Developing Visual Cryptography for Authentication on Smartphones

Ching-Nung Yang[1(✉)], Jung-Kuo Liao[1], Fu-Heng Wu[1], and Yasushi Yamaguchi[2]

[1] National Dong Hwa University, Hualien, Taiwan
cnyang@mail.ndhu.edu.tw
[2] University of Tokyo, Tokyo, Japan
yama@graco.c.u-tokyo.ac.jp

Abstract. Visual cryptography scheme (VCS) is a kind of cryptography that can be directly decoded by human visual system when transparent films are stacked. It requires no computation for decryption and can be stored in physical materials such as films. Therefore VCS can be a basis for providing secure and dependable authentication scheme, because it cannot be harmed by electronic and/or computational tricks. In this paper, we develop VCS for authentication on smartphones. Several authentication schemes using VCS are designed. Image quality of VCS is an inevitable issue because of small display areas of mobile devices. Thus, we will deal with VCS for continuous-tone images (gray-scale images and color images) that can enhance the image quality of VCS, so that feasible authentication schemes for smartphones will be achieved by using this continuous-tone VCS. Our authentication scheme can avoid the inconvenience of using password everywhere in modern digital life, and also resists attacks from hackers and the man-in-middle attack. This type of authentication using VCS may have a huge impact on future authentication schemes for mobile devices.

Keywords: Visual cryptography scheme (VCS) · Continuous-tone VCS · Authentication · 2D barcode · Smartphone · Threshold scheme

1 Introduction

The visual cryptographic scheme (VCS) has been firstly proposed by Naor and Shamir [1]. VCS is often implemented as a threshold (k, n) scheme, which a secret image is subdivided into n shadow images (called shadows). Any k shadows can be simply superimposed together to recover the secret image. However, (k-1) or fewer shadows cannot obtain any secret information. The attractiveness of VCS is that the reconstruction does not require any computation, and can be visually decoded via the human visual system by directly stacking shadows. This novel stacking-to-see property of VCS can be applied on securely and cheaply sharing short messages, e.g., passwords or safe-combination, in the situations where we want to recover the key without computer for some secure reasons. Although VCS cannot recover the original image without distortion, the simplicity of VCS actually provides new applications in visual authentication,

J. Wan et al. (Eds.): Industrial IoT 2016, LNICST 173, pp. 189–200, 2016.
DOI: 10.1007/978-3-319-44350-8_19

steganography, and image encryption. For example, some VCS applications combining watermark, fingerprint, Google street view, and bar code were introduced in [2–5].

Especially, the stacking-to-see property makes VCS ideally suited for use in visual authentication, and can let a user perform verification personally. This type of authentication involving human factor actually enhances the system security like seeing-is-believing. The first visual authentication using VCS was proposed by Naor and Pinkas [6]. RcCune et al. also adopted VCS to enhance the security in logging to a wireless AP [7]. Some security criteria of VSS-based authentication are formally discussed in [8]. To enhance the recognition of PIN code in visual authentication, the segment-based VCS was introduced [9]. Other VCS-based authentication schemes can are accordingly proposed [10–12].

In this paper, we adopt the high image quality of continuous-tone VCS to print shadow on a film, which can be stuck on the smartphone screen. Finally, a simple, efficient and secure VCS-based authentication on smartphone can be achieved. Several VCS-based authentication schemes are designed. The rest of this paper is organized as follows. In Sect. 2, the notion of VCS is briefly reviewed. In Sect. 3, we propose two authentication schemes (QR-code-based authentication and content-based CAPTCHA-like visual authentication). By integrating various VCS, we design a multi-server system authentication in Sect. 4. Comparison and discussion are included in Sect. 5. The conclusion is in Sect. 6.

