Proposal for Optical One-time Password Authentication Using Digital Holography

Seok Hee Jeon¹ and Sang Keun Gil²*

¹Department of Electronic Engineering, Incheon National University, Incheon 22012, Korea
²Department of Electronic Engineering, The University of Suwon, Hwaseong 18323, Korea

(Received August 12, 2016 : revised October 10, 2016 : accepted October 10, 2016)

A new optical one-time password (OTP) authentication method using digital holography is proposed, which enhances security strength in the authentication system. A challenge-response optical OTP algorithm based on two-factor authentication is presented using two-step phase-shifting digital holography, and two-way authentication is also performed using challenge-response handshake in both directions. Identification (ID), password (PW), and OTP are encrypted with a shared key by applying phase-shifting digital holography, and these encrypted pieces of information are verified by each party by means of the shared key. The encrypted digital holograms are obtained by Fourier-transform holography and are recorded on a CCD with 256 quantized gray-level intensities. Because the intensity pattern of such an encrypted digital hologram is distributed randomly, it guards against a replay attack and results in higher security level. The proposed method has advantages, in that it does not require a time-synchronized OTP, and can be applied to various authentication applications. Computer experiments show that the proposed method is feasible for high-security OTP authentication.

Keywords: Optical encryption, Digital holography, Phase-shifting holography, One-time password, Optical cryptosystem

OCIS codes: (060.4785) Optical security and encryption; (090.0090) Holography; (090.2880) Holographic interferometry; (070.0070) Fourier optics and signal processing; (070.4560) Data processing by optical means

I. INTRODUCTION

In recent years, various services such as online banking, cyber stock exchange, and electronic commerce have been provided through communication networks for the Internet and mobile phones. Accordingly, we access to the Internet many times a day by getting a login and exchanging personal information, such as ID and PW. Conventional methods for authentication use the following things: what you know (i.e. ID, PW), who you are (i.e. fingerprint, DNA, iris pattern), or what you have (i.e. OTP). However, due to the development of hacking techniques, authentication based on ID and PW reveals the imperfection of such systems, and its security level has been degraded. To avoid disclosing ID and PW, one-time password (OTP) was invented to ensure authentication [1]. The OTP is a disposable password that allows a client to get a login for a server system. However, the OTP method has a weakness: interception by an unauthorized intruder. Since the OTP is the essence of most authentication systems, it is very important to protect the OTP. Some algorithms use two-factor authentication, which can be performed with a combination of two factors from ‘what you know’ and ‘what you have’, to increase security level. This presents a problem for challenge-response algorithms, though, which require both client and server to have a shared secret [2]. To hide OTPs in two-factor authentication, OTP encryption is more effective than using the unencrypted OTP alone. In general, conventional electronic cryptographic systems treat binary data, but these methods involve lots of computation and are not fast enough for high-volume data. Recently, various kinds of optical encryption methods have been proposed for security systems, as optical
systems offer parallel and fast processing [3-10]. One method of optical encryption uses optical holography [11, 12]. However, this method makes it difficult to deal with the encrypted information over a digital network, owing to the analog signal of a complex function with phase and amplitude. To overcome this problem, optical encryption techniques using phase-shifting digital holography are used to record and reconstruct the complex values of a hologram digitally [13-15]. In particular, we have presented some papers on optical encryption using phase-shifting digital holography [16-21].

In this paper we propose a new security-enhanced optical OTP authentication method using two-step quadrature phase-shifting digital holography based on orthogonal polarization, and show its feasibility for OTP authentication. In the proposed method, a new challenge-response optical OTP protocol based on two-factor authentication is presented, and two-way authentication is performed using the challenge-response handshake in both directions. In Section II, the proposed OTP authentication and its optical implementation are described. In Section III, computer experiments show results of optical OTP authentication using the proposed method. Finally, conclusions are briefly summarized in Section IV.

