ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 16-03-12

j.inst.Korean.electr.electron.eng.Vol.20,No.3,291~294,September 2016
http://dx.doi.org/10.7471/ikeee.2016.20.3.291

디지털 홀로그래피를 이용한 one-time pattern 상호 인증 방법

One-time Pattern Mutual Authentication Method by using Digital Holography

길 상 근*★

Sang-Keun Gil*★

Abstract

A new optical one-time pattern password(OTPT) mutual authentication method is proposed, which presents a two-factor authentication by 2-step phase-shifting digital holography and performs a two-way authentication by a challenge-response handshake of the optical OTPT in both directions. Because a client and a server use OTPT once as a random number and encrypt it for mutual authentication, it protects against a replay or a man-in-the middle attack and results in higher security level.

요 약

본 논문은 새로운 광학적 일회용 패턴암호 상호 인증 방법을 제안한다. 이 방법은 2-단계 위상천이 디지털 홀로그래피 기법을 사용하여 이중 인증을 제공하고, 광학적 일회용 패턴암호를 상호 양방향으로 시도-응답 악수 기법을 구현하여 양방향 인증을 수행한다. 클라이언트와 서버는 상호 인증시 일회용 패턴암호를 무작위 수로 선택하여 오직 한번만 사용하고 이를 암호화하여 전송하기 때문에, 되풀이 공격이나 중간자 공격과 같은 암호공격으로부터 암호시스템을 보호하고 보안수준을 한층 더 높일 수 있다.

Key words : Optical security and encryption, Digital holography, Authentication, Fourier optics and optical signal processing, Data processing by optical means.

* Dept. of Electronics Engineering, The University of Suwon

★ Corresponding author :skgil@suwon.ac.kr, 031-220-2664

Manuscript received Sep. 20, 2016; revised Sep. 26. 2016; accepted Sep. 28. 2016.

Ⅰ. 서론

네트워크에서 서버에 로그인하기 위해서 현재 일반적으로 많이 사용되고 있는 인증 방식이 일회용 암호(one-time password, OTP)이다[1]. 하지만 이러한 OTP 방식은 ID나 패스워드의 보안 약점을 개선했지만 클라이언트와 서버간의 동기화를 요구할 뿐만 아니라 일방적으로 클라이언트의 인증만 허용되고 클라이언트는 정확하게 신뢰성 있는 서버에 접속되었는지는 알 수가 없다.

이러한 약점을 극복하기 위해서 본 논문에서는 상호 인증이 가능하고 OTP 정보가 2-차원으로 암호화되어 암호강도가 매우 높은 계층 보안(layered security) 광 암호화 시스템을 제안한다[7]. 제안한 디지털 홀로그래픽 광 인증 방법은 이중(two-factor) 인증과 양방향(two-way) 인증을 수행할 수 있다.

II. 본론

본 논문에서 제안한 일회용 패턴암호(one-time pattern password, OTPT) 상호 인증 방법은 단계적으로 세 단계의 과정으로 이루어진다. 요구(Request) 단계에서는 클라이언트가 서버에 1차 인증을 받기 위한 ID+password와 서버의 진위를 확인하기 위한 일종의 OTP인 C-OTPT를 암호화하여 보낸다. 시도(Challenge) 단계에서는 서버가 클라이언트의 ID+password를 인증한 다음, 복호화된 C-OTPT와 클라이언트를 재인증하기 위한 S-OTPT를 암호화하여 보낸다. 응답(Response) 단계에서는 클라이언트는 서버가 보낸 C-OTPT를 복호화 확인하여 서버를 인증한 다음, 재인증을 위한 복호화된 S-OTPT와 다음번 인증을 위한 새로운 OPT인 C-OTPT를 보낸다. 그림 1은 이러한 상호 인증 알고리즘을 보여준다.

