

# Multimedia Tools and Applications

## Content Based Authentication of Visual Cryptography

--Manuscript Draft--

<b>Manuscript Number:</b>	MTAP-D-15-01208R1
<b>Full Title:</b>	Content Based Authentication of Visual Cryptography
<b>Article Type:</b>	Manuscript
<b>Keywords:</b>	Visual cryptography, secret sharing, digital image processing
<b>Corresponding Author:</b>	W. YAN, PhD AUT University Auckland, New Zealand NEW ZEALAND
<b>Corresponding Author Secondary Information:</b>	
<b>Corresponding Author's Institution:</b>	AUT University
<b>Corresponding Author's Secondary Institution:</b>	
<b>First Author:</b>	W. YAN, PhD
<b>First Author Secondary Information:</b>	
<b>Order of Authors:</b>	W. YAN, PhD
	G. Wang, Msc
	M. Kankanhalli, PhD
<b>Order of Authors Secondary Information:</b>	
<b>Funding Information:</b>	

## Responses to Reviewers' Comments

MULTIMEDIA TOOLS AND APPLICATIONS

### Content Based Authentication of Visual Cryptography

(MTAP-D-15-01208)

#### Reviewer #1

**Q 1.1.** The article shows deep expertise of its authors in this particular field of research. Despite that most of the paper is devoted to explanation of the reasoning and general philosophy of the proposed approach (with some repetitions of the basic points), it is quite well organized and seems technically sound. In conclusion, to my opinion this topic will be very interesting for the readers of Multimedia Tools and Applications, and I recommend the publication perhaps after some minor revision.

**A. 1.1.** We thank you very much for your kind comments, we now have corrected our paper and hope most of mistakes and errors have been removed from this version. Thank you.

#### Reviewer #2

**Q 2.1.** This paper proposed a visual cryptography method which can authenticate each share by generating the 2-d barcode with hash. However, this paper is lack of details.

**A 2.1.** Thanks for your comments, now we have added the details in this paper (marked with blue colour), including the mathematical equations.

**Q 2.2.** there are many unclear places. For example, how to generate the shares, how to extract visual features, how to transform these visual features into binary string, how to embed barcode and so on. Sometimes, the transform is DWT transform, sometimes, it is walsh transform.

**A 2.2.** Thanks for your comments, we now have done our best to introduce those fundamental knowledge of Visual Cryptography (VC), we do hope a VC beginner could understand our work well. In this paper, we define DWT as Digital Wash Transform, because it is used for binary image processing in this paper.

**Q 2.3.** the figures are not coincide with the text.

**A 2.3.** We now revise our paper and hope the text matches the figures.

#### Reviewer #3

**Q 3.1.** ... They should give more detailed discussions about the pixel extension of visual secret and time consuming.

**A 3.1.** What we discussed in this paper is about VC authentication. Therefore we use the standard visual cryptography scheme, the security and time consuming of the VC scheme have been guaranteed by the previous papers related to this scheme, therefore we did not discuss these issues more in this paper.

**Q 3.2.** In page 8, there is a reference mistake: "The 2D barcode of embedding this Hash code into Data Matrix is shown in Figure 5." It should be "...Figure 3."

**A. 3.3.** Thanks for your comment, we now have correct our mistake.

#### **Reviewer #4**

**Q 4.1** This paper analyzes VC authentication problems using visual and cryptographic features and introduces the unique Hash code for VC authentication. The content of the paper is very interesting.

**A 4.1.** Thanks for your comments on this paper, we are very much obliged to you.

**Q 4.2.** The description of the proposed method is not very clear. It is very difficult to get the authors' contributions.

**A 4.2.** Since current VC research could not take traditional image processing and traditional cryptography into consideration, our motivation in this work is to take a further step, and combine the two areas together and push the VC research forward. Our idea is very new, we therefore re-write the most parts of the paper and hope the new version could be better for you to understand our contributions.

**Q 4.3.** The English of the paper should be polished carefully.

**A 4.4.** Thanks for your comments, we now revised the paper and hope this new version suits you better.

[Click here to view linked References](#)

# Content Based Authentication of Visual Cryptography

G. Wang<sup>1)</sup>, W. Yan<sup>1)</sup> and M. Kankanhalli<sup>2)</sup>

<sup>1)</sup>Auckland University of Technology, New Zealand

<sup>2)</sup>National University of Singapore, Singapore

*Abstract*— Visual Cryptography (VC) has been developed as a significant research arena in media security. Despite of its obvious strengths, recent investigations have debated this scheme from adverse aspects, its problem is lack of authentication of VC shares, VC authentication related to digital image processing and cryptography has not been fully integrated together in the past years. In this paper, we analyze both visual features and cryptographic features of VC shares and take use of them for VC authentication. Compared to those existing methods, our contribution is the first one to integrate visual features and cryptographic features of VC shares into Hash code for the purpose of VC authentication.

