1998) Cryptanalysis of MD4. J Cryptol 11:253–271
8. Denso ADC:QR code Essentials (2011)
9. Gao, M., Sun, B. Blind Watermark Algorithm Based on QR Barcode. In: Wang, Y., Li, T. (eds.) Foundations of Intelligent Systems, vol. 122, pp. 457–462 (2012)
10. Guo T, Liu F, Wu CK (2013) Threshold visual secret sharing by random grids with improved contrast. J Syst Softw 86(8):2094–2109
11. Hahn, H., Jung, J. Improving performance of the decoder for two-dimensional barcode symbology PDF417. In: Braz, J., AraÚJo, H., Vieira, A., EncarnaÇÃO, B. (eds.) Information in Control, Automation and Robotics I, pp. 233–237 (2006)
12. Hegde, C., Manu, S., Shenoy, P., Venugopal, K., Patnaik, L. Secure authentication using image processing and Visual Cryptography for banking applications. In: 16th International Conference on Advanced Computing and Communications, pp. 65–72 (2008)
13. Horng G, Chen T, Tsai D-S (2006) Cheating in visual cryptography. Des Codes Crypt 38:219–236
14. Hou Y-C (2003) Visual cryptography for color images. Pattern Recogn 36:1619–1629
15. Hu CM, Tzeng WG (2007) Cheating prevention in visual cryptography. IEEE Trans Image Process 16(1):36–45
16. International Organization for Standardization ISO/IEC 16022–2000: Information technology international symbology specification-Data matrix. Switz Joint Tech Comm ISO/IEC JTC 1:67–87 (2004)
17. Jiang, F., Liu, Z., Feng, X. Research of Encodation Schemes Selecting Optimization for Character 2D Barcode. In: Yang, Y., Ma, M. (eds.) Proceedings of the 2nd International Conference on Green Communications and Networks 2012 (GCN 2012): Volume 1, vol. 223, pp. 615–623. Springer Berlin Heidelberg (2013)
18. Kuo, D., Wong, D., Gao, J., Chang, L. A 2D Barcode Validation System for Mobile Commerce. In: Bellavista, P., Chang, R.-S., Chao, H.-C., Lin, S.-F., Sloot, P.A. (eds.) Advances in Grid and Pervasive Computing, vol. 6104, pp. 150–161 (2010)
19. Lau, D.L., Arce, G.R.: Modern digital halftoning. CRC Press (2011)