2 Preliminary

The main technology used in this paper is VCS, which is a kind of cryptography that can be decrypted directly with human visual system without any computation. Naor and Shamir's (k, n)-VCS [1] is implemented by $n \times m$ black and white Boolean matrices B_1 and B_0. The collection C_1 (respectively, C_0) is a set obtained by permuting the columns of B_1 (respectively, B_0) in all possible ways. When sharing a black (respectively, white) secret pixel, the dealer randomly chooses one matrix in C_1 (respectively, C_0) and select a row to a relative shadow. In a black-and-white VCS, each pixel is subdivided into m subpixels in each of n shadows. A (k, n)-VCS uses h black subpixels and $(m-h)$ white subpixels (denoted as $h\mathrm{B}(m-h)\mathrm{W}$), and $l\mathrm{B}(m-l)\mathrm{W}$, where $0 \leq l < h \leq$ m, to represent black and white secret pixels, respectively. The values of h and l are the blackness of black color and white color.

Here, we use the (2, 2)-VCS with $B_1 = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}$ and $B_0 = \begin{bmatrix} 1100 \\ 1100 \end{bmatrix}$ of $m = 4$ (no aspect ratio distortion) to illustrate a simple 2-out-of-2 VCS. For each row, it is observed that we have 2B2 W, and thus shadows are noise-like. When stacking two shadows, we have 4B0 W and 3B1 W for black and white secret pixels (i.e., $h = 4$ and $l = 2$), and we can visually decode the secret image. Figure 1 illustrates this (2, 2)-VCS where a secret image (a chessboard-like picture in Fig. 1(a)) is reconstructed by stacking two transparent films on which random-dot-like images are printed. This kind of VCS can be realized as follows. Suppose an image on a film has pixels each of which consists of 2 by 2 subpixels where two of them are white and rests are black.

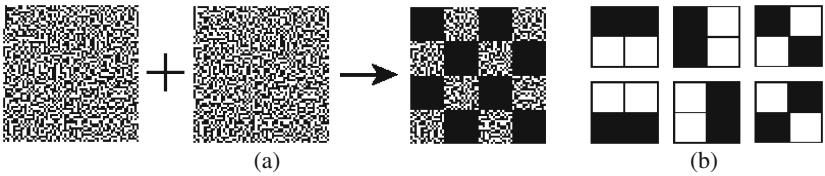

Fig. 1. A (2, 2)-VCS with $m = 4$, $h = 4$ and $l = 2$: (a) shadows and the stacked result (b) six patterns of 4-subpixl block.

There are six patterns of such subpixel arrangements as depicted in Fig. 1(b). The pattern remains the same if the same patterns are stacked. The result becomes totally black when the reverse patterns in each column of Fig. 1(b) are stacked.

3 The Proposed Visual Authentication Schemes

Our paper is not just to design VCS-based authentication schemes on smartphones. Image quality of VCS is an inevitable issue because display areas of mobile devices are very limited. Therefore, we will show how to enhance the image quality of the stacked result of VCS.

3.1 QR Code Based Authentication

Because two-dimensional (2D) barcode contains only black/white point, which is the same to the traditional VCS. So, the combination of these two technologies is reasonable. In fact, there are already some literatures on combining VCS and 2D barcode [5, 13]. In [5], the authors studied embedding the public and private information into 2D barcode by VCS. Another approach [13] adopts 2D barcode on shadows for cheating prevention. Our combination of VCS and 2D barcode is different to these two types. Our shadows are noise-like and the stacked result is 2D barcode. Table 1 shows the advantages of such combination.

Table 1. Advantages of the proposed combination of VCS and 2D barcode.

Advantage	Description
Robustness ability	The recovered image of VCS has distortion, while 2D barcode has the robustness against error. If the errors of superimposed image are within the fault-tolerant ability of 2D barcode, then barcode decoder can correctly decode the secret. Therefore, via this combination, the robustness of 2D barcode can make up for the poor image of VCS
Embedding capacity	2D barcode has the small size and meantime can carry the large and various data (such as: images, text, symbols and other types of information). This feature can make up the shortcoming of traditional VCS that only decodes a simple image
Easy decoding	2D barcodes are widely used in business, and barcode decoders are already very common, and meanwhile all smartphones can decode 2D barcode. Thus, we can easily decode 2D barcode anywhere

QR code (abbreviated from Quick Response Code) is a type of matrix 2D barcode, which is first designed for the automotive industry in Japan. This barcode is a machine-readable optical label. It has large storage capacity, high-speed identification, and small printed area, and thus is widely used. In this paper, we adopt QR code in the proposed authentication scheme.