II. THEORY

2.1. The Proposed OTP Authentication

To cope with the security weakness of single-password authentication, in which the same password is reused repeatedly, an OTP is widely used as a disposable password to authenticate clients. The OTP is a password that is valid for only one login session or transaction, providing high security against man-in-the-middle attacks based on replaying a captured password: The OTP is invulnerable to replay attack, because a hacked OTP that was already used is no longer valid. Methods of generating an OTP are classified as synchronous and asynchronous protocols, according to whether or not the authentication server and the client are synchronized. The synchronous approach is divided into time-synchronization and event-synchronization methods. Time-synchronization authentication is an algorithm that computes OTPs from a shared secret key plus the current time, and in which OTPs are valid only for a short period of time between the server and the client. This method does not require the server’s challenge value. Event-synchronization authentication uses a mathematical algorithm to generate a new password associated with the previous password, in which OTPs are effectively generated by a one-way hash chain and must be used in a predefined order, starting from an initial seed. The merit of this method is that if the one-way function is a cryptographic hash function, decrypting it is computationally infeasible. However, it requires synchronization of the OTP generation number between server and client. Meanwhile, asynchronous authentication is a challenge-response protocol that uses a mathematical algorithm in which the server presents a question (challenge), and the client must provide a valid answer (response) to be authenticated. The advantages of this method are that it is easy to implement and does not demand synchronization between server and client. However, this challenge-response algorithm does require client and server to have a shared secret.

Figure 1(a) shows a protocol for conventional electronic challenge-response OTP authentication. The authentication server verifies the client using the OTP protocol. After authentication, a secret key is sent from server to client and is used to encrypt the client’s data, which later will be decrypted by the server with the shared secret key. To access the server, a client sends ID and PW to the authentication server (Request). The authentication server checks the client’s ID and PW and sends the client the seed and sequence, which includes the OTP generation parameter (Challenge). Next the client generates an OTP, produced through multiple iterations of a secure hash function along with a seed and sequence, and then sends it to the server (Response). The server verifies the OTP by computing the secure hash function and comparing the result with the previously accepted OTP. After authentication, the home server delivers a secret key for encrypting the client’s data. This key may be generated and shared by the Diffie-Hellman key-exchange agreement protocol.

Although OTP authentication is in some ways more secure than a static fixed password, it is still vulnerable to man-in-the-middle attacks, so OTPs should not be disclosed to any eavesdroppers. OTP encryption and layered security are recommended in order to hide an OTP; these methods are more secure than using an unencrypted OTP. Two-factor authentication is a form of layered security, consisting of ID, PW, and OTP. Layered security such as two-factor authentication is safer than using only one-factor of security during login process.

For this reason, we propose a new challenge-response OTP method based on two-factor authentication. The layered security is implemented using an encrypted OTP, in combination with an encrypted ID and PW that are stored in memory. In addition, two-way (mutual) authentication is performed using the challenge-response handshake in both directions. The server confirms that the client knows the shared secret, and the client also confirms that the server knows it, which protects against a fake server impersonating the true server.

Figure 1(b) shows the protocol for the proposed challenge-response OTP authentication and secret key delivery. At the start of accessing the server, the client sends to the authentication server an encrypted ID and PW, acquired by encrypting the ID and PW with a private key (Request). The authentication server decrypts the client’s ID and PW with the same private key, then encrypts the private key with the shared key which is computed with the cipher transmitted by the client, and sends it to the client (Check). The encrypted private key is decrypted with the same shared key that was generated in the previous ‘Request’
FIG. 1. A protocol for OTP authentication and secret key delivery: (a) the conventional electronic challenge-response OTP method, (b) the proposed challenge-response OTP method.

2.2. Optical Implementation of the Proposed OTP Authentication

The principal idea in this paper is that the OTP authentication is optically implemented by means of a digital holographic technique [22]. This is accomplished by two-step quadrature phase-shifting digital holography based on orthogonal polarization to encrypt and transmit a client’s ID, PW, and OTP to the server. These encrypted ID, PW, and OTP are then decrypted by the server and used to verify the client. For the proposed OTP authentication, we use a two-step quadrature phase-shifting holographic optical setup that employs simply two polarizers and one phase retarder to produce the quadrature phase shifting [21]. Figure 2 is the optical schematic for the proposed OTP authentication using two-step phase-shifting digital holographic optical encryption. Schematically, the optical setup contains a quarter-wave plate ($\lambda/4$-plate). It is used as a phase retarder, which generates $p$-polarization interference without phase shift along the vertical direction, and $s$-polarization interference with a phase shift of $\pi/2$ along the horizontal direction. These two interference patterns correspond to the two intensities resulting from the two-step phase-shifting digital holography. The collimated laser light passes through a linear polarizer (P1) whose polarization direction is $45^\circ$ with respect to the horizontal axis. A beam splitter (BS1) divides the collimated light into two linearly polarized plane waves, as reference and object beams. In the reference beam the $45^\circ$ linearly polarized light passes through the $\lambda/4$-plate, which sets the fast axis along the vertical axis. Then, after passing through the $\lambda/4$-plate, quadrature phase shift of $\pi/2$ occurs only on the horizontal axis. If we align an output analyzer (P2) whose polarization direction is set on the horizontal axis, a $\pi/2$ phase-shifted reference beam is obtained on the horizontal axis. On the other hand, when we align an output analyzer (P3) whose polarization direction is set on the vertical axis, no phase shift occurs in the vertical reference beam. This scheme makes it possible to acquire two-step quadrature phase-shifting digital holograms with $\pi/2$ phase shift between $s$- and $p$-polarizations on the CCDs separately. Binary information (such as a plain text) to be encrypted is displayed on SLM1, which is attached to a random phase mask (RPM1),
and is Fourier-transformed on CCD1 and CCD2 by a lens (L1) as the object beam, while another set of binary information (such as an encryption key) is displayed on SLM2, which is also attached to a random phase mask (RPM2) and is also Fourier-transformed on CCD1 and CCD2 by a lens (L2) as the reference beam.

