2015

A visual one-time password authentication scheme using mobile devices

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Man Ho Au
Hong Kong Polytechnic University, aau@uow.edu.au

Ari Moesriami Barmawi
Telkom University

Publication Details

Chow, Y., Susilo, W., Au, M. Ho. & Barmawi, A. Moesriami. (2015). A visual one-time password authentication scheme using mobile devices. In L. C. K. Hui, S. H. Qing, E. Shi & S. M. Yiu (Eds.), Proceedings of the 16th International Conference on Information and Communications Security (ICICS 2014) (pp. 243-257). Switzerland: Springer International Publishing.

A visual one-time password authentication scheme using mobile devices

Abstract
The use of passwords for user authentication has become ubiquitous in our everyday lives. However, password theft is becoming a common occurrence due to a variety of security problems associated with passwords. As such, many organizations are moving towards adopting alternative solutions like one-time passwords, which are only valid for a single session. Nevertheless, various one-time password schemes also suffer from a number of drawbacks in terms of their method of generation or delivery. This paper presents the design of a challenge-response visual one-time password authentication scheme that is to be used in conjunction with the camera on a mobile device. The main purpose of the proposed scheme is to be able to send a challenge over a public channel for a user to obtain a session key, while safeguarding the user's long-term secret key. In this paper, we present the authentication protocol, the various design considerations and the advantages provided by the scheme.

Disciplines
Engineering | Science and Technology Studies

Publication Details
Chow, Y., Susilo, W., Au, M. Ho. & Barmawi, A. Moesriami. (2015). A visual one-time password authentication scheme using mobile devices. In L. C. K. Hui, S. H. Qing, E. Shi & S. M. Yiu (Eds.), Proceedings of the 16th International Conference on Information and Communications Security (ICICS 2014) (pp. 243-257). Switzerland: Springer International Publishing.

A Visual One-Time Password Authentication Scheme using Mobile Devices

Yang-Wai Chow[1], Willy Susilo[1], Man Ho Au[2] and Ari Moesriami Barmawi[3]

[1] Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia
{caseyc, wsusilo}@uow.edu.au,
[2] Department of Computing, Hong Kong Polytechnic University, Hong Kong
csallen@comp.polyu.edu.hk,
[3] School of Computing, Telkom University, Indonesia
mbarmawi@melsa.net.id

Abstract. The use of passwords for user authentication has become ubiquitous in our everyday lives. However, password theft is becoming a common occurrence due to a variety of security problems associated with passwords. As such, many organizations are moving towards adopting alternative solutions like one-time passwords, which are only valid for a single session. Nevertheless, various one-time password schemes also suffer from a number of drawbacks in terms of their method of generation or delivery. This paper presents the design of a challenge-response visual one-time password authentication scheme that is to be used in conjunction with the camera on a mobile device. The main purpose of the proposed scheme is to be able to send a challenge over a public channel for a user to obtain a session key, while safeguarding the user's long-term secret key. In this paper, we present the authentication protocol, the various design considerations and the advantages provided by the scheme.

Keywords: Authentication, one-time password, mobile device, visual cryptography

1 Introduction

In this day and age, passwords are widely used in everyday life for user authentication on the Internet. Despite having been used for many years, text passwords are still the most dominant form of web authentication due to its convenience and simplicity [26]. However, the use of passwords has been shown to be plagued by various security problems [2, 3]. In addition, over the years many security attacks, such as spyware and phishing attacks, have been used to extract sensitive information from computers, emails, fraudulent websites, etc., resulting in password theft becoming a common occurrence.

For this reason, many business companies and organizations are moving toward adopting alternative solutions to the traditional static password approach.

Static password approaches are particularly vulnerable as these passwords can easily be stolen by an adversary via a variety of means (e.g. keyloggers, phishing attacks, Trojans, etc.), and used without the password owner's knowledge. This has led to the increasing popularity of One-Time Password (OTP) schemes, where a password is only valid for a single session. For example, Google's authentication framework using two-step verification employs an OTP approach [7]. In Google's two-step verification, the first step involves the user using the traditional username and static password authentication. In the second step, the user will be asked for a six-digit verification code (the OTP) which the user can obtain through a number of different means, for example, via a Short Message Service (SMS) text message, a voice call to a preregistered phone number, a list of pre-generated one-time codes, or an offline application pre-installed on the user's smartphone [7].