Via combining VCS and 2D barcode, we can recover a 2D barcode by sticking a film on a smartphone screen. Then, we provide this bar code to decoder for authentication. As shown in Fig. 2(a), there are three entities in the proposed QR-code-based authentication: verification server (VS), smartphone (SP) and barcode decoder (BD). By using a (2, 2)-VCS, VS generates two shadows and keep one as a verification shadow in VS, and print the other shadow on a film. This low-cost, credit-card sized film can be stuck to smartphone screen. At this time, the film with a smartphone plays the role of a "pass token" like using the Passbook in iPhone. If the user wants to login for some sites, SP sends a request to VS. After receiving the login request, VS sends the verification shadow to SP. The SP holder put the film on smartphone screen, and submit this SP with a display of QR code to BD for authentication. Another application scenario of QR-code-based authentication is shown in Fig. 2(b). User may have various films in pocket. VS can send verification shadow to any check in counter. For various occasions, the user adopts a different film.

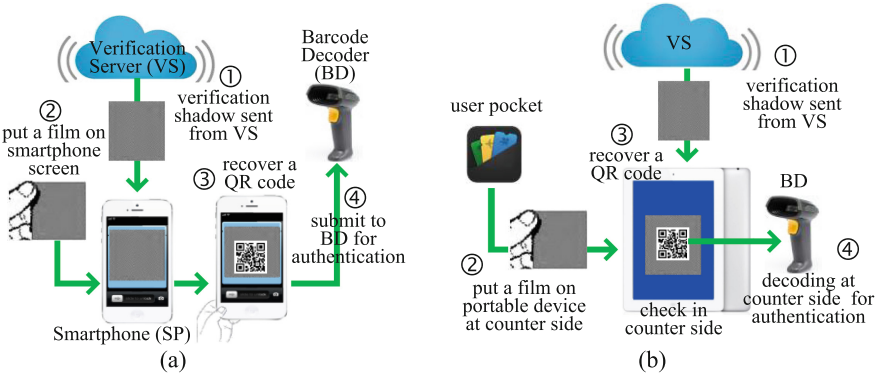

Fig. 2. QR-code-based authentication scheme (a) application scenario 1: verification shadow is sent to smartphone (b) application scenario 2: verification shadow is sent to the check in counter.

As we already mentioned, the reconstructed pixels of VCS by stacking a film are not real binary which may cause errors. If the distorted 2D barcode (the stacked result of VCS) is beyond the error-tolerant ability of QR code. The barcode decoder cannot successfully decode this barcode and the authentication fails. In this paper, we propose two solutions. The first approach is to intentionally distribute errors among a QR code according to Reed-Solomon (RS) code. Another approach is to design a new-type subpixel from the notion of continuous-tone VCS [14], to enhance the image quality of QR code. These two approaches are briefly described below.

Using Error Correcting Capability of RS Code: QR code adopts the RS code for error control coding, and it has a strong error correcting ability. There are four fault-tolerance levels of L, M, Q, H, with fault-tolerance of 7 %, 15 %, 25 % and 30 %, respectively. Obviously, the higher fault-tolerance level is, the lesser embedding data we have. Figure 3 is an example of QR code (Model 2 Version 5-H), where D blocks are the data blocks, E blocks are the parity digits for D blocks via RS code encoding. The QR code in Fig. 3 has four RS codes: two (33, 11, 11) RS codes and two (34, 12, 11) RS codes. The error correction capability are 11 for all four codes, one has the code length 33 (information length 11), and the other has the code length 34 (information length 12). For this example, QR code has fault-tolerance of 11/33 or 11/34 about 30 %.