The encryption and decryption principle using two-step quadrature phase-shifting digital holography is described in Refs. [20, 21]. If Fourier-transformed functions of a binary plain text \( o(x, y) \) to be encrypted and an encryption key \( r(x, y) \) are supposed to be \( O(\alpha, \beta) \) and \( R(\alpha, \beta) \) respectively, where \( (x, y) \) are transversal coordinates at the input spatial plane and \( (\alpha, \beta) \) are transversal coordinates at the spatial frequency plane,

\[
O(\alpha, \beta) = |O(\alpha, \beta)|e^{i \phi_O(\alpha, \beta)},
\]

\[
R(\alpha, \beta) = |R(\alpha, \beta)|e^{i \phi_R(\alpha, \beta)},
\]

then the two-step quadrature phase-shifting digital holographic method gives two interference intensities recorded on the CCD in the form of a digital hologram:

\[
I_1(\alpha, \beta) = |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2|O(\alpha, \beta)||R(\alpha, \beta)| \cos \Delta \phi,
\]

\[
I_2(\alpha, \beta) = |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2|O(\alpha, \beta)||R(\alpha, \beta)| \cos(\Delta \phi - \pi/2),
\]

where \( \Delta \phi = \phi_O - \phi_R \) is the phase difference between object and reference beams. These two digital holograms are encrypted data called *cipher texts*. The DC-term intensity of \( |O(\alpha, \beta)|^2 \) is acquired on CCD1 by blocking the reference beam in the optical setup shown in Fig. 2. Similarly, the DC-term intensity of \( |R(\alpha, \beta)|^2 \) is acquired on CCD1 by blocking the object beam. After receiving the encrypted digital holograms and applying a DC-term removal technique, Eq. (3) is modified as

\[
I_1'(\alpha, \beta) = I_1(\alpha, \beta) - A(\alpha, \beta) = B(\alpha, \beta) \cos \Delta \phi,
\]

\[
I_2'(\alpha, \beta) = I_2(\alpha, \beta) - A(\alpha, \beta) = B(\alpha, \beta) \sin \Delta \phi,
\]

where \( A(\alpha, \beta) \) is \( |O(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 \) and \( B(\alpha, \beta) \) is \( 2|O(\alpha, \beta)||R(\alpha, \beta)| \). Then the phase difference between object and reference beams and the magnitude are calculated as follows:

\[
\Delta \phi = \phi_O - \phi_R = \tan^{-1}\left(\frac{I_1'}{I_2'}\right),
\]

\[
|O(\alpha, \beta)||R(\alpha, \beta)| = \frac{1}{2} \left( |I_1'|^2 + |I_2'|^2 \right).
\]

From Eqs. (5) and (6), the complex hologram with encryption information is expressed as

\[
H(\alpha, \beta) = |O(\alpha, \beta)||R(\alpha, \beta)|e^{i \Delta \phi}.
\]

![FIG. 3. Block diagrams of the proposed optical OTP authentication: (a) encryption/decryption procedure for the ID+PW request and the OTP seed, (b) encryption/decryption procedure for OTP authentication and the secret key.](image-url)
Using this complex hologram and the encryption key information of $R(\alpha, \beta)$, the complex distribution with plain text information is reconstructed, and the original binary plain text is decrypted:

$$D(\alpha, \beta) = \frac{H(\alpha, \beta)R(\alpha, \beta)}{[R(\alpha, \beta)]^2} = |O(\alpha, \beta)|e^{i\phi}\left|\frac{e^{i\phi}R(\alpha, \beta)}{R(\alpha, \beta)}\right| = |O(\alpha, \beta)|e^{i\phi}.$$  

(8)

$$d(x, y) = |F^{-1}[D(\alpha, \beta)]| = |F^{-1}[O(\alpha, \beta)]| = |\psi(x, y)|.$$  