There are a number of common ways in which OTPs can be generated and distributed. However, it has been contended that a number of these methods suffer from various drawbacks. For instance, it has been observed that sending an OTP via SMS to a user's mobile phone cannot be considered to be secure [18]. For one thing, the security of SMS OTP relies on the confidentiality of the SMS messages and the security of the cellular networks, which cannot be guaranteed as there are already several potential attacks that can be conducted on these services. Furthermore, specialized mobile phone Trojans have been created that compromise the security of SMS OTP approaches [18]. Moreover, this approach can be problematic to use if the user is in a location with poor mobile phone reception.

An approach that is commonly used by banks and financial institutions, is to supply the user with a security token which generates OTPs. One technique to generate OTPs on a security token is to use a time dependent pseudo-random algorithm. This approach relies on accurate time synchronization between the token and the authentication server, as the OTPs generated using this approach are only valid for a short period of time. As such, this approach suffers from synchronization issues and the potential for clock skew [23]. Another approach of generating OTPs on security tokens is to use a one-way function in the form of a hash chain. However, hash chains are known to have storage and computational complexity issues [24].

In this paper, we propose a challenge-response visual OTP authentication scheme that uses the camera on a mobile device to obtain the OTP. The purpose of the scheme is to be able to send a challenge over a public channel for a user to obtain a session key, while safeguarding the user's long-term secret key. Our approach is based on the concept of visual cryptography and as such does not rely on mobile phone network reception, or having to establish a network link between a computer and a mobile phone. This paper presents the authentication protocol along with various practical issues that had to be considered in the design of the visual OTP scheme.

Our Contribution. This paper presents the design of a visual one-time password authentication scheme. The proposed scheme is a challenge-response approach that relies on a camera on a mobile device to receive the challenge and to present the response on the mobile device's display. The advantage of this approach is that it does not suffer from common OTP issues concerning mobile phone reception, hash chain complexities or time synchronization mechanisms. In addition, unlike SMS-based approaches, our approach is not restricted to mobile phones and can be used on any mobile device with a camera and display, including tablet computers. In the proposed scheme, the challenge can even be sent on printed media instead of via electronic means.

2 Related Work

Over the years, researchers have proposed a variety of different authentication approaches. In this section, we review the research in the area of authentication that is relevant to our work.

2.1 Visual Authentication

The notion of using human-computer cryptographic approaches for identification and authentication have been around for many years. These approaches typically rely on a challenge-response mechanism that requires a human user to interact with a computer in some manner in order to perform authentication. For example, Matsumoto [16, 17] investigated human-computer cryptographic schemes that presented challenges to users in the form of visual images. The approach that was examined in his study relied on the human ability for memorizing and processing to solve the simple challenges. Since then, other researchers and practitioners have also proposed and developed various graphical password schemes. Graphical passwords attempt to leverage human memory for visual information with the shared secret being related to images [1]. This capitalizes on the natural human ability to remember images, which is believed to exceed memory for text [3]. However, graphical passwords are not immune to security attacks. For example, graphical password schemes may suffer from shoulder surfing attacks where credentials are captured through direct observation of the login process, or by recording the process using a recording device [1].

Other schemes that have been proposed in this area are based on using the human visual system to solve the challenge. Naor and Pinkas [19] proposed an authentication and identification approach that is based on visual cryptography. Visual cryptography was introduced by Naor and Shamir [20] as a means of using images to conceal information. The main idea behind visual cryptography is to divide a secret image into a set of shares, each to be printed on a separate transparency. Individually, the shares look like random black and white pixels that reveal no information about the secret image. When the appropriate number of shares are stacked together, the human visual system averages the black and white pixel contributions of the superimposed shares to recover the hidden

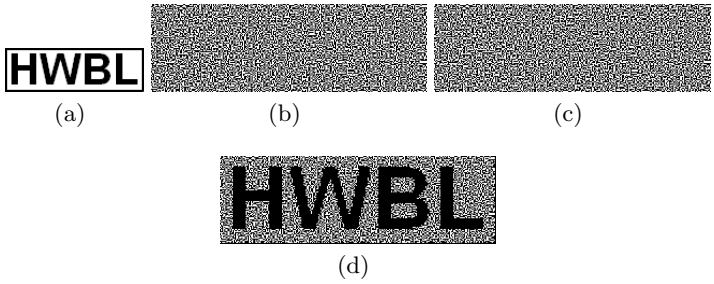

Fig. 1. Example of Naor and Shamir's visual cryptography scheme. (a) Secret image; (b) Share 1; (c) Share 2; (d) Result of superimposing shares 1 and 2.

information. Thus, the concealed information can be decrypted by the human visual system without any need of a computer to perform decryption computations [4]. Figure 1 depicts an example of Naor and Shamir's visual cryptography scheme. The secret image, shown in Figure 1(a), is divided into two shares, which are shown in Figures 1(b) and 1(c) respectively. The secret can be recovered by superimposing the two shares, as shown in Figure 1(d).

