# A NOVEL ONE-TIME PASSWORD MUTUAL AUTHENTICATION SCHEME USING BIOMETRICS-BASED KEY AND VISUAL SECRET SHARING

**[1]WEI-BIN LEE, [2]YU-TING LIN, [3]MIN-HSUAN TSAI, [4]HSING-BAI CHEN**

[1,2,3]Department of Information Engineering and Computer Science, Feng Chia University, Taiwan, R.O.C.

[4]Hospital and Social Welfare Organizations Administration Commission, MOHW,Taiwan, R.O.C.

E-mail: wblee@fcu.edu.tw, yoyo21220@gmail.com.tw, rjamwxede@hotmail.com

**Abstract-** Most websites will askfor user identification and verify the password for authentication. Whena user is away from home or office and needs to use a public computer,a static password is dangerousto use because it may be cracked, guessed, or stolen. It implies that a dynamic password instead of static one should be employed in a public computer. A sensitive key tokenused to generate the dynamic password. This attracts attackers' attention and increases the cost of maintaining thetoken. In addition, it will be not secure that the sensitive token is used in an untrusted computer to generate a dynamic password.In this paper, anovel one-time passwordmutual authentication scheme is proposed to remedy these problems.

**Keywords-** Authentication, One-Time Password, Visual Secret Sharing, Biometric

## I. INTRODUCTION

Public computers in libraries, hotels, Internet cafes, and airports are vulnerable to the possibility of having been installed with malware that records every keystroke and then sends this information back to the thief. One golden rule is never to type a credit card number while using any public computer.However, rules can't always be followed.Sometimes people simply have to use a public computer for some reason. A lot of tips can help users improve their security when using a public computer, and protecting their passwords is the most critical. A dynamic password is better than static one because it is automatically revoked after it is compromised by being cracked, guessed, or stolen.

A one-time password (OTP) can be generated using numerous techniques. Some researches use software such as instant messaging (IM) [10] or e-mail [15]. However, the computer itself may be cracked, attacked.

Other researchers usea device to generate anOTPsuch assmart-card-based [1][14]or proprietary- tokens-based OTP schemes, e.g., RSA SecurID [2], Authenex A-Key Token [16], and SafeNet etoken pass [17].Carrying tokes such as RSA token or smart card will make the user burden.

Most studies have opted to use asmartphonefor minimizing the equipment needed and becausea large customer-base already owns a smartphone.According to a report by venture capital firm KPCB, 45% of smartphone users access the internet service [3], and the internet-use growth rate is rising every year. To generatean OTP,thesmartphone uses either a short

message service (SMS) [4][9][11] or a software tool [7][12][13].The SMS sends a message for a high price. Using a software tool can reduce the cost;however, this technique requires the storage and protectionof a token, whichis less secure than having nothing to store. In 2011, Lee et al. proposed the OTP authentication scheme [8]that employs abiometrics-based key to maintain no sensitive token;however, no consideration was given to the fact that the computer may beeasily compromised.

Don't insert the token or key the password into untrusted computer are the better way, but the OTP is generated by combining something. In this paper, we introduce an OTPauthentication scheme that uses abiometrics key to generate a secret sharing image (SSI) for using a public computer.

## II. BACKGROUND

In this section, the related techniques are reviewed respectively as following:

### A. Visual Secret Sharing

In 1995, Naor et al. proposed the visual secret sharing scheme [5],in which an image is separated into two shared images. The first shared image may be selected randomly, andaccording to the original image and the first shared image, each pixel in the second image is selected from the original and the first shared images. If a pixel from the original image is white, the second shared image would have the same pixel as the first one. If the pixel of original image is black, the second shared image would choose a pixel that is complementary to the first shared image. The content in the original image can be identified if the two shared images are then overlapped. Table 1 shows a synopsis of visual secret sharing, and Figure 1 showsthe visual secret sharing model.

| | | |
|---|---|---|
| Original image | □ | ■ |
| Shared image 1 |  |  |
| Shared image 2 |  |  |
| Overlapping image |  | ■ |

**Table 1.Visual secret sharing synopsis**

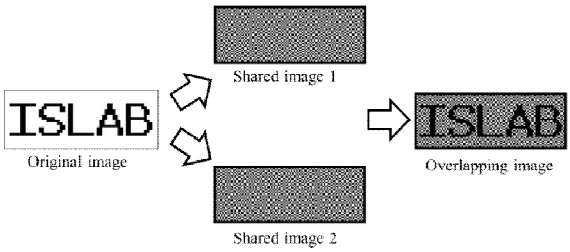


**Figure 1.Visual secret sharing model**

### B. Fuzzy Extractor

In 2008, Dodis et al. proposed the fuzzy extractor to generate a biometric cryptographic key. With the fuzzy extractor, the biometric Bi is the input of the generation function Gen(.), and the outputs are the secret string Ri and the helper string Pi, written as Gen(Bi)→(Ri, Pi). To obtain the secret string Ri, Pi, and Bi'must be generated via the reproduction function Rep(.) if and only if Bi' is close enough to Bi, written as Gen(Bi)→(Ri, Pi). For more detailed information on the fuzzy extractor, please refer to [5].