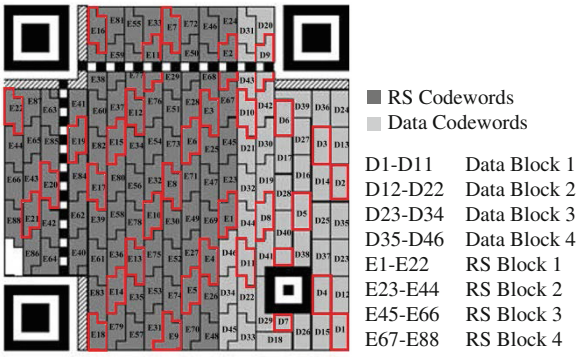

Fig. 3. Model 2 version 5-H QR Code. (Color figure online)

We study how to distribute these errors, and make errors being within the error tolerance of RS code. Here, we use a simple example (Example 1) to show the strategy of dispersing errors. As shown in Fig. 3, the red color implies the first (33, 11, 11) RS code with data blocks D1-D11 and parity blocks E1-E22. Suppose that we use perfect black VCS (PBVCS), which has the 100 % blackness for the black secret pixel but has the distorted white secret pixel. For this case, this 2D barcode can decode the correct black dot, while the decoded result of white dot may be wrong.

In Example 1, we explain how to ensure that some of the white dot in 2D barcode can be correctly decoded. However, at this time, the black dot may be not recovered. We hope that the errors can be uniformly dispersed in these four RS codes, such that the errors of each RS code does not exceed 11 (i.e., within the error tolerance), and finally the QR code is decodable.

Example 1: Consider the (2, 2)-VCS in Fig. 1. Because we have 4B for black dot, so the decoding of black dot in QR code is correct, but there might be wrong for decoding the white dot.

Figures 4(a)–(d) show all four cases of the middle secret pixel is white: (□□□), (□□■), (■□□) and (■□■). Consider the case in Fig. 4(a), we can adjust the subpixel of upper left corner in the right 4-pixel block to the upper right corner (the adjusted

subpixel denoted as the gray color). This adjustment ensures the correct decoding of the middle pixel. At this time, left and right dots also has chance of decoding correctly. Figures 4(b) and (c) illustrates the adjustments of (□□■) and (■□□). For the case that the left and right are all black (■□■), we can only choose one side to change black secret pixel to white secret pixel. As shown in Fig. 4(d), the red subpixels imply changing from black color to white color. In this case, the right dot will be wrongly decoded. These adjustments are only the horizontal adjustments. To precisely disperse errors, we should consider the comprehensive adjustment with 8 around subpixels P1-P8, as shown in Fig. 4(e). In fact, we can further improve the adjustment by using the black matrix $B_1 = \begin{bmatrix} 1100 \\ 0110 \end{bmatrix}$ with the black secret pixel 3B1 W. Because 3B1 W is not the perfect black, it may cause decoding errors of some black secret pixels. However, at this time, Fig. 4(d) can be modified to Fig. 4(f), and finally all secret pixels may be correctly decoded.

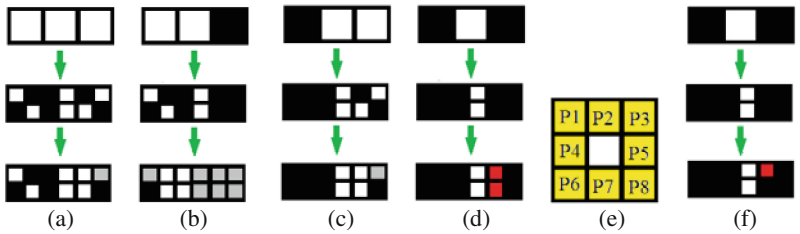

Fig. 4. Adjusting subpixels to ensure the correct decoding of the middle white secret pixel: (a) left and right are all white (□□□) (b) left white and right black (□□■) (c) left black and right white (■□□) (d) left and right are all black (■□■) (e) the comprehensive adjustment (f) the adjustment for the case (■□■) by 3B1 W. (Color figure online)

The adjustment and the choice of fault-tolerance level (Level L, M, Q, H) have great relevance. Both strategies should be completely tested and analyzed to select a best adjustment policies.

