Journal of the Korea Convergence Society
Vol. 10. No. 2, pp. 7-11, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.2.007

무아레를 이용한 융합 보안토큰생성과 전파공격 보호 기법

이수연[1], 이근호[2*]
[1]백석대학교 정보통신학부 학생, [2]백석대학교 정보통신학부 교수

A Scheme of Improving Propagation Attack Protection and Generating Convergence Security Token using Moire

Su-Yeon Lee[1], Keun-Ho Lee[2*]
[1]Student, Division of Information Communication, BaekSeok University
[2]Professor, Division of Information Communication, BaekSeok University

요 약 급격한 전파를 이용하는 기기의 다양화와 대중화로 인해 많은 전파 관련 보안 문제들이 일어나고 있다. 일상적인 생활에서의 전파의 안전은 매우 밀접한데 전파의 방해와 교란은 단순 생활의 불편뿐 아니라 신체의 직접적인 피해를 입힐 수도 있기 때문에 전파보호는 매우 중요한 과제이다. 본 논문에서는 전파 교란과 교섭을 막기 위한 방안으로 백색광 광원, 투영격자와 광원으로 영사식 무아레를 측정 하여 기준격자 및 변형격자의 영사 이미지를 획득한 후 위상도를 알고리즘에 적용하여 화상처리 알고리즘으로 무아레 무늬를 생성하고 무늬 위상도를 3차원 형상도로 생성한다. 이렇게 측정된 얼굴 형상을 이용한 암호화된 토큰을 만들어 토큰링을 통한 정보의 수신여부를 결정 하여 인증 강도, 호출자의 정보 등이 포함된 동적 보안 속성을 가진 수평 전파를 전송하고 java직렬화와 직렬화 해제 기능을 이용하여 토큰의 고유성을 확인 수평전파를 송·수신 하여 문제점을 해결하는 기법을 제안하였다.

주제어 : 무아레, 전파위조, 보안토큰, 보안전파, 수평전파

Abstract Due to diversification and popularization of devices that use rapid transmission, there are many security issues related to radio waves. As the disturbance and interference of the radio wave can cause a direct inconvenience to a life, it is a very important issue. In this paper, as a means to prevent radio disturbance and interference, the projected image of the reference grid and the deformed grid is obtained by measuring the projected moiré using the white light source, projecting grid and the light source, and a moiré pattern is generated with an image processing algorithm by applying a phase diagram algorithm, and generated moiré pattern phase diagram creates a three-dimensional shape. By making an encrypted token using this measured face shape, the transmission of the information through token ring is determined in order to transmit the horizontal transmission having the dynamic security characteristics which includes authentication strength and caller information, etc. And by confirming the uniqueness of the token and by sending and receiving the horizontal transmission using java serialization and deserialization function, a problem solving method is suggested.

Key Words : Moire, jamming ,security token, security radio wave ,horizontal radio wave

*This research was supported by Basic Science Research Program through the National resarch Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A3B03935976) and was supported by Korea Sanhak Foundation
*Corresponding Author : Keun-Ho Lee (root1004@bu.ac.kr)
Received November 29, 2018 Revised February 1, 2019
Accepted February 20, 2019 Published February 28, 2019

1. 서론

개인 소형 기기 종류와 이용자가 기하급수적으로 늘어나면서 전파 피해, 전파이용과 보호의 중요성이 대두되고 있다. 드론이나 네비게이션 등은 위성으로부터 발신되는 신호를 받아 위치를 파악하고, 스마트기기들은 GPS를 이용하여 위치기반 서비스와 통신서비스를 제공하고 있다. 전파공격은 수신기에 대한 교란전파 공격을 의미하며, 크게는 국가 간의 전파 교란공격이나 정보 취득의 목적으로 무선 전파를 이용하기도 하며, 민간 항공기의 전파 교란으로 안전의 위협을 가하는 실제 사례들이 있었으며 개인의 통신이용을 방해하고 재머 등을 사용해 생활의 불편함을 주는 등 여러 가지 방법으로 피해를 주고 있다.

위에서 언급한 문제점들 중 개인사용자의 전파 이용 시 발생하는 문제점들을 미연에 방지하고자 자가면역체계의 역할을 적용하여 이상행위에 대한 움직임 포착과 그에 적합하게 안전성을 높일 수 있는 무아레를 이용해 생성한 보안 토큰으로 외부의 공격을 미연에 방지하고자 제안하였다.

본 논문에서는 생체인식 기술의 보편화에 의해 생체인증의 방법과 수단 또한 늘어나 접근성이 높아져 위조와 주변 환경에 제약받을 경우 인식률이 낮아지고 이로 인해 보안의 취약점이 발생한다. 기존의 이러한 문제점들을 보완하고자 디지털 영사식 방법을 통한 무아레 현상을 생체인증에 접목시켜 보다 정확한 생체인증을 진행할 수 있도록 하고 영사식 무아레 현상을 이용해 인식한 생체정보를 사용해 생성된 인증키로 생산된 보안토큰 접목한 전파의 보안을 제안하고자 한다.

2. 관련연구

2.1 전파공격 종류

– 재밍(jamming)

전파 방해 행위인 재밍(jamming)은 전파가 강한 주파수를 이용해 기계가 기존 주파수를 대신 강한 전파의 주파수를 수신하면서 순간적으로 먹통이 되거나 오작동을 일으키는 것으로 방해의 목적으로 보낸 강한신호 때문에 위성으로부터 받은 신호를 복원하지 못해 정확한 위치와 시간을 계산하는데 영향을 준다[1].