## III. THE PROPOSED SCHEME

The proposed scheme is composed of two phases: registration and login.The notations used throughout this paper are listed as follows:

| | |
|---|---|
| IDu: | User's personal identification |
| IDs: | Service provider's URL |
| MK: | Server's master key(to be kept secret). |
| □: | XOR. |
| OTP: | One-time password |
| TS: | Time stamp |

| | |
|---|---|
| Bu : | User's biometric. |
| H(.): | Hash function. |
| Gen(.): | Fuzzy extractor generation function whose input is a user's biometric Bu and outputs are a helper string Puand a secret stringRu. |
| Rep(.): | Fuzzy Extractor reproduction functionwhose output is a secret string Ru and inputs are a user's biometric Bu and a helper string Pu. |
| F1(.): | A shadow image generation function whose output is ImgOPS1 and inputs are TS and H(IDu, MK). |
| F2(.): | A shadow image generation function whose output is ImgOPS2 and inputs are ImgOPS1 and ImgOP. |
| FR(.): | A superimposing two-shadow function. |
| Txt2Img(.) | Transform text to image. |
| Dig2Bar(.) | Transform digital to barcode. |

A. Registration Phase

The first time a user visits the service page, he/she must register the server. Assuming that the connection between the user and the server in the registration is in a secure channel,the registration steps are as follows (see Figure 2):

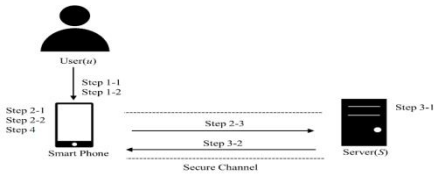


**Figure 2.Registration Phase**

**Step 1.** User inputs registration information.

Step 1-1. Input IDu and IDs on a smartphone.

Step 1-2. Capture biometric (Bu) using a smartphone.

**Step 2.** The smartphone generatesSKu and sends it to the server.

Step 2-1. Generate Ru and Pu using Gen(Bu)→(Ru, Pu).

Step 2-2. Generate SKu = H(IDu, Ru).

Step 2-3. Send registration request, IDu,and SKu to the server.

**Step 3.** The server generatesAK.

Step 3-1. GenerateUK = H(IDu, MK)and AK = UK ⊕SKuafter receiving the request.

Step 3-2. SendAK to the user's smartphone.

**Step 4.** The smartphone storesAK and Pu and finishes the registration phase.

B. Login Phase

When the user wants to access the service from the registered server,the following login steps are performed (see Figure 3):

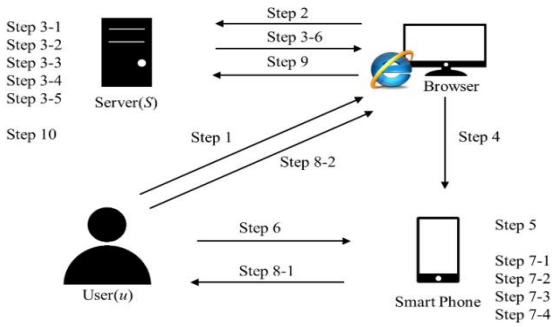


**Figure 3.Login Phase**

**Step 1.** The user inputsIDs and IDu on the browser.

**Step 2.** The browser sendsIDu and login request to the server.

**Step 3.** The server generates a barcode and a shared image.

Step 3-1. GenerateUK = H(IDu, MK)after receiving the request.

Step 3-2. Generate OTPand transform it to image ImgOP =Txt2Img(OTP).

Step 3-3. Generate a shared image ImgOPS1 = F1(UK, TS).

Step 3-4. GenerateImgOPS2 = F2(ImgOPS1, ImgOP).

Step 3-5. Transform TS to barcode ImgBar = Dig2Bar(TS).

Step 3-6. Send shared image ImgOPS2 and barcode ImgBar to the browser (see figure 4).