Enhancing the Image Quality of QR Code: We adopt the notion of continuous-tone VCS to design a new subpixel structure, to enhance the image quality of the QR code. Here, we use circular subpixel structure (see Fig. 5) to describe the continuous-tone VCS (note: to really implement the continuous-tone VCS, we should use the square structure [14]). Barcode decoders measure the intensity of the light reflected back from the barcode, and determines the grayness of dots. Thus, we can use the inner and outer rings, and add the gray color in Fig. 5, to adjust the grayness of the recovered pixel and ensure that each secret pixel can correctly decoded by barcode decoder.

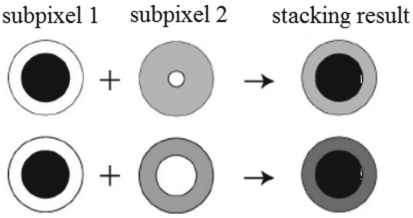

Fig. 5. The concept of the subpixel of continuous-tone VCS.

3.2 Content Based CAPTCHA-like Visual Authentication

In the QR-code-based authentication, the film with a smartphone is a "pass token" like using the Passbook in iPhone. Suppose that, for some reasons, the verifier cannot provide barcode decoder. For the case, we have to authenticate by visually decoding the content of the recovered image. Also, consider the case that adopts QR-code-based authentication in the advertising of electronic commerce by clicking. However, the proposed QR-code-based authentication cannot prevent the click fraud if an attacking software uses the shadow. We adopt the seeing-is-believing property into authentication to address problems of the non-availability of barcode decoder and the anti-bot. The proposed content-based CAPTCHA-like visual authentication is shown in Fig. 6.

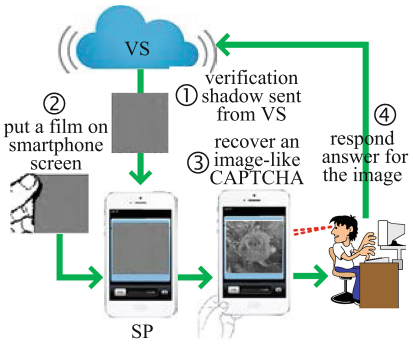

Fig. 6. Content-based CAPTCHA-like visual authentication scheme.

When using CAPTCHA for authentication, users often enter some alphanumeric words. In our content-based CAPTCHA-like authentication, the server sends natural images. Users should respond the correct answer for verification according to the reconstructed image. Because the visual authentication is content based, users have to clearly decode the image. We can use continuous-tone VCS to gain the high-quality gray/colorful image which will be integrated to the content-based authentication. The conventional CAPTCHA can include graphs, sounds, texts, pictures, smart/mathematical query, and even videos. The most popular and simple way of CAPTCHA is the distorted texts. In fact, our content-based CAPTCHA-like visual authentication

Table 2. Query types of the proposed content-based CAPTCHA-like visual authentication.

Query type	Description
Image content identification	Consider the recovered image (a yellow rose) in Fig. 6. Based on the understanding of this image, we can ask the questions gradually, e.g., (i) What is the flower color? (ii) What is the flower? (iii) How many pieces of petals does this flower has?,…, and so on
Face recognition	This is a face image detection test. After receiving a photo from verification server, the user has to click on several face images (e.g., the same person but may be with different hair style, the sketch, or different angle of photo) to solve this face CAPTCHA
Landmark recognition	The same notion of the face recognition, but use the famous scenery all over the world
Smart/Mathematical	Based on the recovered texts, we can ask the questions by smart/mathematical CAPTCHA
Hybrid query	Combine various query types within an image

can also uses this approach. However, this will has the vulnerability that the distorted texts may be recognized by optical character recognition (OCR) software. Here, we adopt content-based challenge response. Table 2 shows some effective query types of the proposed content-based CAPTCHA-like visual authentication.