*Index Terms*—visual cryptography, secret sharing, digital image processing

## I. INTRODUCTION

Visual Cryptography (VC) was initialized by Naor and Shamir in 1994 [1]. As a powerful technique in information security, VC exhibits its immense potentiality of visually protecting secrets from the view of secret sharing [2, 3]. Visual Cryptography Scheme (VCS) is defined that a secret image (usually black and white) is divided into several images having the identical size called VC shares. Each of the shares has not obvious appearance of the original secret image though viewers are able to clearly perceive the secret by simply overlaying them together using transparent operation of digital images.

The encryption of VCS is based on pixel expansion that one pixel on the original secret image is presented by a number of sub-pixels in its corresponding square regions on the shares [2]. The color of a specific pixel on VC shares is determined by the expansion rules of VCS. With regarding to the decryption of VC, there are a twofold of VC secret revealing operations, namely, XOR (Exclusive OR) and OR. Taken these two binary operations into consideration, XOR operation of digital images is better in revealing the secret image than that of OR [2], OR operation is regarded as the simplification. On the superimposed VC secret image, a brighter region is represented by a group of white and black pixels while darker regions are filled up with black pixels only. The contrast between bright regions and dark regions is easily identified by our Human Visual System (HVS) [2], thus, VCS requires visible contrast in secret revealing indeed.

There are two roles in VC: (1) a participant who is the holder of VC shares; (2) a dealer who is responsible for the distribution of VC shares. In a  $(k, n)$ -VCS, a secret image is split into  $n$  shares and it could be revealed by superimposing at least  $k$  shares together. Nevertheless, the secret is invisible if the number of authorized VC shares is less than threshold  $k$ .

Amongst various VC schemes, there are five ones which have been well investigated [5]. Traditional visual cryptography refers to the basic VC scheme which utilizes only black and white pixels to present binary images while the VC shares are the binary images without semantic information [1]. Extended visual cryptography is similar to traditional visual

1  
2  
3  
4 cryptography, but the shares in extended visual cryptography are images with meaningful cover  
5 information without any clues related to the secret [2]. Dynamic visual cryptography refers that  
6 VC shares are applied to reveal more than one secret [4], we shift two shares in multiple  
7 directions slightly, multiple secrets will be discovered. Color visual cryptography is used to share  
8 color secret images which are presented by color halftone schemes, real color images having 24  
9 bits depth in RGB channel are able to be shared if the halftoning technology is adopted [7,8].  
10 Furthermore, progressive visual cryptography copes with the cases where the secrets are revealed  
11 step by step using multiple shares which depends on the needs of secret revealing, different  
12 quality of secret image in multiple resolutions will be presented for different requirements [7].  
13  
14

15  
16 The main advantages of VCS are grouped into three categories [5]. The first is that VC secret  
17 is revealed by using only VC shares which are convenient to be carried, unlike other  
18 cryptographic methods that need complicated computations and computing machines for the  
19 decryption. Different from those traditional cryptographic methods which tackle a string of  
20 ASCII letters (characters) called plain text, VCS takes advantages of secret images as the input  
21 for encrypting and decrypting the secret. Compared to encrypt plain text, VC encryption has  
22 much larger capacity for holding the secret. Besides, VCS is a one-time padding cryptographic  
23 scheme which makes it unconditionally secure though the key size is a bit big. Moreover, VC is  
24 a scheme based on secret sharing which are able to be kept by all participants.  
25  
26

27  
28 Meanwhile the advantages of VCS are very appealing and inspired by relevant security  
29 applications; relevant work has shown that there exists an authentication problem, the VC shares  
30 are easily to be duplicated. Cheating compromises VCS authentication from both malevolent  
31 participants and intruders [12,13,14], the problem of VCS from visual and cryptographic aspects  
32 in authentication has not been comprehensively solved.  
33

34  
35 VC cheating typically includes cutting and pasting as well as malicious modifying, those  
36 operations could disrupt the decryption, which affect VC participants to get the original secret  
37 correctly since partial VC shares could be manipulated by using image editing tools while the  
38 secret is still possible to be restored. Other operations may affect VC authentication from image  
39 quality degradation such as compressing, duplicating, and photocopying, etc. [5,13]  
40

41  
42 Cheating prevention has been raised due to VC security. In VC, cheaters are able to create  
43 fake shares so as to coax the VC dealer for obtaining the secret. The typical case is multiple  
44 secret sharing based on common shares. The authentication of this case is therefore needed to  
45 check authenticity of the shares before secret revealing. [13,14]  
46

47  
48 There are two authentication methods available for checking the VC shares and secret: (1)  
49 adopting additional shares to check authentication of the shares and the secret; (2) utilizing blind  
50 authentication technique to prevent estimating genuine secret. A scheme of embedding 2D  
51 barcodes into VC shares as an authentication channel has been developed recently [3,18], this  
52 method is effective with minor effects on the VC shares.  
53

54  
55 In this paper, we will take use of visual features and cryptographic features for VC  
56 authentication [12,17,19]. To the best of our knowledge, this is the first time that computable  
57 features are combined together for authentication of VC shares. The remaining content of this  
58 paper is organized below. We will detail those visual features and delineate how these features  
59 will be applied to VC authentication in Section II (A), cryptographic features of VC shares will  
60 be depicted in Section II (B). In Section III, we will combine these two features together and  
61  
62  
63  
64  
65