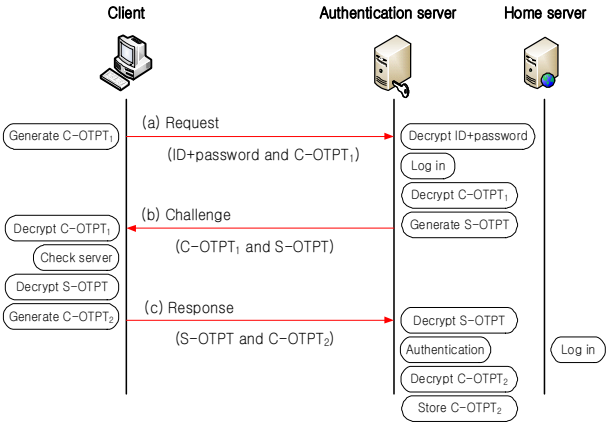

Fig. 1. Proposed one-time pattern password mutual authentication

그림 1. 제안한 one-time pattern password 상호 인증 알고리즘

그림 2는 본 논문에서 제안한 상호 인증을 위해 직교 편광과 2-단계 위상천이 디지털 홀로그래피를 이용한 광학적 암호화 시스템이다[8]. 광학장치도에서 P는 편광기로 직교 편광 2-단계 디지털 홀로그램을 얻는데 이용되고, SLM은 공간광변조기로 데이터 표시의 입력장치로 사용된다. 한편 RPM은 random phase mask로 렌즈(L)에 의해 퓨리어 변환되는 광 패턴의 공간주파수 영역을 넓게 하는데 이용된다. 여기서 두 개의 간섭계가 사용되는데 두 개의 암호화될 정보가 상호 공유한 비밀키에 의해 동시에 암호화되고, 암호화된 디지털 홀로그램들은 상대방에게 전송되어 복호화 된다. 2-단계 위상천이 디지털 홀로그래피에 의해 CCD에서 얻어진 광세기는 다음 식과 같고 무작위한(random) 형태의 암호문으로서 전송된다. 여기서 O는 암호화될 데이터가 포함된 물체광을, R은 암호화 키로서의 참조광을 나타내고 $\Delta\phi=\phi_O-\phi_R$는 두 광의 위상차를 나타낸다.

$$I_1 = |O|^2 + |R|^2 + 2|O||R|\cos\Delta\phi \quad (1)$$

$$I_2 = |O|^2 + |R|^2 + 2|O||R|\cos(\Delta\phi - \pi/2) \quad (2)$$

한편 전송된 디지털 홀로그램으로부터 (3)식과 같이 복소 홀로그램으로 복원되며, 복원된 홀로그램 정보와 암호화시 사용한 암호화 키 R에 의해서 원래의 데이터가 (4)식과 (5)식과 같이 복호화 된다.

$$H = |O||R|e^{j\Delta\phi} \quad (3)$$

$$D = \frac{HR}{|R|^2} = \frac{|O||R|e^{j(\phi_O-\phi_R)}|R|e^{j\phi_R}}{|R|^2} = |O|e^{j\phi_O} \quad (4)$$

$$d = |F^{-1}[D]| = |F^{-1}[O]| = o(x,y) \quad (5)$$

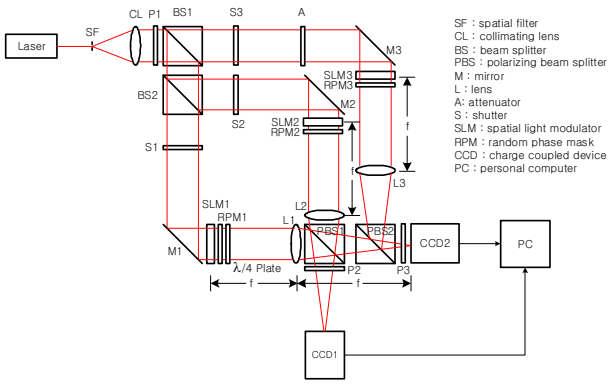

Fig. 2. Digital holographic optical setup for one-time pattern password mutual authentication

그림 2. One-time pattern paasword 상호 인증을 위한 디지털 홀로그래픽 광학 장치

그림 3부터 그림 5는 제안한 OTPT 상호 인증 방법에 대한 실험결과를 보여 준다. 그림 3(a)와

(d)는 Request 단계의 클라이언트의 인증에 필요한 ID와 패스워드가 포함된 QR 코드와 첫 번째 C-OPTP를 나타내고, (b)와 (e), (c)와 (f)는 각각 서버에서 복원되고 복호화된 데이터를 보여준다. 그림 4(a)와 (d)는 Challenge 단계의 서버에서 복호화된 첫 번째 C-OPTP와 서버가 생성한 S-OPTP를 나타내고, (b)와 (e), (c)와 (f)는 각각 클라이언트에서 복원되고 복호화된 데이터를 보여준다. 여기서 C-OPTP가 일치하면 서버가 인증된다. 그림 5(a)와 (d)는 Response 단계의 클라이언트에서 복호화된 서버의 S-OPTP와 클라이언트가 생성한 두 번째 C-OPTP를 나타내고, (b)와 (e), (c)와 (f)는 각각 서버에서 복원되고 복호화된 데이터를 보여준다. 여기서 S-OPTP가 일치하면 클라이언트가 재인증된다.