In the scheme proposed by Naor and Pinkas [19], the user is required to carry a small transparency, small enough to be carried in a wallet, and the authentication and identification process simply involves the user overlaying the transparency on the message sent by an informant in order to view the concealed information. However, in their scheme, unless the user carries a stack of transparencies, which would be impractical, a single transparency will have to be used for multiple authentication sessions. It has been highlighted that since basic visual cryptography schemes are equivalent to one-time pads, an observer can eventually learn the user's secret by repeated observation [3]. In addition, Naor and Shamir's visual cryptography scheme suffers from the pixel expansion problem, as illustrated in Figure 1, where each pixel in the secret image is split into four sub-pixels in the shares and the recovered image. As such, the shares are four time the size of the secret image.

To overcome a number of drawbacks with this scheme, Tuyls et al. [27] proposed a scheme where every user was to be given a small decryption display. Their approach was similarly based on visual cryptography where the small decryption display was used to replace the need for transparencies. The small decryption display required very limited computing power to perform authentication and security and since the user was required to carry his/her own trusted decryption display, it would be impossible to be contaminated by Trojans or viruses. However, this approach requires the user to use a special authentication device.

A commercially available scheme called PassWindow [22] uses a similar approach where a small transparent display is embedded in an ID card or some form of payment card. The pattern on the transparent display changes periodically based on a pre-generated sequence of patterns. To perform authentication,

the user has to overlay the transparent display of the card over a patterned image sent from the server and to visually identify the digits that form as a result of superimposing the card's display onto the image. However, it should be noted that an image on screen can potentially appear at different sizes depending on the user's display settings. This approach requires that the size of the image that is displayed on screen be exactly the same as the size of the card's transparent display.

2.2 Authentication using a Personal Device

A number of other authentication approaches that have been proposed make use of personal devices that a user usually carries around (e.g. a cellphone). In a study on how to provide a user with authenticated communication when using an untrusted computer, Clarke et al. [5] proposed a method of using a trusted personal device equipped with a camera to monitor the screen of the untrusted computer. All communication is then authenticated by a trusted proxy. This approach is quite costly in terms of computational resources required to monitor the communication.

Mannan and Oorschot [15] proposed a protocol that they called MP-Auth (*M*obile *P*assword *Auth*entication), which uses a mobile device to protect user passwords from easily being recorded. In their approach, the mobile device is assumed to be free from malware as the user will enter the password into the mobile device rather than into an untrusted computer. In another approach proposed by Jeun et al. [11], the user uses an application to store his encrypted password in his smart phone and that application program is used to send the password from the smart phone itself, instead of requiring the user to enter his password via a computer's keyboard.

Phoolproof is another scheme that uses mobile phones for authentication. Phoolproof is a mutual authentication protocol used to prevent phishing using a trusted mobile phone [21]. To use the system, the user must establish a shared secret with the server using an out-of-band channel. This long-term secret is stored on the mobile phone. In order to use this protocol, the mobile phone must establish a secure Bluetooth connection with the web-browser where mutual authentication occurs between the mobile phone and the website.

2.3 One-Time Passwords

To overcome some of the problems associated with static passwords, OTP approaches are increasingly being used for authentication. There are various techniques for generating and distributing OTPs. In addition, several approaches were devised to use OTPs in conjunction with mobile devices.

Paterson and Stebila [23] examined an approach of using OTPs in conjunction with one-time Password Authentication Key Exchange (PAKE) protocols in order to ensure more secure use of OTPs. In a scheme called oPass proposed by Sun et al. [26], a trusted cellphone is used to communicate with the web server (via SMS) and the web-browser (via Wi-Fi or Bluetooth). The user does

not input his password into the web-browser, but rather is required to enter his long-term password into the oPass program which will generate an OTP that will be sent by way of an encrypted SMS to the server.

Mulliner et al. [18] investigated attacks against SMS based OTPs and state that attacks against cellular networks and mobile phones have shown that SMS messages cannot be deemed to be secure. They proposed a virtual dedicated OTP channel inside the mobile phone operating system to secure OTP SMS messages from being intercepted by Trojans by removing these messages from the general delivery process and redirecting them to a special OTP application.

Instead of using a mobile device, Huang et al. [9] proposed a scheme where the OTP is delivered via an instant messaging service. This approach assumes that the website which adopts the OTP authentication method must join an instant messaging network and use the network to communicate with the users.