1  
2  
3  
4 address the scheme so as to solve the VC authentication problem. Our results and analysis will  
5 be illustrated in Section IV. Finally, the conclusion will be drawn in Section V.  
6  
7

## 8 9 II. RELATED WORK

10 Based on rules of VCS, the extended VC was conducted due to the request of enhancing visual  
11 semantics of the shares. Dynamic VC was proposed to meet demand of improving capacity of  
12 secret information [4]. Color and grayscale VCS aim at expanding the diversity of available  
13 pixels to improve its visual effects [7,8]. As VCS is an instance of secret sharing in  
14 cryptography, its encryption and decryption are constructed on the basis of access structure  
15 [1,2,5].  
16  
17

18  
19 In traditional VCS, secret encryption and decryption are achieved by image sharing which is  
20 the scheme that applies secret sharing to digital images. Typically, in  $(k, n)$ -VCS, the secret  
21 image is divided into  $n$  VC shares identically and VC decryption cannot succeed unless at least  $k$   
22 pieces are superimposed together.  
23

24 Since there are multiple black and white pixels in traditional VC, the superimposed result for  
25 secret revealing is hard to be secured. This is due to the fact that VC decryption is based on OR  
26 operation which appears to have the trouble of contrast loss. While our Human Visual System  
27 (HVS) is able to percept the black and white regions if the contrast is good enough. It is proved  
28 that using only black pixels to present a black pixel in secret image apparently has better  
29 contrast. In VC schemes, the contrast is evaluated by using Hamming weight  $w(v)$ : for any  
30 existing  $h_x$ ,  $\alpha > 0$ , in the set  $C_0$ ,  $w(v) < h_x - \alpha m$ ; while in the set of  $C_1$ ,  $w(v) > h_x$ , where  
31  $h_x$  and  $h_x - \alpha m$  represent the darkness level and whiteness level respectively;  $m$  is the pixel  
32 expansion level;  $\alpha$  denotes the relative difference.  
33  
34  
35

36 In order to uplift the contrast of OR operation in VC, previous studies demonstrated four  
37 solutions [1,8]. The first contrast enhancing method was designed based on the structure of basis  
38 matrix, the second is to utilize the disciplines of contrast. Unlike the two methods  
39 abovementioned, the third one was to employ search algorithms for seeking the scheme which is  
40 able to generate the maximum contrast. Despite contrast of the discovered secret is based on OR  
41 operation, VC schemes could be rectified, the fourth effective way of improving contrast is to  
42 reveal VC secret with other operations such as XOR, or to distribute more than one shares to  
43 each participant [2].  
44  
45

46 Except traditional VCS, other VC schemes are also under consideration including size-  
47 invariance VC [1], extended VC, progressive color VC [2], previous research work has  
48 investigated possible applications of VC in printing industry and digital watermarking, etc. [9,  
49 10,11]  
50  
51

52 Participants who hold VC shares are lack of ability to identify authenticity of all shares and the  
53 secrets, given cheaters the opportunity to create unauthorized shares which simulate the  
54 behaviors of valid shares so as to obtain the hidden secret. Thus cheating prevention approaches  
55 are needed to block the cheating happens. [13,14] A variety of cheating methods have been  
56 created and each of the methods is capable of implementing a cheating scheme. In VCS, both  
57 participants and intruders have the opportunity to cheat others. Particularly, collusive participants  
58 have such chances to cheat by providing forged overlaying results of their shares to other  
59  
60  
61  
62  
63  
64  
65

participants. The forgery VC shares from intruders are generated by encrypting fake secret image into shares with different scales and pixel deployment methods. Due to the security weaknesses of existing VC shares, the work related to VC cheating solutions has been arisen such as transform one VCS to another which matches the cheating prevention requirements. Our contribution in this paper is to propose a cheating prevention scheme via VC authentication by using the assistances from visual and cryptographic features of VC shares.

### A. Visual Features of VC

As VC is to process digital images having visual secret, VC secret image and VC shares certainly are able to be analyzed by using techniques from digital image processing. Therefore, we are able to select visually computable features of digital images for VC authentication. Specifically, we decide to use pixel colors, histogram, entropy, moments and centroid, Tamura textures, coefficients of Discrete Walsh Transform (DWT), etc. Each of these features is related to binary images like VC shares. Even though the information stored in VC shares is always massive, the secret image is not able to be perceived by our HVS straightforward. Moreover, the security of VC shares is also related to computable features of the image, therefore it is crucial to deal with the VC authentication issues from the visual viewpoint.

Digital image processing has been utilized to extract image features in both spatial and frequency domains. In spatial domain, the typical features include pixel colors, histogram, entropy, moments and centroid, etc., we thus apply the above listed features to authenticate VC shares in this paper.