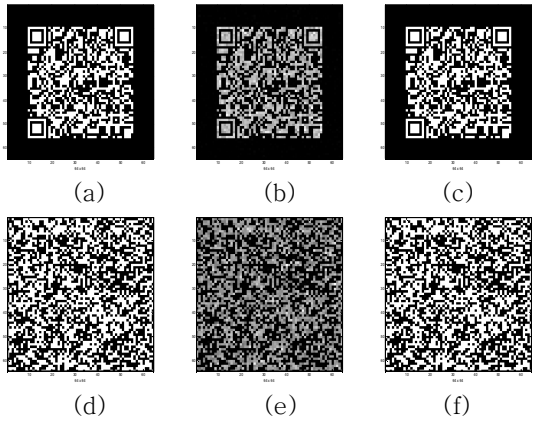

Fig. 3. Decrypted client's one-time pattern: Request
그림 3. 복호화된 클라이언트의 one-time pattern: Request

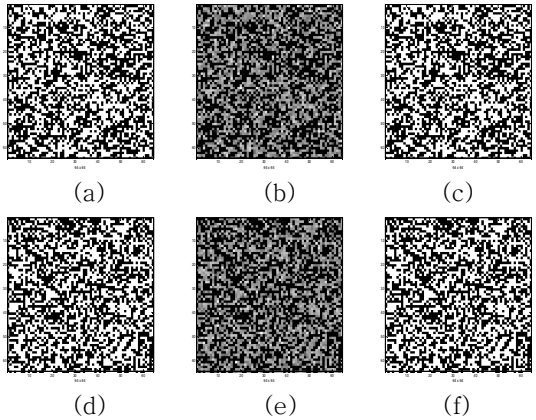

Fig. 4. Decrypted server's one-time pattern: Challenge
그림 4. 복호화된 서버의 one-time pattern: Challenge

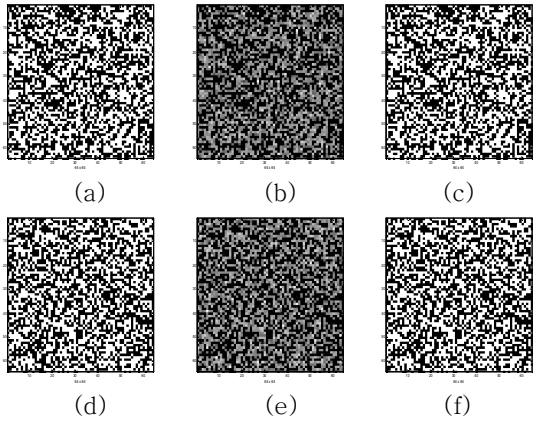

Fig. 5. Decrypted client's one-time pattern: Response
그림 5. 복호화된 클라이언트의 one-time pattern: Response

III 결론

본 논문에서는 2-단계 위상천이 디지털 홀로그래피 기법을 사용하여 이중 인증에 기반한 새로운 광학적 시도-응답 양방향 상호 인증을 제안하였다. OTPT 정보가 광학적 2-차원으로 구현되어 기존의 OTP 방식보다 암호 길이가 매우 크고 양방향 상호 인증에 필요한 OTPT도 무작위 수로 선택함으로써 되풀이(replay) 공격이나 중간자(man-in-the-middle) 공격에 암호강도가 매우 높은 계층 보안 시스템을 구현할 수 있다. 또한 클라이언트와 서버가 OTPT를 임의적이고 독립적으로 생성하고 인증할 수 있어 서로간의 동기화가 필요하지 않는 장점을 지닌다.

References

[1] D. McDonald and R. Atkinson, "One-time passwords in everything(OPIE): Experiences with building and using stronger authentication," *Proceedings of the 5th USENIX Security Symposium*, 1995

[2] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Optical Engineering* Vol.33, pp1752-1756, 1994

[3] R. Arizaga and R. Torroba, "Validation through a binary key code and a polarization sensitive digital technique," *Optics*

Communications, Vol.215(1), pp31-36, 2003
[4] 12. X. Meng, L. Z. Cai, X. L. Yang, X. X. Shen, and G. Y. Dong, and Y. R. Wang, "Two-step phase-shifting interferometry and its application in image encryption," Opt. Lett. 31, 1414-1416 (2006).
[5] X. Meng, L. Z. Cai, X. L. Yang, X. X. Shen, and G. Y. Dong, and Y. R. Wang, "Two-step phase-shifting interferometry and its application in image encryption," Optics Letter. Vol. 31(10), pp1414-1416, 2006
[6] S-K Gil, "Application to 2-D page-oriented data optical cryptography based on CFB mode," *j.inst.Korean.electr.electron.eng.*, Vol.19(3), pp424-430, 1994
[7] S. K. Gil, S. H. Jeon, and J. R. Jeong, "Security enhanced optical one-time password authentication method by using digital holography," *Proceedings of SPIE*, Vol.9386, pp93860U, 2015
[8] S. K. Gil, "2-step quadrature phase-shifting digital holographic optical encryption using orthogonal polarization and error analysis," *Journal of the Optical Society of Korea*, Vol.16(4), pp354-364, 2012