20. Lee Y-S, Chen T-H (2012) Insight into collusion attacks in random-grid-based visual secret sharing. Signal Process 92:727–736
21. Liu F, Wu CK, Lin XJ (2008) Color visual cryptography schemes. Inf Secur, IET 2:151–165
22. Liu F, Wu CK, Lin XJ (2010) Some extensions on threshold visual cryptography schemes. Comput J 53(1):107–119
23. Liu F, Wu C, Lin X (2011) Cheating immune visual cryptography scheme. IET Inf Secur 5:51–59
24. Memon N, Wong PW (1998) Protecting digital media content. Commun ACM 41:35–43
25. Metz C (1999) AAA protocols: authentication, authorization, and accounting for the internet. IEEE Internet Comput 3:75–79
26. Myodo, E., Sakazawa, S., Takishima, Y.: Visual cryptography based on void-and-cluster halftoning technique. In: Image Processing, 2006 I.E. International Conference on, pp. 97–100. IEEE (2006)
27. Myodo, E., Takagi, K., Miyaji, S., Takishima, Y.: Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: Multimedia and Expo, 2007 I.E. International Conference on, pp. 2114–2117. IEEE (2007)
28. Nakajima, M., Yamaguchi, Y.: Extended Visual Cryptography for Natural Images. In: WSCG, pp. 303–310 (2002)
29. Naor, M., Pinkas, B. Visual Authentication and Identification. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 322–336 (1997)
30. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptology – EUROCRYPT' 94, pp. 1–12. Springer (1995)
31. Revenkar PS, Anjum A, Gandhare WZ (2010) Survey of VC schemes. Int J Secur Appl 4:49–56
32. B. V. Rompay, "Analysis and Design of Cryptographic Hash functions, MAC algorithms and Block Ciphers", Ph.D. thesis, Katholieke Universiteit, Leuven, Belgium (2004)
33. Rouillard, J.: Contextual QR codes. In: ICCGI 2008. The Third International Multi- Conference on Computing in the Global Information Technology, July 27-August 1, pp. 50–55 (2008)
34. Shyu SJ, Huang S-Y, Lee Y-K, Wang R-Z, Chen K (2007) Sharing multiple secrets in VC. Pattern Recogn 40:3633–3651
35. Sobti R, Geetha G (2012) Cryptographic hash functions: a review. IJCSI Int J Comput Sci Issues 9:461–479
36. Solms, S.H., Solms, R.: Information Technology Governance. Information Security Governance, pp. 1–7. Springer (2009)
37. Stoleru D (2005) Extended visual cryptography schemes. Dr Dobb's J 30:36–39
38. Touch JD (1995) Performance analysis of MD5. SIGCOMM Computing Commun Rev 25:77–86
39. Tuyls, P., Hollmann, H. D. L., Lint, J. H. V., Tolhuizen, L.: XOR-based VC schemes. Designs, Codes and Cryptography 37, 169–186 (2005) 19 Veltkamp, R. C.: Shape matching: similarity measures and algorithms. Paper presented at the Shape Modeling and Applications, SMI 2001 International Conference on (2001).
40. Vincent E, Laganière R (2005) Detecting and matching feature points. J Vis Commun Image Represent 16:38–54
41. Wang G (2014) Content based authentication of visual cryptography. Master Thesis. Auckland University of Technology, New Zealand
42. Wang, Z., Arce, G.R.: Halftone visual cryptography through error diffusion. In: Image Processing, 2006 I.E. International Conference on, pp. 109–112. IEEE (2006)
43. Wei-Qi Yan, Duo Jin, Kankanhalli, M.S. Visual cryptography for print and scan applications, Proceedings of the IEEE ISCAS'04, pp.572 - 575 (2004)
44. Weir J, Yan W-Q (2009) Dot-size variant VC. In: Ho ATS, Shi YQ, Kim HJ, Barni M (eds) IWDW 2009. LNCS, vol 5703. Springer, Heidelberg, pp 136–148
45. Weir, J., Yan, W.: A Comprehensive Study of VC. In: Shi, Y. (ed.) Transactions on Data Hiding and Multimedia Security V, vol. 6010, pp. 70–105. Springer Berlin Heidelberg (2010)
46. Weir, J., Yan, W.: Authenticating VC Shares Using 2D Barcodes. In: Shi, Y., Kim, H.-J., Perez-Gonzalez, F. (eds.) Digital Forensics and Watermarking, vol. 7128, pp. 196–210. Springer Berlin Heidelberg (2012)
47. Weir, J., Yan, W.-Q: Sharing multiple secrets using VC. In: Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on, pp. 509–512 (2009)
48. Yan, Y., Li, Q., Cao, M., Chen, H., Xue, J.: Application Research of Two-Dimensional Barcode in Information Construction of Colleges. In: Lu, W., Cai, G., Liu, W., Xing, W. (eds.) Proceedings of the 2012 International Conference on Information Technology and Software Engineering, vol. 212, pp. 71–80. Springer Berlin Heidelberg (2013)
49. Yang C-N, Chen T-S, Ching M-H (2006) Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme. Integr Computer-Aided Eng 13:189–199
50. Yang, C., Laih, C.: Some new types of visual secret sharing schemes. In: National Computer Symposium (NCS 1999), vol. III, pp. 260–268 (1999)
51. Zhang, C., Ma, L., Mao, D.: A 2D Barcode Recognition System Based on Image Processing. In: Zhu, M. (ed.) Electrical Engineering and Control, vol. 98, pp. 683–688. Springer Berlin Heidelberg (2011)
52. Zhou, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography. In: ICIP 2003. International Conference on, pp. I-521-524 vol. 521 (2003)



G. Wang is a master degree student with Auckland University of Technology, New Zealand. His research interest is visual cryptography.

F. Liu received his PhD degree from Chinese Academy of Sciences, China, his research interest is visual cryptography.

W. Yan received his PhD degree from Chinese Academy of Sciences, China, his research interest is media security.