Moments are geometric features for describing an object such as region, size location as well as shape.[22] The moments in VC authentication are to deal with the problem of size invariance. The computation of moments of a share  $I$  is given by:

$$m_{pq} = \sum_{(u,v) \in I} u^p v^q \cdot I(u, v) \quad (1)$$

where  $p, q$  is order of the moment,  $(u, v)$  is coordinate of a pixel in image  $I$ . As for the binary images which only contain black and white pixels, therefore it is to be simply calculated by:

$$m_{pq} = \sum_{(u,v) \in I} I(u, v) \quad (2)$$

Moments are usually defined by using physical interpretations. Similarly, the mass distribution is also represented by image moments function. The total mass of a region is  $m_{00}$  and the centroid of the region is:

$$u_c = \frac{m_{10}}{m_{00}}, v_c = \frac{m_{01}}{m_{00}} \quad (3)$$

where  $m_{10}$  and  $m_{01}$  are the first order moments. Therefore, the central moments are computed as:

$$m_{pq} = \sum_{(u,v) \in I} (u - u_c)^p (v - v_c)^q I(u, v) \quad (4)$$

Moments are size invariant image features. In context of VC, the similarity between the given VC share and the genuine VC share is able to be calculated by using moments. Moreover, as the moments are commonly used for pattern recognition, the similarity between the secret image and a VC share is able to be measured. Different from the case of comparing two shares, the similarity is expected to be as low as possible.

Entropy is a measure of information capacity of the input image. Image entropy is the quantity which is generated histogram. An image that is perfectly flat has entropy of zero. The entropy is,

$$e = -\sum_{i=1}^n h_i \ln(h_i) \quad (5)$$

where  $h_i$  represents pixels in VC share,  $n$  is the number of pixels.

Texture has widely varieties based on the actual needs in practice. A global descriptor of six image characteristics is constituted by directionality, contrast, roughness, line-likeness, regularity and coarseness. These features correspond to the psychological point of view on the texture attributes.[23,24]

Directionality of Tamura texture is calculated by using the sharpness of peaks in image histogram.

$$F_{dir} = \sum_p^{n_p} \sum_{\theta \in w_p} (\theta - \theta_p)^2 H_D(\theta) \quad (6)$$

where  $p$  represents a peak,  $w_p$  represents the peak of the scope,  $H_D(\theta)$  represents the histogram constructed by calculating the numbers of all pixels' gradient vectors .

In Tamura texture [23,24], contrast is calculated by a global metric representing the grayscale histogram with its distribution. Contrast of an image is calculated by:

$$F_{con} = \frac{\sigma}{\alpha_4^{1/4}} \quad (7)$$

where  $\alpha_4 = \frac{\mu_4}{\sigma^4}$ ,  $\mu_4$  is the 4-th order moment of the mean value of gray pixels and  $\sigma$  is the variance.

Computing coarseness of Tamura texture is a method to pick a large size as the best one when a coarse texture is presented, the measurement of coarseness in Tamura texture is:

$$F_{crs} = \frac{1}{m \times n} \sum_i^m \sum_j^n S_{best}(i, j) \quad (8)$$

where  $m$  and  $n$  are the effective width and height of the image respectively.

Line-likeness in Tamura texture is an element of texture which comprises of lines. When the direction and neighboring direction for a given edge are nearly equal, we think such a group of edge points as a line.

$$F_{lin} = \sum_i^n \sum_j^m P_{Dd}(i, j) \cos \left[ (i - j) \frac{2\pi}{n} \right] / \sum_i^n \sum_j^m P_{Dd}(i, j) \quad (9)$$

where  $P_{Dd}(i, j)$  is defined as the relative frequency with which two neighboring cells separated by a distance  $d$  along the edge direction occur on the image, one with the direction code  $i$  and the other with the direction code  $j$ .

Regularity is used to describe repetitive patterns in mathematical form. The equation of computing regularity is defined as:

$$F_{reg} = 1 - r(\sigma_{crs} + \sigma_{con} + \sigma_{dir} + \sigma_{lin}) \quad (10)$$



where  $r$  is a normalizing factor and each  $\sigma_{xxx}$  means the standard deviation of corresponding  $F_{xxx}$ .

In frequency domain, broadly used transforms for digital image processing include Discrete Walsh Transform (DWT), DWT uses 1 and -1 as the input, which is more suitable for the authentication of VC shares. DWT transform is,

$$W_{xy}(u, v) = \frac{1}{N} \frac{1}{N} \sum_{y=0}^{N_y-1} \sum_{x=0}^{N_x-1} I(x, y) \cdot (-1)^\alpha \quad (11)$$

Its inverse transform is,

$$I(x, y) = \sum_{v=0}^{N_y-1} \sum_{u=0}^{N_x-1} W_{xy}(u, v) \cdot (-1)^\alpha \quad (12)$$

where  $\alpha = \sum_{r=0}^{P_x-1} x_r u_r + \sum_{s=0}^{P_y-1} y_s v_s$ ,  $I(x, y)$  is a pixel of the image located at  $(x, y)$ . The coefficients are used to identify authentication of VC shares. We apply the above listed features to VC authentication in this paper.

## B. Cryptographic Features of VC

In addition to visual features, cryptographic features of VC shares are effective computable characteristics in VC authentication. Previous focus of VC security is mainly on what extent that this technique is used in cheating immunization and how to design appropriate schemes to make VC more robust against attacks from cheaters.