3 Model and Definition of the Visual One-Time Password Authentication System

In this section, we will first define the visual one-time password authentication system and its scenario, and then we will propose a visual authentication protocol. We extend this definition from the visual authentication scheme proposed by Naor and Pinkas [19].

Visual OTP Authentication Scenario
Without losing generality, we assume that there are three entities involved, namely H (Henry), S (Sandra) and an adversary E (Evan). H is a human and therefore H has human visual capabilities. The purpose of the visual OTP authentication system is to enable Sandra to attest whether Henry is present in the protocol in the presence of Evan. Note that Evan can observe the channel used between Henry and Sandra. The security parameter k is involved, such that storage capacities and computing power of Sandra and Evan are polynomial in k.

There are two main stages in the visual OTP authentication scenario. The first stage is the initialization stage, where Sandra can communicate with Henry in an offline private initialization channel, which is inaccessible to Evan. In the second stage, Sandra communicates with Henry via a public channel, in which Evan can also access.

In the first stage, Sandra issues a long-term secret key, lk, to Henry, where its size is polynomial in the security parameter k. In the second stage, Sandra tests to ensure that Henry has acquired lk by producing a random number r, which is sent via a public channel. Henry will then construct a shared visual secret, which is a function of lk and r. For simplicity, this visual share is denoted as S_1. Subsequently, Sandra produces a short-term secret key, sk, and constructs its visual version, S_{sk}. Then, Sandra will construct another visual share S_2, where $S_2 = S_{sk} - S_1$ (an example of an algorithm that can be used to generate S_1 and S_2 is provided in Algorithm 1 below). Subsequently, S_2 is presented to Henry via

a public channel. Evan has access to the public channel, and therefore, he has access to both r and S_2. Nevertheless, Evan does not have access to S_1. Using his visual observation capability, Henry can acquire the short-term key, sk, from S_1 and S_2.

Visual OTP Authentication Protocol
S would like to communicate to H to test whether H can reproduce a short-term secret key, sk, in the presence of an adversary E.

- S chooses a random r.
- S generates the short-term key sk and its visual representation S_{sk}.
- S produces the first share S_1, which is a function of lk and r.
- S computes the second share S_2, which is computed from $S_{sk} - S_1$.
- S sends (r, S_2) to H via a public channel.
- H needs to reproduce S_1 from lk and r.
- H uses his visual capability to acquire S_{sk} from S_1 and S_2, and hence, obtains sk.

We note that the public channel is accesible to E. In addition, only S can generate a valid S_2. E will not be able to generate a valid S_2 without knowledge of lk.

Definition 1. Security. *A visual OTP authentication protocol is called* secure *if E cannot retrieve sk after observing the public channel used by S and H to communicate.*

4 Proposed Visual OTP Scheme

4.1 Design

The overall design of the proposed visual OTP scheme is described as follows.

Initialization Stage. H registers with S, in which S will issue a long-term secret key, lk, which has a polynomial size in the security parameter k. lk will be transmitted to H via a secure and authenticated channel. In practice, S can make use of either a traditional public key cryptography (assuming H is equipped with a public key) or an identity-based encryption (assuming the identity of H is known - in a smart phone scenario, this could be via the phone's International Mobile Station Equipment Identity (IMEI) or phone number).

Challenge-Response Stage. In this stage, S selects a random number r, which has a polynomial size in the security parameter k. Then, S will conduct the following:

- Produce a Quick Response (QR) code that contains r, QR_r.
- Generate a short-term secret key sk, and its visual representation S_{sk}.
- Generate the first share S_1, which is derived from $lk||r$, where $||$ denotes concatenation.

- Generate the second share $S_2 = S_{sk} - S_1$.
- Present QR_r and S_2 to H via a public channel.

Upon receiving the challenge (QR_r, S_2), H conducts the following:

- Scan the QR code to retrieve r.
- Use the long-term secret key, lk and r to produce S_1.
- Use H's visual capability to retrieve sk from S_1 and S_2.
- Output sk.

Note that the value of sk is obtained visually and is never stored anywhere.

Figure 2 depicts an example of a practical scenario where the visual OTP scheme can be implemented for conducting an online transaction. The figure gives an overview of the communication between the different components involved in the overall process. In the scenario, the user must first register his mobile device with the authentication server via a secure private channel. The server will in turn generate lk and send this to the user's mobile device. Registration only happens once for the server and mobile device to establish a long-term secret key. Subsequently, whenever the user initiates an online transaction from a web-browser, the server will generate and send (QR_r, S_2) (i.e. the challenge) which will be displayed on the web-browser. Upon receiving (QR_r, S_2), the user will use the camera on his mobile device to scan QR_r. With the value of lk and r, the user's mobile device will be able to generate S_1. On the mobile device's display, S_1 will be overlaid on S_2 to produce S'_{sk} (i.e. the visual reconstruction of S_{sk} on the mobile device's display), and the user will be able to visually obtain sk (i.e. the response/OTP). Only the server can generate a valid S_2, and only the user can obtain sk using S_1 which is generated on the mobile device.