(9)

Figure 3 shows block diagrams of the proposed security-enhanced optical OTP authentication method using phase-shifting digital holography. The proposed system consists of a secure bi-directional communication channel. The encrypted information is transmitted to the other side. In Fig. 3, the phase-shifting digital holographic encryption is optically implemented by two-step quadrature phase-shifting digital holography based on orthogonal polarization, according to the optical schematic shown in Fig. 2. The encrypted ID, PW, and OTP seed are decrypted by the server and the client respectively. First, Fig. 3(a) shows the encryption/decryption procedure for the request and OTP seed. A client’s ID and PW are encrypted with the private key and transmitted to an authentication server. The private key is a kind of symmetric key that is needed to perform a block encryption algorithm at the beginning of the process. Basically, this private key is generated from a secret shared key derivation function after installing the authentication application in registration, and is stored in memory. When the first request comes to the server, it is used to decrypt the cipher of the ID and PW. The encrypted digital holograms are acquired from the intensities recorded on CCDs in the optical setup, transmitted to the other party, and changed into shared keys in each encryption/decryption session. The OTP seed has information about OTP generation parameters, which will be used to generate an OTP at the client. In this paper the OTP seed is chosen to be the same as the OTP itself intentionally, because the OTP encrypted with the shared key can be regarded as a kind of OTP seed. Second, Fig.
Proposal for Optical One-time Password Authentication Using ... Seok Hee Jeon and Sang Keun Gil

FIG. 5. Binary data format for computer experiments: (a) a client’s ID and PW via ASCII code conversion, (b) a binary image representation with zero padding of the client’s ID+PW to be encrypted, (c) a randomly generated binary bit pattern as a private key.

III. COMPUTER EXPERIMENTS

To prove the validity of the proposed security-enhanced optical OTP authentication method, we check its performance by computer experiments with two-step quadrature phase-shifting digital holography based on orthogonal polarization.

Figure 5(a) shows a client’s ID and PW, which represents binary data code from ASCII code conversion, and Fig. 5(b) shows a binary image representation with zero padding of the client’s ID+PW to be encrypted, the size of which is 64 × 64 pixels. Figure 5(c) shows a private key of 64 × 64 pixels, which for convenience is a randomly generated binary bit pattern. The client’s ID + PW is encrypted with the private key in the ‘Request’ stage. Figure 6 shows example intensity histograms for the encrypted digital holograms, obtained using two-step phase-shifting digital holography to encrypt the client’s ID+PW shown in
FIG. 6. Intensity histograms of the encrypted digital holograms with 256 gray levels: (a) the encrypted client’s ID+PW when the phase shift is 0, (b) the encrypted client’s ID+PW when the phase shift is π/2, (c) the DC term of the client’s ID+PW, (d) the DC term of the private key, (e) the modified intensity of Fig. 5(a) after DC-term removal, (f) the modified intensity of Fig. 5(b) after DC-term removal.

FIG. 7. Complex hologram (H1) calculated with the reconstructed phase and amplitude: (a) the amplitude map, (b) the phase map.

FIG. 8. Result of decryption of the client’s ID + PW when the same (correct) private key is used: (a) the reconstructed image pattern obtained from complex hologram (H1) and the same private key, and (b) the correctly decrypted binary image of the client’s ID + PW after binarization with the proper threshold value, exactly same as the client’s ID + PW shown in Fig. 5(b).
Proposal for Optical One-time Password Authentication Using … - Seok Hee Jeon and Sang Keun Gil

FIG. 8. Result of decryption of the client’s ID+PW when the same private key is used for decryption: (a) the reconstructed image obtained from the complex hologram (H1) and the same private key, (b) the correctly decrypted binary image of the client’s ID+PW using the proper threshold.

FIG. 9. A shared key1 generated using the complex hologram (H1), which is transmitted from the client: (a) the reconstructed amplitude image of the complex hologram (H1), (b) the shared key1 using the proper threshold.

FIG. 10. Result of decryption of the server’s private key: (a) the reconstructed image obtained from complex hologram (H2) and the same shared key1, (b) the correctly decrypted binary image of the server’s private key using the proper threshold.

Figure 9 shows one example of the shared key1 that is generated by the complex hologram (H1). The reconstructed amplitude image pattern of the complex hologram (H1) is shown in Fig. 9(a), which is the same as Fig. 7(a). The shared key1 after binarization with the proper threshold value is shown in Fig. 9(b). The server’s private key is encrypted using this shared key1 in the ‘Check’ stage.