Cryptographic Hash function [6] is easy to be used for calculating Hash value of input data, on the contrary, it is impossible to get data from a given Hash code, extremely hard to modify a data without altering the Hash and uneasily to find two different data with the same Hash code. A Hash function is the way that maps data of arbitrary length to a specific domain with a fixed length. Our solution for content based authorization of VC is based on the Hash code embedded in 2D barcodes so as to distinguish the authentic shares from the unauthorized ones [3,18]. The advantage of using the Hash code of these features is that modified shares are to be prevented in the authentication and decoding process. Thus we select the Hash code in VC authentication. All the relevant information of 2D barcodes is to be copied and kept by the dealer who is subsequently able to easily check the correctness of authentication information stored in 2D barcodes of the VC shares.

The proposed scheme of embedding 2D barcodes is mainly for the purpose of security. Embedding 2D barcodes into the most similar region in VC shares effectively hides the 2D data into the surroundings. In the scenario where a VC share holder attempts to cheat others by modifying the share which is embedded with the 2D barcodes, VC dealers are able to prevent this hoax promptly by verifying the information included in the 2D barcodes.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of VC shares. VC shares must not be changed during transmission, and the steps must be taken to ensure that the data is not altered by unauthorized users or intruders. In addition, integrity also means responsibly detecting any changes in the data that might occur as a result of authentication failure. Thus the cheating activities are noticed and then prevented before revealing the VC

1  
2  
3  
4 secret. In VC, since there are various features that are encrypted and used in authentication  
5 process, the checksum is able to be used to improve the integrity protection.  
6

7 By adding authentication process in VC, all the authorized participants have the chance to read  
8 the secret. VC shares are helpful to distribute the secret meanwhile the embedded 2D barcodes  
9 identify the real shares from the unauthorized ones.  
10

11 2D barcodes perform as a key of access to VC shares, and the authentication of VC shares thus  
12 is ensured since the information stored in a 2D barcode is only read by certain scanners. The VC  
13 authentication of VC shares compares a user's authentication credentials with others. The user is  
14 granted to access the VC secret revealing process only if the information matches. If the  
15 credentials are different, the request of access is denied and the authentication fails.  
16  
17

18 The information stored in 2D barcodes on VC shares needs to be verified and the process of  
19 secret recovery is conducted based on the result of data matching. The focus of this paper is on  
20 authentication aspect that reflects the security of VC shares.  
21

22 In terms of VC authorization, digital signatures are created with the private key of the sender  
23 that only viewers with public key are able to read the information. With regard to integrity, VC  
24 participant is able to detect whether the document has been altered if the share is signed. For the  
25 availability, the signer cannot deny what (s)he signed on the VC shares that anyone with correct  
26 signature has the right to reveal the secret.  
27  
28

29 In this paper, we will combine visual features and cryptographic features of a VC share  
30 together and make use of them for VC authentication [18,19,20]. The reason why they are  
31 combined together for authentication is that the two features reflect the essence of VCS, we need  
32 the VC shares to have visual attributes like noises which help us to hide secret meanwhile we  
33 also hope the VC shares are secure. To the best of our knowledge, this is the first time that these  
34 two kinds of different features are combined for VC authentication.  
35  
36  
37  
38

### 39 III. OUR CONTRIBUTIONS 40

41 In this paper, we aim at VC authentication by taking advantage of both visual and cryptographic  
42 features of a VC share. As mentioned in Section II, available VC visual features include colors,  
43 histogram, moments, centroid, entropy and texture [17]. Any subtle modifications on the shares  
44 are reflected in the changes of these features. In order to facilitate the comparison, it is important  
45 to select a method in the context of VC authentication.  
46  
47

48 In our proposed scheme, the feature vector  $\mathbf{V}$  is composed of visual features  $f_i$  ( $i = 1, 2, \dots, n$ ).  
49 Each feature is treated as a component of the vector, we write the feature vector as  $\mathbf{V} = (f_1, f_2, \dots,$   
50  $f_n)$ . Each component of this vector has its specific meaning, the comparison of feature vectors of  
51 VC share is calculated by the scalar magnitude.  
52

53 The proposed scheme is illustrated in Figure 1. In this scheme, the first step is to select (2, 2)-  
54 VC scheme to divide the original secret image into two shares. Next, we use both visual features  
55 and cryptographic features to calculate the digital signature, and assign the signature to the 2D  
56 Barcode. Subsequently we apply Discrete Walsh Transform (DWT) to the shares and embed 2D  
57 barcodes into the transformed shares. There are two benefits of printing signatures on the share.  
58 On one hand, visual features are stored and encoded into digital signatures; on the other hand, as  
59  
60  
61  
62  
63  
64  
65

tampers of VC authentication severely affect the secret revealing and share verification, digital signature plays a key role in preventing forged shares and protects the genuine share from being modified. In order to verify the digital signatures, we take use of digital certificate from the key Certificate Authority (CA) which distributes authorized public key for authentication. Finally, the new shares are created by inverting DWT on the transformed shares. Since the two VC shares are coherent with each other in a VC scheme, we only modify Share 2 in Figure 1, correspondingly we need to create a new Share 1. Therefore if a VC scheme has more than two shares, once one share has been tampered, we need to re-create remaining shares based on the new share.