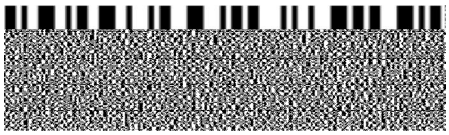

**Figure 4. Barcode ImgBarand shared image ImgOPS2.**

**Step 4.** The user captures these images from the browser using the camera of smartphone (see Figure 5).

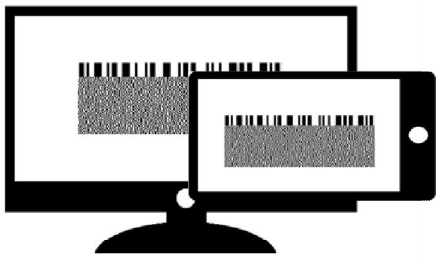

**Figure 5. CaptureImgOPS2 and ImgBar using the camera of smartphone.**

**Step 5.** The smartphone checks whether TS, scanned from ImgBar, exceeds the expiration time or not. If it holds, the following steps will be performed.

**Step 6.** The user captures biometric Bu'by using the smartphone.

**Step 7.** The smartphone overlaps shared images.

Step 7-1. GenerateRu' usingRep(Bu', Pu)→(Ru').

Step 7-2. Generate SKu'= H(IDu, Ru')and UK'= AK⊕SKu'.

Step 7-3. Generate shared image ImgOPS1'= F1(UK', TS).

Step 7-4. Overlap the two shared images ImgOPS1' and ImgOPS2to be captured by the user.

**Step 8.** The user receives anOTP from the overlapped image.

Step 8-1. Get OTPfrom viewing the overlapped image.

Step 8-2. Input OTP on the browser.

**Step 9.** The browser sendsOTP to the server.

**Step 10.** The server checks whether |TS'-TS|<ΔT,where TS' is current system time of the server,is satisfied andverifieswhetherthe receivedOTPis correct or not. If they do not hold, return message "Login Failed" and stop the connection with the user. Otherwise, return message "Login Success" to the user.

## IV. SECURITY ANALYSIS

Hackers can threaten auser's computer environment using a variety of methods, includinga man-in-the-middle attack, a reply attack, phishing, malware injection, and a stolen-verifier attack. In this section, these attacks will be analyzed.

A. Man-in-the-middle attack

By controlling the transmission channel between the server and browser, an attacker may obtain theImgOPS2 and OTP. However, the server checks whether |TS'-TS|<ΔTwhen authenticating. Therefore, the server can detect aman-in-the-middle attack.

B. Reply attack

Byeavesdroppingon the transmission channel between the server and browser, an attacker may obtain theOTP. However, the OTP ischanged every login session and then is revoked afterauthentication. Therefore, an attacker cannotaccessthe serverusing the same OTP.

C. Phishing attack

Attackerscan also attempt to acquire sensitive information by masquerading as the server. However, if the attacker does not have theMK, he cannot generate the corresponding ImgOPS2. Therefore, the phishing server can be detected by the user.

D. Malware injection attack

By injecting malware into the browser, an attackermay steal the OTP and theImgOPS2. However, the OTP will be changed at the next login. Therefore, this stolen information cannot be usedfor the next authentication.

E. Stolen-verifier attack

By stealing the verification table from the server, an attacker may acquire some sensitive information. However, in our scheme, the server does not store users' sensitive information. Therefore, no sensitive information can be stolen from the server.

## V. EXPERIMENT

In our experiment, we use the computer to simulate the smartphone. First, when the user wants to login to the server, the server will usethe MK,OTP, and TS to generate the firstSSI(see Figure 6). Then, the biometrics key is obtained by capturing the face from thesmartphone camera (see Figure 7).



**Figure 6.Simulation of the server login page.**

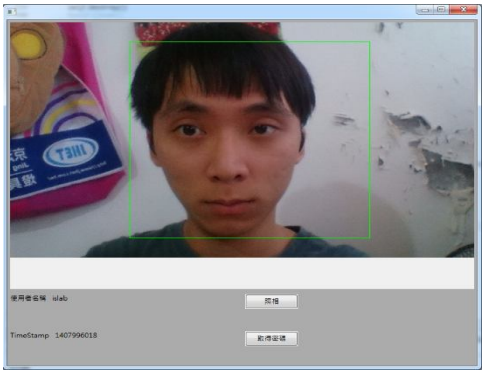

**Figure 7.Simulation of the smartphone and capturing the biometrics key.**

The biometrics key and TS will generate the second SSI (see Figure 8). Finally, the mobile image is superimposed on the server image, and the user can view the OTP(see Figure 9).