4 Integration with Various VCSs

The two authentication schemes in Sect. 3, QR-code-based scheme and content-based CAPTCHA-like scheme, are only on the basis of (2, 2)-VCS. The proposed smartphone authentication can be integrated with various VCSs for different applications. In this section, we show two integrations with multi-secret VCS (MVCS) [15] and participant specific VCS (PSVCS) [16], respectively.

Figure 7 only demonstrates the use of MVCS in QR-code based authentication. Of course, the MVCS can also be combined into content-based CAPTCHA-like visual authentication scheme. Suppose that the (2, 2, 2)-MVCS [15] has two shadows: one is the verification shadow S_1 in server and the other shadow S_2 (printed on a film) is kept by smartphone holder. The so-called (2, 2, 2)-MVCS implies that two shadows should be stacked to recover the secret. Two secrets can be recovered from stacking S_1 and S_2, and stacking S_1 and S_2, which S_2 is the image S_2 flipped with 180°. As shown in Fig. 7, we can obtain two QR codes from $Q_1 = (S_1 + S_2)$ and $Q_2 = (S_1 + S_2)$, and can login to various databases.

Consider another application scenario, multi-server environment, which various servers can collaborate to provide different services. Here, we adopt a (t, k, n)-PSVCS [16] to design a multi-serve authentication scheme. The so-called (t, k, n)-PSVCS, where $t \leq k \leq n$, needs t specific shadows and other $(k\text{-}t)$ shadows to decode the secret image. Here we use an example of a digital content service (providing software, music, movies,…, ad etc.) to describe a multi-server system. When considering the security and the load balancing, we share the digital contents in cloud servers by secret

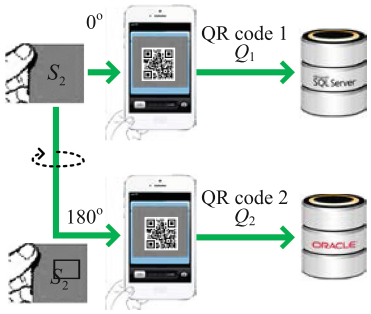

Fig. 7. Integrating (2, 2, 2)-MVCS into QR-code-based authentication for logining to various databases.

sharing and distribute them into multiple service servers (SSs). In order to protect these digital media contents and manage their digital rights, we have one or more ticket grant sever (TGS). If the user wants to login the digital content service system by his pass token (the film with his smartphone), he needs all TGSs and some SSs to get the access permission. Suppose that this digital content service system has ($t-1$) TGSs, (n-t) SSs, and need (k-t) SSs agreed to provide services. The (t, k, n)-PSVCS satisfies this conditions: t specific shadows (one film kept by smartphone holder and ($t-1$) shadows in TGS), and other ($k-t$) common shadows (($k-t$) SSs).

The procedure of multi-serve authentication can be implemented by either QR code based or content based. Figure 8 is an example that there are total 9 entities including one TGS (Server 1), seven SSs (Server 2–Server 8), and one user. The authentication of this multi-server system can be accomplished by the (t, k, n)-PSVCS, where $t = 2$, $k = 5$ and $n = 9$. Suppose that the shadows of Server i, $1 \leq i \leq 8$, is S_i, and that the film kept by smartphone holder is S_h. For recovering the secret information, S_1 and S_h are necessarily required and the total threshold should be five. As shown in Fig. 8, Case ① can login successfully because $\{S_1, S_2, S_3, S_4, S_h\}$ has S_1 and S_h, and the threshold is also five. However, other two cases fail. In Case ②, although $\{S_2, S_3, S_5, S_6, S_h\}$ achieves the threshold, S_1 is not involved. For Case ③, S_1 and S_h are involved but $\{S_1, S_3, S_4, S_h\}$ does not achieve the threshold.