Before the final operation of secret revealing, the new share is applied to the DWT transform so as to obtain the 2D barcode. The decryption process will continue till the authentication information in 2D barcode is verified correctly. Hash code of VC share needs to be stored in 2D barcode. Available information including pixel number, histogram information, moments, entropy and Tamura texture is shown in Figure 2.

As an extension of our proposed scheme, using visual and cryptographic features is still effective for VC authentication when applying to  $(k, n)$ -VC, and each of the shares has independent authentication process which makes sure the authentication of all VC shares.

Furthermore, locations where 2D barcodes are embedded will affect the result of inverting DWT transforms. It is preferable that the embedded regions on the share are similar to the barcodes, which have slight visual change on the new shares shown as Figure 3.

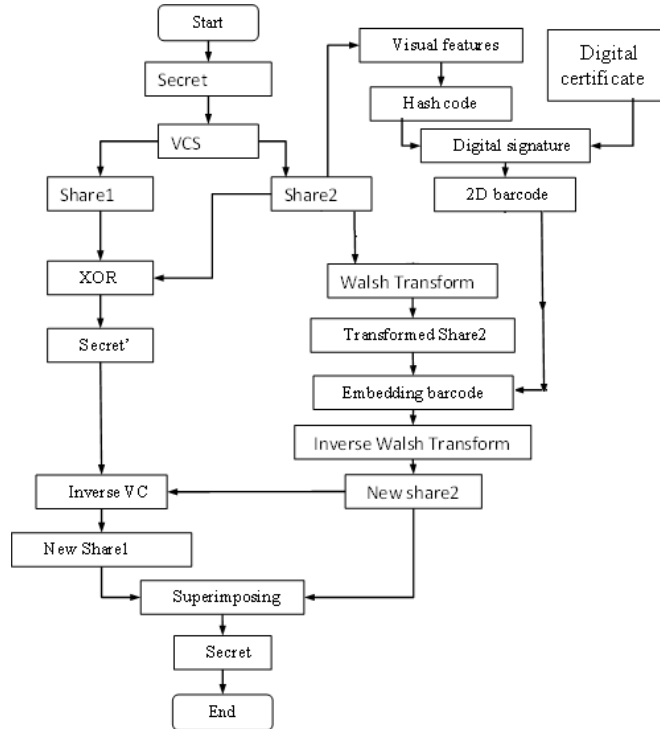


Fig. 1 The process generating VC shares

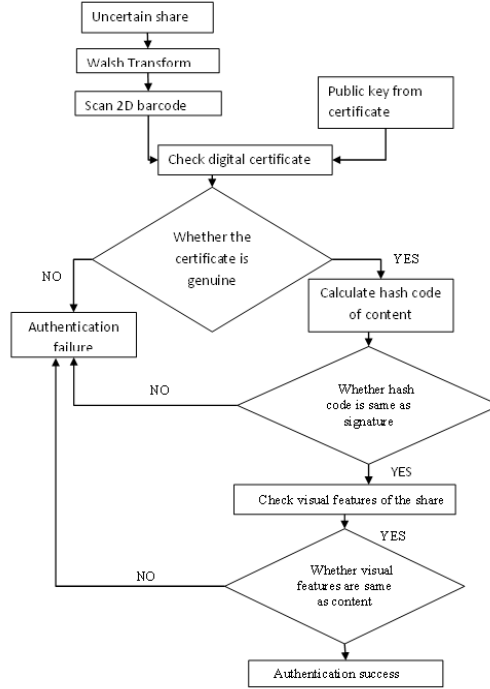


Fig. 2. The proposed process of VC authentication

#### IV. RESULTS AND ANALYSIS

In order to test the proposed scheme of embedding 2D barcodes with Hash code into VC shares, a dataset of test images has been created for evaluation purpose. The test images were collected from TV test card, Fax test card, test-bed of image compression and digital image watermarking and so on. However, as the nature of 2D barcodes and basic VC operations, the pictures need to be converted into binary ones. If a picture is not meaningful or has not perceptible contrast, it should be omitted from the dataset. Figure 4 demonstrates the pictures in the dataset embedded with 2D barcodes. These pictures were selected in various width and height. The original secret images are listed on the left side and the VC shares were processed by using the proposed scheme shown in the middle. The images on the right side of Figure 4 are the revealed secrets.

According to our proposed scheme, all these features are put into a computable vector, the vector is encoded into Hash codes. The values of the visual features are shown in Table I, the Hash code of this vector is:

*B96CC5EA402D4E164A8F885D86F017C5EEEA563A1445D1560954034A10CD2DA9*

The 2D barcode of embedding this Hash code into Data Matrix is shown in Figure 3. Since slight difference of Hash code will lead to a significant change in the result, we commit modifications on a VC share and conduct experiments using our proposed scheme to authenticate the modified share. The result is shown in Table II.