4.2 Practical Issues

In the proposed scheme, r has to be sent to H over a public channel. While it is not necessary to encode and transmit r within a QR code, we find that this is the most appropriate and convenient method of delivery. The QR code is a two-dimensional code that was invented by the company Denso Wave [6]. These days, QR codes are ubiquitous on the Internet and the information contained within a QR code can easily be scanned by a mobile device with a camera. In addition, QR codes have a inbuilt error detection and correction mechanism that can be used to correctly decode corrupted QR codes, which may contain certain errors. Furthermore, QR codes contain a number of patterns to determine rotational orientation and alignment. Since (QR_r, S_2) is sent to H as a single image, QR_r can be used to facilitate the alignment of S_1 and S_2.

It is well known that traditional visual cryptography suffers from the alignment problem, in that when stacking shares, it is difficult to align the shares [14, 30]. Practical approaches typically suggest the use of some reference frame to align the transparencies [19]. However, unlike traditional approaches that use physical transparencies or tokens, our approach relies on the use of a mobile

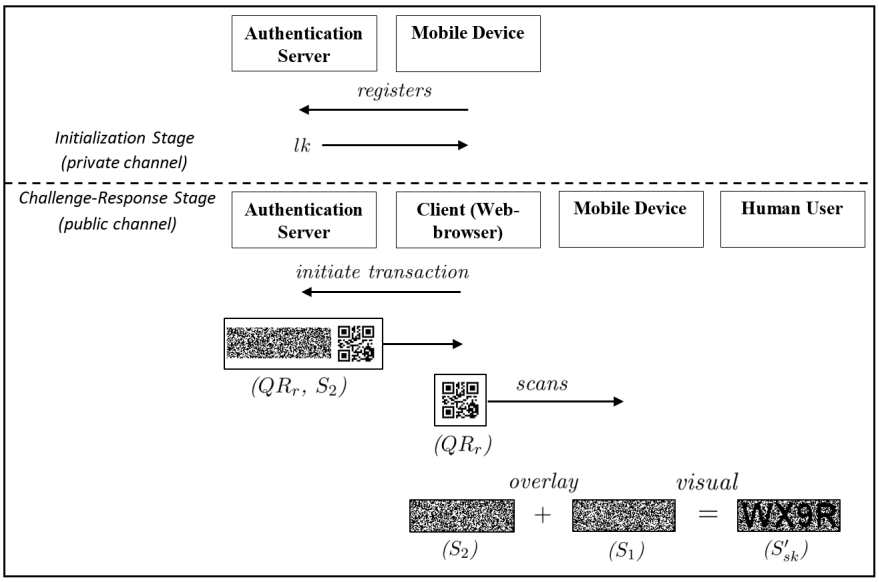

Fig. 2. Overview of the communication between the various components in the visual OTP scheme.

device like a smart phone or a tablet. As such, using the camera's video stream to capture (QR_r, S_2), this can be used in conjunction with image processing techniques to overlay S_1 over S_2. This is akin to techniques using in augmented reality to overlay virtual content onto elements of the real world [28]. Adopting this method will allow the mobile device to appropriately scale and rotate S_1 in order for it to align with S_2.

Another problem with traditional visual cryptography when displaying a share on a computer screen and trying to place the corresponding share, which is printed on a transparency, on top of the screen, is that monitors can differ greatly and the computer can be set to different display settings. As such, the image of the share on screen may not be displayed at the same size as the share printed on the transparency. This will prevent the shares from being correctly superimposed, and thus the secret cannot be recovered. In the approach proposed in this paper, we rely on the mobile device to virtually overlay S_1 over S_2. This means that it does not matter what size S_2 is displayed at, as long as the mobile device can accurately capture the image of S_2, because the mobile device can scale S_1 to the appropriate size. To facilitate this, the size of the squares in S_2's image should not be too small.

As previously shown in Figure 1, traditional visual cryptography suffers from the pixel expansion problem which significantly increases the size of the resulting shares. While there are a number of size invariant visual cryptography schemes like the probabilistic approaches proposed by Ito et al. [10] and Yang [29], these schemes do not produce the ideal visual quality required for the visual OTP.