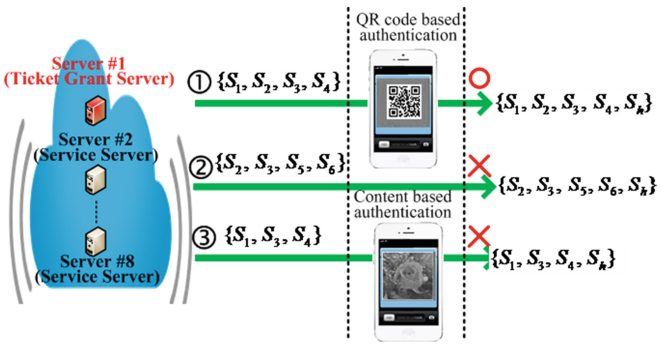

Fig. 8. Multi-server system authentication scheme.

5 Comparison and Discussion

There are some researches on authentication using VCS. A comparison between our authentication schemes and other VCS-based authentication schemes [6, 10–12] is listed in Table 1. All these schemes adopt the stacking-to-see property of VCS to achieve visual human-verifiable authentication. The schemes in [10, 11] use extended VCS (EVCS) instead of VCS. The EVCS has the meaningful cover image on shadow and give no sign that some secret data has been hidden. Our scheme and the schemes in [6, 12] have noise-like shadows. The schemes in [6, 10–12] use the simple 2-out-of-2 scheme. Our multi-server authentication scheme uses (t, k, n)-PSVCS for multi-server environment.

The major difference between our research and others is that we propose a novel technology on smartphone for authentication together with a new VCS for continuous-tone images. Our research brings the following contributions. (1) The authentication schemes can avoid the inconvenience of using password everywhere in modern digital life. The technology brings convenience and benefits for most people, because it only requires users to stack a low-cost small film onto smartphones. (2) The authentication schemes can resist any malicious attacks by crackers and the man-in-middle attacks. It is secure for multiple applications including online banking and mobile ticketing. So, the technology has a lot of business opportunities. (3) Image quality assessment for VCS can provide new criteria for image quality. The assessment is important for evaluating and controlling the image quality, because there exist trade-offs among several indices of image quality in VCS. (4) A new continuous-tone VCS may achieve better image quality than conventional VCS. It is crucial for VCS applications running on smartphones, because their display areas are very limited. (5) This technology, a low-cost, credit-card sized film stuck to smartphone, has the competitive advantages on “size” and “price”. (6) The shadow image can be easily printed to various materials, and integrated into different products. So, the technology will have the large commercial value (Table 3).

As we know, there are some patents of applying VCS on smartphones. Please refer [17, 18]. Recently, the team of Liverpool Hope University announces an authentication scheme via smartphone by using VCS [17]. Also, their technology has been patented in the UK and USA and has patents pending in Canada and Europe. However, their approach is different to us. The shadow of user is sent to an APP and stored in the smartphone. Afterwards, users use this shadow to stack the received image from the server to reveal the secret code. The approach in [18] seems similar to our approach, i.e., printing shadow on a soft film. But, it does not combine 2D barcode, content based authentication, and multi-server environment. The only same idea of [18] as our approach is to print the shadow on a film. This technology [18] is now announced for sale at TYNAX website, which is a global patent and technology exchange website.

Table 3. A comparison between our authentication schemes and other VCS-based authentication schemes.

	Scheme in [6]	Scheme in [10]	Scheme in [11]	Scheme in [12]	Our scheme
VCS	(2, 2)-VCS	(2, 2)-EVCS	(2, 2)-EVCS	(2, 2)-VCS	(2, 2)-VCS (t, k, n)-PSVCS[#1]
Application scenario	Bank	Bank	Website	ID-card	Smartphone
Server/Client shadow	1/1	1/1	1/1	1/1	1/1 (n–1)/1[#1]
Secret image	Password	Signature	Password	ID photo	QR code[#2] Natural image[#3]
Cover image	NO	YES	YES	NO	NO
Involved servers	1	1	1	1	1 (k–1)[#1]
Different privilege of server	NO	NO	NO	NO	NO YES[#1]
Authentication type	Visual auth.	Visual auth.	Visual auth.	Visual auth.	Barcode auth.[#2] Visual auth.[#3]

#1 multi-server authentication scheme. #2 QR-code-based authentication scheme.
#3 content-based CAPTCHA-like visual authentication scheme.