Table I Tamura Texture Value of a VC Share

Feature	Coarseness	Contrast	Directionality
<i>Value</i>	0.9125	0.25	19.3
<i>Feature</i>	Line-likeness	Regularity	Moment
<i>Value</i>	0.1244	0.95	6.61
<i>Feature</i>	Entropy	Centroid	
<i>Value</i>	0.94	(505.5008, 637.5004)	

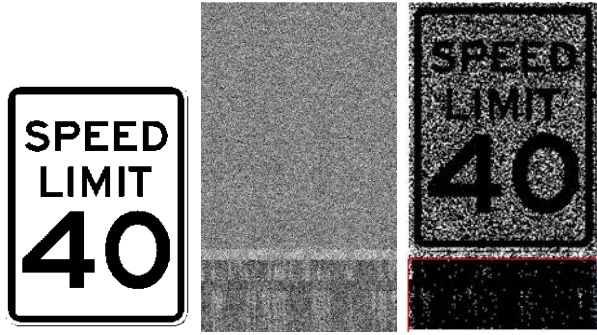
Table II The comparisons between genuine share and modified shares

Share	Hash Code	Authentication Result
Original Share	B96CC5EA402D4E164A 8F885D86F017C5EEEA 563A1445D1560954034 A10CD2DA9	N/A
Slightly Modified Share	F32E0FFF80C7892E98D 74286BCFC119A476E0E CAF5244DA23E5CF8F1 B51EAD1C	Fail
Slightly Modified Share	3DE1C857EA8CC508AE 5FA70EE2DD3E9C3A86 F48A9CC35819D06112E 1B54AC633	Fail
Largely Modified Share	301976929CD68C6D9B C0A2DD99C0F0726983 10E0B500DD1A41AF3B E92A818611	Fail
Largely Modified Share	A2E8980A9845CB637E9 96F191C2C69084399E8 DD26B8142E5C272F7B F082E7DD	Fail

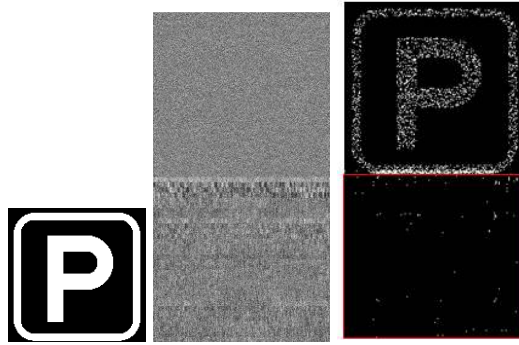


1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65

(c) VC example 3



(d) VC example 4



(e) VC example 5

Fig. 4. VC experimental results

Table III Similarity between original secret and the recovered secret

VC Images	Image Size	Similarity
1	886×432	90%
2	936×1186	91%
3	624×872	91%
4	606×800	90%
5	550×528	90%

The result in Table III shows that recovered secret is closely similar to that of original secret. One noticeable change is that there is a black region under each share (marked with red color) and the image of restored secret. This could be thought as a kind of salting in encryption since

1  
2  
3  
4 the required width and height of the image for DWT transform are required to be as a power of  
5 two. However it does not significantly affect the visual quality of each share, the embedded 2D  
6 barcode is revealed for the authentication purpose [3][18].  
7  
8  
9

## 10 V. CONCLUSION

11  
12 In this paper, we analyzed VC authentication problems using visual and cryptographic features.  
13 We provided the unique Hash code for VC authentication [6]. If a share is tampered, the Hash  
14 code will be definitely different. Our contribution is that it is the first time to apply visual and  
15 cryptographic features of VC shares in authentication when comparing to the existing work.  
16 While combining visual and cryptographic features in VC shares is able to be contributed to VC  
17 authentication, accompanying benefits include a comprehensive analysis of VC shares and the  
18 adaption of this scheme in most cases of VC. However, significant issues appear to be argued  
19 including properly embedding the 2D barcodes into the shares without affecting the visual  
20 quality of secret revealing.  
21  
22

23  
24 Despite 2D barcodes are embedded into VC shares, it may affect the visual quality by  
25 modifying parts of the shares. When taken the consideration of embedding 2D barcode into these  
26 shares, an optimized solution is to retrieve all the possible shares of the secret and searching for  
27 the best pair of share using 2D barcode.  
28

29  
30 Even though there are a range of benefits of using 2D barcodes in shares, our contributions  
31 addressed in this paper have practical implications for practitioners. The VC research work in  
32 this paper is expected to extend its vision from current VC access structure to a much wider  
33 domain such as analysis of VC content features. We will analyze further modern cryptographic  
34 features and algorithms for VC authentication in future.  
35  
36  
37

## 38 REFERENCES

- 39  
40 [1] Naor, M., and Shamir, A. (1995) Visual cryptography. In *Advances in Cryptology—*  
41 *Eurocrypt'94*, 1-12, Springer.  
42  
43 [2] Weir, J. and Yan, W. (2010) A comprehensive study of VC. In: *Springer Transactions on*  
44 *Data Hiding and Multimedia Security V*, 70-105. Springer (LNCS 6010).  
45  
46 [3] Weir, J. and Yan, W. (2012) Authenticating VC shares using 2D Barcodes. In: *IWDW 2012:*  
47 *196-210*. Springer (LNCS 7128).  
48  
49 [4] Weir, J. and Yan, W., (2009) Sharing multiple secrets using VC. In *IEEE ISCAS*, 509-512.  
50  
51 [5] Weir, J. and Yan, W. (2012) *Visual cryptography and its applications*, Bookboon.  
52  
53 [6] Stallings, W. (2013) Inside SHA-3. *IEEE Potentials*, 32(6): 26-31.  
54  
55 [7] Jin, D., Yan, W. and Kankanhalli, M. (2005) Progressive color visual cryptography. *Journal*  
56 *of Electronic Imaging*, 14(3).  
57  
58 [8] Hou, Y., Chang, C., and Tu, S. (2001) Visual cryptography for color images based on  
59 halftone technology. In *IEEE conference on Image, Acoustic, Speech and Signal Processing*.  
60  
61  
62  
63  
64  
65