Therefore, for the purpose of generating S_1 and S_2, a random grid visual cryptography approach was deemed to be the most suitable approach. Random grid visual secret sharing was first proposed by Kefri and Keren [12], and over the years a number of random grid approaches have been investigated [8, 25]. Using a random grid visual cryptography scheme, it is possible to produce shares with no pixel expansion.

In the proposed visual OTP scheme, the shared image S_1 will be generated from $lk||r$ and a pseudo-random number generator. Thus, S_1 is a random grid. S_1 can be used in conjunction with the secret image S_{sk} to generate the corresponding challenge image S_2. Algorithm 1 gives an example of a random grid visual secret sharing method that was adapted from Shyu [25], which can be used in the proposed visual OTP scheme. In this approach, black pixels in S_{sk} are reproduced at 100% in S'_{sk} and white pixels (i.e. transparent pixels) are reproduced at 50%. Figure 3 shows the results of using Algorithm 1 on a secret image. The secret image, shares 1 and 2, along with the reconstructed image are shown in Figures 3(a), 3(b), 3(c) and 3(d) respectively.

Algorithm 1 An algorithm for generating S_1 and S_2 from S_{sk}

```
function GenerateShares(S_sk, lk, r)
    imgWidth ← S_sk width
    imgHeight ← S_sk height
    for i = 1 to imgWidth do
        for j = 1 to imgHeight do
            /* Generate S_1 as a random grid */
            S_1[i, j] ← randomPixel(lk||r) /* randomPixel() outputs 0 or 1 */
            /* Generate S_2 */
            if S_sk[i, j] = 0 then
                S_2[i, j] ← S_1[i, j]
            else
                S_2[i, j] ← ¬S_1[i, j]
            end if
        end for
    end for
end function
```

Another practical issue to consider when implementing the visual OTP scheme is how clearly the user will be able to perceive the OTP in the visual reconstruction of the secret image. For this we should consider the color of the text and the background. There are two possible variations as depicted in Figure 4, where Figure 4(a) shows the reconstructed secret using black text on a white background and Figure 4(b) shows the reconstructed secret using white text on a black background. It has been argued that using white contents on a black background gives rise to better perceived visual quality in the reconstructed image for images with thin lines [13].

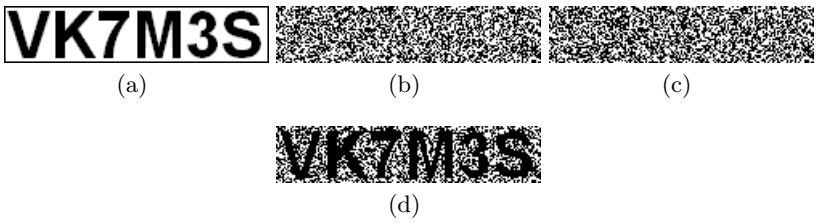

Fig. 3. Random grid visual cryptography approach. (a) Secret image; (b) Share 1; (c) Share 2; (d) Result of superimposing shares 1 and 2.

Fig. 4. Text and background color. (a) Black text on a white background; (b) White text on a black background.

5 Discussion

5.1 Advantages of the Visual OTP Scheme

The fundamental purpose of the proposed visual OTP scheme is to be able to send a challenge over a public channel for the user to obtain a session key that can be used as an OTP, while safeguarding the user's long-term secret key. In this scheme, the user also does not have to remember any passwords.

As mobile devices are ubiquitous in this day and age, the proposed approach does not require the user to carry around a specialized authentication card or device, or a printed list of OTPs. In addition, unlike authentication schemes like SMS OTP based approaches, authentication in the proposed method does not require any form of communication with a mobile phone network. As such, mobile phone network reception is not an issue. This also means that the visual OTP scheme can be applied to any mobile device which has a camera and is not restricted to only be usable on smart phones. The user simply has to install the visual OTP software and register it with the authentication server.

While the OTP can be used to authenticate the user, another feature provided by the scheme is that the user can also verify that the message containing the challenge was sent by a legitimate party. This is because in the proposed scheme, without knowledge of the long-term secret key an adversary cannot generate a valid challenge. This also prevents an adversary from tampering with the challenge image, as changing QR_r will mean that the mobile device will not be able to generate the correct visual pattern (i.e. S_1) to solve the challenge, and changing S_2 will not produce a valid result when overlaying S_1 over S_2. Furthermore, such an event would raise the suspicion of the user, as it would indicate that the challenge may have been tampered with.

Another advantage of the proposed scheme, is that the challenge does not have to be transmitted via electronic means. For example, if a bank wants to send a letter to an individual who has registered with the bank, the bank can send the person a letter with the challenge printed on paper. The person can verify that the letter was indeed sent from the bank (as only the bank can generate a valid challenge) and also receive the OTP which can be used for authentication purposes with the bank.