6 Conclusion

In this paper, several authentication schemes, QR-code based authentication, content-based CAPTCHA-like visual authentication and multi-server system authentication, are designed. Meantime, we also study methods to improve image quality of VCS, on which we develop a low-cost, credit-card sized film stuck to smartphone screen. On the basis of this soft film, a simple, cheap, efficient and secure authentication can be achieved. Additionally, our technology can be combined with existing VCSs to achieve more comprehensive application scenarios.

Acknowledgments. This work was supported in part by Ministry of Science and Technology, Taiwan, under Grant 104-2918-I-259-001 and 104-2221-E-259-013.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Surekha, B., Swamy, G., Rao, K.S.: A multiple watermarking technique for images based on visual cryptography. Int. J. Comput. Appl. **1**(11), 77–81 (2010)
3. Monoth, T., Anto, P.B.: Tamperproof transmission of fingerprints using visual cryptography schemes. Procedia Comput. Sci. **2**, 143–148 (2010)
4. Weir, J., Yan, W.: Resolution variant visual cryptography for street view of google maps. In: Proceedings of ISCAS, pp. 1695–1698 (2010)
5. Yang, C.N., Chen, T.S., Ching, M.H.: Embed additional private information into two-dimensional barcodes by the visual secret sharing scheme. Integr. Comput. Aided Eng. **13**(2), 189–199 (2006)
6. Naor, M., Pinkas, B.: Visual authentication and identification. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 322–336. Springer, Heidelberg (1997)
7. McCune, J.M., Perrig, A., Reiter, M.K.: Seeing-is-believing: using camera phones for human-verifiable authentication. In: Proceeidngs of IEEE Symposium on Security Privacy, pp. 110–124 (2005)
8. Yang, C.N., Chen, T.S.: Security analysis on authentication of images using recursive visual cryptography. Cryptologia **32**(2), 131–136 (2008)
9. Borchert, B., Reinhardt, K.: Applications of visual cryptography. In: Chapter 12 of Visual Cryptography and Secret Image Sharing, Boca Raton, FL. CRC Press/Taylor and Francis (2011)
10. Jaya, Malik, S., Aggarwal, A., Sardana, A.: Novel authentication system using visual cryptography. In: Information and Communication Technologies (WICT), pp. 1181–1186 (2011)
11. Goel, M.B., Bhagat, V.B., Katankar, V.K.: Authentication framework using visual cryptography. Int. J. Res. Eng. Technol. **2**, 271–274 (2013)
12. Ratheesh, V.R., Jogesh, J., Jayamohan, M.: A visual cryptographic scheme for owner authentication using embedded shares. Indian J. Comput. Sci. Eng. **5**, 190–194 (2014)
13. Weir, J., Yan, W.: Authenticating visual cryptography shares using 2D barcodes. In: Shi, Y. Q., Kim, H.-J., Perez-Gonzalez, F. (eds.) IWDW 2011. LNCS, vol. 7128, pp. 196–210. Springer, Heidelberg (2012)
14. Nakajima, M., Yamaguchi, Y.: Enhancing registration tolerance of extended visual cryptography for natural images. J. Electron. Imaging **13**, 654–662 (2004)
15. Chen, S.K., Lin, S.J., Lin, J.C.: Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. J. Vis. Commun. Image Representation **21**, 900–916 (2010)
16. Yang, C.N., Sun, L.Z., Yan, X., Kim, C.: Design a new visual cryptography for human-verifiable authentication in accessing a database. J. Real-Time Image Process. (2015). doi:10.1007/s11554-015-0511-9
17. Liverpool and Sefton Chambers of Commerce. http://www.liverpoolchamber.org.uk/article.aspx/show/5641
18. Global Patent & Technology Exchange. http://www.tynax.com/listing/4027