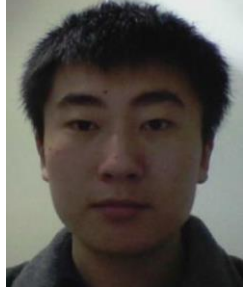






- 1  
2  
3  
4 [9] Hersch, R. D., and Chosson, S. (2004) Band moiré images. *ACM Transactions on Graphics*  
5 (TOG), 23(3): 239-247.  
6  
7 [10]Indebetouw, G., and Czarnek, R. (1992) Selected papers on optical Moire and applications.  
8 Society of Photo Optical, 64.  
9  
10 [11]Desmedt, Y. and Van Le, T. (2000) Moire cryptography. In: the 7th ACM conference on  
11 Computer and Communications Security, 116-124.  
12  
13 [12]Memon, N. and Wong, P. (1998) Protecting digital media content. *Communications of the*  
14 *ACM*, 41(7), 35-43.  
15  
16 [13]Hu, C. and Tzeng, W. (2007) Cheating prevention in visual cryptography. *IEEE*  
17 *Transactions on Image Processing* 16(1), 36-45  
18  
19 [14]Chen, Y., Tsai, D.-S. and Horng, G. (2012) Comment on “Cheating Prevention in Visual  
20 Cryptography”. *IEEE Transactions on Image Processing*, 21, 3319-3323  
21  
22 [15]Weir, J., and Yan, W. (2009) Dot-Size Variant VC. In: *IWDW 2009 (LNCS, 5703)*, 136–  
23 148, Springer.  
24  
25 [16]Yan, W., Jin, D. and Kankanhalli, M. (2004) Visual cryptography for print and scan  
26 applications. In *IEEE ISCAS'04*. 5, 572  
27  
28 [17]Corke, P. (2011) Image feature extraction robotics. *Vision and Control*, Springer, 73: 335-  
29 379.  
30  
31 [18]Wang, G., Liu, F. and Yan, W. (2016) 2D Barcodes for visual cryptography. *Multimedia*  
32 *Tools and Applications*, 75(2): 1223-1241.  
33  
34 [19]Wang, G. Liu, F. and Yan, W. (2014) Braille for visual cryptography. *IEEE International*  
35 *Symposium on Multimedia*, Taichung, Taiwan, pp. 175-276.  
36  
37 [20]Wang, G. (2015) Content based authentication of visual cryptography. Master Thesis,  
38 Auckland University of Technology, New Zealand.  
39  
40 [21]F. Liu and W. Yan (2015) *Visual Cryptography for Image Processing and Security Theory,*  
41 *Methods, and Applications*, Springer. (2-nd Edition)  
42  
43 [22]Corke, P. (2011) Image Feature Extraction. *Robotics, Vision and Control*, Springer, 73, 335-  
44 379.  
45  
46 [23]Tamura, Hideyuki, Mori, Shunji, & Yamawaki, Takashi. (1978) Textural Features  
47 Corresponding to Visual Perception. *IEEE Transactions on Systems, Man and Cybernetics*,  
48 8(6), 460-473.  
49  
50 [24]Liao, S. and Huang, T. (2013) Video copy-move forgery detection and localization based on  
51 Tamura texture features. *The 6th International Congress on Image and Signal Processing*  
52 (CISP).  
53

54 **G. Wang** received a master degree from Auckland University of Technology, New Zealand. His research interest is  
55 visual cryptography.

56 **W. Yan** received his PhD degree from the Chinese Academy of Sciences China, his research interests are digital  
57 security, forensics and surveillance.  
58

59 **M. Kankanhalli** is a Professor of the National University of Singapore, his research interests are multimedia  
60 systems and media security.  
61  
62  
63  
64  
65

	<p><b>G. Wang</b> received a master degree from Auckland University of Technology (AUT), New Zealand. His research interest is visual cryptography.</p>
	<p><b>W. Yan</b> received his PhD degree from the Chinese Academy of Sciences, his research interest is media security.</p>
	<p><b>M. Kankanhalli</b> is a Professor of the National University of Singapore, his research interest is Multimedia Systems and Multimedia Security.</p>

	<p><b>G. Wang</b> received a master degree from Auckland University of Technology (AUT), New Zealand. His research interest is visual cryptography.</p>
	<p><b>W. Yan</b> received his PhD degree from the Chinese Academy of Sciences, his research interest is media security.</p>
	<p><b>M. Kankanhalli</b> is a Professor of the National University of Singapore, his research interest is Multimedia Systems and Multimedia Security.</p>