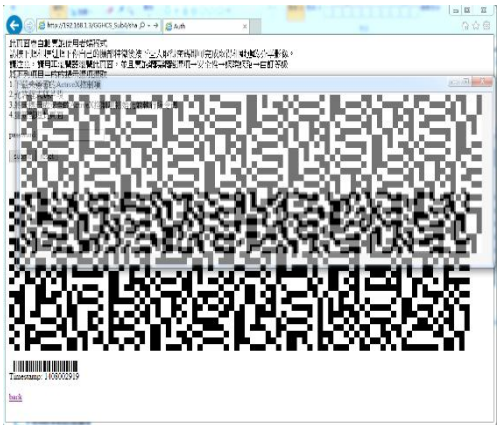

**Figure 8. Secondsecret sharing image (SSI) generated by the smartphone**



**Figure 9.Superimposed image to obtain the OTP.**

In Figure 9, we can clearly see the text, which proves that the captured shared image can be overlapped to obtain an OTP.

## CONCLUSIONS

In this paper, we have proposed a new one-time password mutual authentication scheme that does not require theuse of a network or high-priced SMS to generate an OTP.Nor must the user remember anything during this process. The scheme can directly link to the true user and minimizeany equipment burden using a user's smartphone. In addition, this scheme protects users who must use a public computer.

**ACKNOWLEDGMENT**

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for itsfinancial support of this research under Contract No. MOST 102－2918－I－035－007－

**REFERENCES**

[1] S.Lee and K.M. Sivalingam, "An efficient one-time password authentication scheme using a smart card," International Journal of Security and Networks, vol. 4, pp. 145-152, Jul. 2009.

[2] RSA SecurID. (n.d.).RetrievedApril, 2014,Available athttp://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.htm.

[3] 2012 Internet Trends. (n.d.).Retrieved April, 2014, Available athttps://www.kpcb.com/insights/2012-internet-trends-update.

[4] F. Aloul, S. Zahidi, andW. El-Hajj, "Two factor authentication using mobile phones," Proc.the 7th ACS/IEEE International Conference on Computer Systems and Applications, Rabat, p.p. 641-644, May 2009.

[5] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology: Eurpocrypt'94, Springer-Verlag, Berlin, pp. 1-12, 1995.

[6] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM Journal of Computing, vol. 38, no. 1, pp. 97-138, Mar. 2008.

[7] K. Choi, C. Lee, W. Jeon, K. Lee, and D. Won, "A mobile based anti-phishing authentication scheme using QR code," Proc. the2011 International Conference on Mobile IT Convergence, Korea, pp.26-28, Sep. 2011.

[8] W.-B. Lee, H.-B. Chen, S.-S. Chang, and C.-C. Yang, "An anti-phishing user authentication scheme without using a sensitive key table," Proc.the 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Dalian, China, pp. 14-16 Oct. 2011.

[9] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 651-663, Apr. 2012.

[10] C.-Y. Huang, S.-P. Ma, and K.-T. Chen, "Using one-time passwords to prevent password phishing attacks," Journal of Network and Computer Applications, vol. 34, no. 4, p.p. 1292-1301, 2011

[11] S.Hallsteinsen,I. Jorstad, and D. Thanh, "Using the mobile phone as a security token for unified authentication," Proc.the Second International Conference on Systems and Networks Communications, Los Alamitos, pp. 25-31, Aug. 2007.

[12] S. Mizuno, K. Yamada, and K.Takahashi, "Authentication using multiple communication channels," Proc.the 2005 workshop on Digital identity management, New York, USA, pp.54-62. Nov. 2005.

[13] Google 2-Step Verification. (n.d.). RetrievedApril, 2014, Available athttps://www.google.com/landing/2step/.

[14] Y.-F. Chang, C.-C. Chang, and J.-Y. Kuo, "A secure one-time password authentication scheme using smart cards without limiting login times," ACM SIGOPS Operating Systems Review, vol. 38, no. 4,p.p. 80-90, Oct. 2004.

[15] A. A. Khan, "Preventing phishing attacks using one time password and user machine identification," International Journal of Computer Applications, vol. 68, no.3, p.p. 7-11, Apr. 2013.

[16] Authenex A-Key Token. (n.d.).Retrieved April, 2014, Available athttp://www.authenex.com/ site_en/ Product-AKeyToken.html.

[17] SafeNet etoken pass. (n.d.). Retrieved April 2014, Available athttp://www.safenet-inc.com/multi-factor-authentication/authenticators/one-time-password-otp/etoken-pass/

★★★