In other authentication approaches that involve the user having to overlay a transparency or an authentication token on top of another pattern, the size of the patterns have to perfectly match. Otherwise the user will not be able to recover the secret by superimpose the different sized patterns. This is not an issue in the proposed approach as the mobile device will be responsible for scaling and aligning the patterns. Therefore, the challenge can be displayed in any size as long as it can be captured by the mobile device's camera. The mobile device will then use augmented reality techniques to overlay the virtual pattern onto the image of the challenge pattern.

It should be noted that the OTP is obtained by the human user via the visual channel and the OTP is never stored on any device. This prevents malicious software like keyloggers or even software designed to monitor the user's activities from obtaining the OTP. Furthermore, the one-time password is only valid for a single use. Additionally, the video stream on the mobile device will be used to overlay the visual patterns and present this to the user in real-time. If there is any software designed to monitor the user's activities, this will require a huge amount of information to be streamed to the adversary, which will significantly degrade the system's performance and alert the user of suspicious activity.

In addition, unlike traditional graphical passwords, which may suffer from shoulder surfing attacks, this is not an issue in the proposed visual scheme. Shoulder surfing attacks are where an adversary standing behind the user, and possibly even recording the user's interactions, maybe able to observe and detect some pattern in the image or from the user's interactions, which will compromise the security of the visual password. In the proposed visual OTP scheme, the visual pattern generated on the mobile device to solve a challenge can only be used for that particular challenge. The mobile device will generate different visual patterns for different challenges.

5.2 Limitations

In this section we discuss some of the limitations of the propose visual OTP scheme.

As with all visual challenges or passwords, the proposed scheme relies on the human visual system. This means that it does not cater for the blind or visually impaired, and cannot be used by an individual with a visual disability. Another potential disadvantage is that the challenge image will have to be displayed at a certain size in order for the mobile device's camera to be able to accurately capture the information contained within the challenge image. While this is not

seen as a major problem, it may adversely affect the layout or aesthetics of a message, document or webpage.

It should be noted that the proposed scheme does not deal with man-in-the-middle or similar attacks. To handle such attacks, the scheme can be combined with other security protocols that are designed to handle man-in-the-middle attacks. In addition, this approach also does not address the situation where the authentication server is hacked. The server is responsible for its own security and it is assumed that all the necessary security mechanisms are in place.

In the proposed scheme, the mobile device captures the challenge image using its video stream and is responsible for overlaying the virtual image on top of the challenge image. As such, it is assume that the mobile device has the computational capabilities required to process augmented reality techniques in real-time. Additionally, since the mobile device has to be used to visually present the solution to the challenge, a separate means of displaying the challenge has to be employed. In other words, if the user wants to conduct an online transaction via a web-browser, this cannot be done using the mobile device's web-browser as the mobile device itself will have to be used in conjunction with the challenge's display to obtain the OTP. However, this requirement is no different from several other authentication schemes that were previously presented in Section 2 of this paper, which also require the use a web-browser and a separate mobile phone to perform authentication.

6 Conclusion

In this paper, we presented the design of a challenge-response visual OTP authentication scheme. Using this scheme, a challenge is sent to a registered individual, this can be via a web-browser or even printed media, and the user can use the camera and display of his mobile device to obtain the solution to the challenge. This approach can be implemented on a variety of mobile devices, such as mobile phones and tablets, with the main requirement being that the device must have a camera. The challenge itself can be transmitted over a public channel without the threat of it being compromised by an adversary, as the adversary can neither correctly generate nor solve the challenge. As such, the scheme does not suffer from the common issues affecting the generation and delivery of OTPs such as mobile phone reception, hash chain complexities or time synchronization mechanisms. In addition, this scheme does not suffer from security issues like shoulder surfing attacks or keyloggers, as the mobile device will generate the specific visual pattern required to solve a particular challenge and will generate a different visual pattern when presented with a different challenge.