The server’s private key is decrypted with this shared key1; Fig. 10 shows the result of decryption of the server’s private key when the same shared key1 is used. Figure 10(a) is the reconstructed image pattern obtained from complex hologram (H2) and the same shared key1, and Fig. 10(b), which is the correctly decrypted binary image of the server’s private key after binarization with the proper threshold value, is exactly same as the client’s private key shown in Fig. 5(c).
After checking the true server, the client’s ID+PW is encrypted again with the shared key2 in the ‘Acknowledge’ stage. Figure 11 shows the result of decryption of the client’s ID+PW when the same shared key2 is used. Figure 11(a) is the reconstructed image pattern obtained from complex hologram (H3) and the same shared key2, and Fig. 11(b), which is the correctly decrypted binary image of the client’s ID+PW after binarization with the proper threshold value, is exactly same as the client’s ID+PW shown in Fig. 5(b).

After verifying the true client, the server’s OTP seed is encrypted with the shared key3 in the ‘Challenge’ stage. Figure 12 shows the result of decryption of the server’s OTP seed when the same shared key3 is used. Figure 12(a) is a binary number image representation with zero padding of the server’s OTP seed to be encrypted, and Fig. 12(b) is the reconstructed image pattern obtained from complex hologram (H4) and the same shared key3. Figure 12(c) shows the correctly decrypted binary image of the server’s OTP seed after binarization with the proper threshold value, which is exactly same as the server’s OTP seed shown in Fig. 12(a).

After checking the server’s OTP seed, the client’s OTP is encrypted with the shared key4 in the ‘Response’ stage. Figure 13 shows the result of decryption of the client’s OTP when the same shared key4 is used. Figure 13(a) is
The reconstructed image pattern obtained from complex hologram (H5) and the same shared key4, and Fig. 13(b), which is the correctly decrypted binary image of the client’s OTP after binarization with the proper threshold value, is exactly same as the server’s OTP seed shown in Fig. 12(a). In this paper, the OTP is chosen to be the same as the OTP seed because the OTP encrypted with the shared key can be regarded as a kind of OTP seed.

After decrypting and checking the client’s OTP, the home server enables the client to get into a log in, and delivers a secret key encrypted using the shared key5 for the client’s data encryption. Figure 14. shows the result of decryption of the server’s secret key when the same shared key5 is used. Figure 14(a) is a randomly generated binary bit pattern as a secret key for simulation, and Fig. 14(b) is the reconstructed image pattern obtained from complex hologram (H6) and the same shared key5. Figure 14(c) shows the correctly decrypted binary image of the server’s secret key after binarization with the proper threshold value, which is exactly same as the server’s secret key shown in Fig. 14(a).

After decrypting the server’s secret key, the client encrypts binary data with this secret key. Figure 15 shows the result of decryption of the client’s data when the same secret key is used for decryption. Figure 15(a) is a binary image representation of the client’s data to be encrypted, and Fig. 15(b) is the reconstructed image pattern obtained from complex hologram (H7) and the same secret key. Figure 15(c) shows the correctly decrypted binary image of the client’s data after binarization with the proper threshold value, which is exactly same as the client’s data shown in Fig. 15(a).

IV. CONCLUSION

A new optical OTP authentication method using phase-shifting digital holography is proposed, which enhances the security level of authentication, compared to the conventional electronic OTP method. Optical encryption of the ID, PW, and OTP for authentication is performed by implementing two-step quadrature phase-shifting digital holography based on orthogonal polarization. The proposed optical phase-shifting digital holographic system generates the encrypted digital holograms, which are Fourier-transform holograms recorded on CCDs with 256 gray-level quantized intensities and then transmitted. These encrypted digital holograms are used as cipher texts to generate a shared secret key. Also, a new
challenge-response optical OTP method based on two-factor authentication is presented, which is a layered security method using an encrypted OTP in combination with an encrypted ID and PW. The exchange of such encrypted ID, PW, and OTP information does not directly reveal the password to an eavesdropper. In addition, two-way authentication is performed using challenge-response handshake in both directions. During the two-way authentication process, the encrypted digital holograms transmitted to the other party have the form of a random pattern. The use of randomness protects against a man-in-the-middle attack, and the possibility of a replay attack. The proposed method also provides unconditional choice of the randomly generated disposable OTP without confinement, which means all authentication servers can alter independent OTPs at their own discretion. Advantages of the proposed OTP authentication system are impossibility of password-reuse attack, unpredictability of OTP generation, confidentiality, and convenient authentication without synchronization. Computer experiments verify that the proposed method allows highly secure OTP authentication applications.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2014.

REFERENCES