References

1. R. Biddle, S. Chiasson, and P. C. van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19, 2012.

2. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE Symposium on Security and Privacy*, pages 553–567. IEEE Computer Society, 2012.
3. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Technical Report 817, University of Cambridge Computer Laboratory, 2012.
4. Y.-W. Chow, W. Susilo, and D. S. Wong. Enhancing the perceived visual quality of a size invariant visual cryptography scheme. In T. W. Chim and T. H. Yuen, editors, *ICICS*, volume 7618 of *Lecture Notes in Computer Science*, pages 10–21. Springer, 2012.
5. D. E. Clarke, B. Gassend, T. Kotwal, M. Burnside, M. van Dijk, S. Devadas, and R. L. Rivest. The untrusted computer problem and camera-based authentication. In F. Mattern and M. Naghshineh, editors, *Pervasive*, volume 2414 of *Lecture Notes in Computer Science*, pages 114–124. Springer, 2002.
6. Denso Wave Incorporated. QRcode.com, http://www.qrcode.com/en/.
7. E. Grosse and M. Upadhyay. Authentication at scale. *IEEE Security & Privacy*, 11(1):15–22, 2013.
8. Y.-C. Hou, S.-C. Wei, and C.-Y. Lin. Random-grid-based visual cryptography schemes. *IEEE Trans. Circuits Syst. Video Techn.*, 24(5):733–744, 2014.
9. C.-Y. Huang, S.-P. Ma, and K.-T. Chen. Using one-time passwords to prevent password phishing attacks. *J. Network and Computer Applications*, 34(4):1292–1301, 2011.
10. R. Ito, H. Kuwakado, and H. Tanaka. Image size invariant visual cryptography. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 82(10):2172–2177, 1999.
11. I. Jeun, M. Kim, and D. Won. Enhanced password-based user authentication using smart phone. In R. Li, J. Cao, and J. Bourgeois, editors, *GPC*, volume 7296 of *Lecture Notes in Computer Science*, pages 350–360. Springer, 2012.
12. O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. *Optics Letters*, 12(6):377–379, 1987.
13. F. Liu, T. Guo, C. K. Wu, and L. Qian. Improving the visual quality of size invariant visual cryptography scheme. *J. Visual Communication and Image Representation*, 23(2):331–342, 2012.
14. F. Liu, C. K. Wu, and X. J. Lin. The alignment problem of visual cryptography schemes. *Des. Codes Cryptography*, 50(2):215–227, 2009.
15. M. Mannan and P. C. van Oorschot. Using a personal device to strengthen password authentication from an untrusted computer. In S. Dietrich and R. Dhamija, editors, *Financial Cryptography*, volume 4886 of *Lecture Notes in Computer Science*, pages 88–103. Springer, 2007.
16. T. Matsumoto. Human identification through insecure channel. In D. W. Davies, editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 409–421. Springer, 1991.
17. T. Matsumoto. Human-computer cryptography: An attempt. *Journal of Computer Security*, 6(3):129–150, 1998.
18. C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert. Sms-based one-time passwords: Attacks and defense - (short paper). In K. Rieck, P. Stewin, and J.-P. Seifert, editors, *DIMVA*, volume 7967 of *Lecture Notes in Computer Science*, pages 150–159. Springer, 2013.

19. M. Naor and B. Pinkas. Visual authentication and identification. In B. S. K. Jr., editor, *CRYPTO*, volume 1294 of *Lecture Notes in Computer Science*, pages 322–336. Springer, 1997.
20. M. Naor and A. Shamir. Visual cryptography. In *EUROCRYPT*, pages 1–12, 1994.
21. B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In G. D. Crescenzo and A. D. Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2006.
22. PassWindow. http://www.passwindow.com/.
23. K. G. Paterson and D. Stebila. One-time-password-authenticated key exchange. In R. Steinfeld and P. Hawkes, editors, *ACISP*, volume 6168 of *Lecture Notes in Computer Science*, pages 264–281. Springer, 2010.
24. Y. Sella. On the computation-storage trade-offs of hash chain traversal. In R. N. Wright, editor, *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 270–285. Springer, 2003.
25. S. J. Shyu. Image encryption by random grids. *Pattern Recognition*, 40(3):1014–1031, 2007.
26. H.-M. Sun, Y.-H. Chen, and Y.-H. Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE Transactions on Information Forensics and Security*, 7(2):651–663, 2012.
27. P. Tuyls, T. A. M. Kevenaar, G. J. Schrijen, T. Staring, and M. van Dijk. Visual crypto displays enabling secure communications. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *SPC*, volume 2802 of *Lecture Notes in Computer Science*, pages 271–284. Springer, 2003.
28. D. Wagner and D. Schmalstieg. Making augmented reality practical on mobile phones, part 1. *IEEE Computer Graphics and Applications*, 29(3):12–15, 2009.
29. C.-N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4):481–494, 2004.
30. C.-N. Yang, A.-G. Peng, and T.-S. Chen. Mtvss: (m)isalignment (t)olerant (v)isual (s)ecret (s)haring on resolving alignment difficulty. *Signal Processing*, 89(8):1602–1624, 2009.