재밍를 위해서는 지향성 안테나를 사용하는 방법이 있으나 수신 할 수 있는 위성의 수가 제한될 수 있어 수신기의 성능에 문제를 줄 수 있다. 이러한 재밍 공격의 경우에는 주변에서의 이상 움직임을 탐지로 인해 일차적인 방어가 가능한데 전자기파를 이용하게되면 벽이나 장애물이라도 투과가 가능 하기 때문에 세밀한 인식을 위해서는 픽셀을 이용한 CV방식 등과 전자기파를 함께 이용한다면 보다 넓은 범주에서의 세밀한 이상 징후를 파악이 가능하다[2]. 비인가된 특정 이상 징후를 스스로 탐지한다면 자가면역시스템의 면역체계를 통하여 자동적으로 그 근원지를 차단하는 방식을 사용하여 인증된 사용자만 데이터에 접근 할 수 있도록 한다면 행해진 공격에 적절한 안전성에 도움을 준다.

– 전파 위조 공격

위조 공격은 미리 확인된 위성의 위치와 시간을 계산해 위성이 보낸 신호와 같은 신호를 보낸 후 원하는 위치로 위성을 이동하거나 시간을 변경시켜 수신기가 위성으로 받은 신호를 선택하지 않고 공격자가 보낸 신호를 선택하도록 시간과 위치를 조작한다[3]. 이런 공격은 시뮬레이터나 무선 통신 연구용으로 사용되고 있는 USRP와 같은 소프트웨어 라디오 장비를 이용해 비교적 쉽게 구현할 수 있다[4].

위조 공격의 경우 탐지하기가 어렵기 때문에 다양한 수신기가 수신 정보를 공유함으로써 가능하다고 이론적으로 알려져 있으나 실제 위조 공격 방지는 현재까지 암호화가 가장 많이 사용되는 거의 유일한 수단이다. 복호화용 키가 모든 수신기에 설치되어야 하며, 키가 유출될 위험이 있어 키 관리의 문제가 있다. 때문에 정보의 변경이 불가한 이용자의 생체정보 중 보편화되어 비교적 안정성이나 위조가 쉬운 지문이나 일반적인 얼굴 인식을 대신해 무아레를 통해 비교적으로 위조나 데이터 변조가 어렵도록 만들어진 데이터를 이용한 암호화 방법을 제안하고자 한다.

2.2 무아레

무아레는 맥놀이 현상이 시각적으로 생기는 것으로 패턴들이 주기적로 겹쳐서 생기는 현상이다[5]. 일정한 간격을 나타내는 물체 사이에 발생하는 무아레 무늬가 갖는 미세한 격자간격을 확대하는 성질과 격자간의 오차를 평균화하는 성질을 이용해 정밀한 측정을 한다[6,7]. 무아레 무늬에는 여러 가지 다양한 성질들이 존재하는데

이중에서 우리가 주목해야 하는 부분은 무아레 무늬가 변화를 통해 실제 물체의 움직임을 파악하여 세밀한 무아레 무늬를 제작하므로 해당 물체의 형상에 대한 보다 정확한 3차원 정보를 가지게 된다[8,9]. 본 논문에서는 이러한 무아레의 특징을 이용해 추출한 생체인식 정보를 토큰을 생성하는데 이용하고자 한다.

3. 적용방안

3.1 영사식무아레 적용 방안

Fig1에서는 암호화 토큰을 생성하는데 사용할 생체인식정보를 백색광을 사용한 광원과 투영격자와 광원으로 영사식무아레(Projection Moire)촬영 방식으로 측정 한다. 장비 프로젝터로 기준격자 및 변형격자의 영사 이미지를 획득한다. 각각의 획득한 위상도를 알고리즘을 적용하여 기준격자 위상도와 변형격자 위상도를 화상처리 알고리즘으로 무아레 무늬를 생성한다. 무아레무늬의 차수를 추출하지 못해 일어난 위상이동법의 모호성의 문제는 2중 파장의 원리를 사용하여 무아레 무늬의 차수 추출을 가능하게 한다. 또한 측정반복을 통해 세 부분의 좌표를 여러번 측정하여 각 부위별로 정확도를 더욱 높일 수 있도록 할 수 있다. 이를 바탕으로 맥놀이 무아레 무늬 위상도를 생성, 무늬 차수를 적용하여 3차원 형상도를 생성한다. 이렇게 측정된 얼굴형상을 암호화 토큰을 적용하여 전파를 보호 하고자 한다.

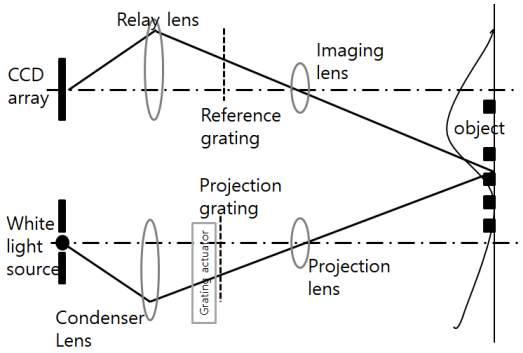

Fig. 1. projection Moire

3.2 보안 토큰 생성과 적용방안

3.2.1 보안 토큰 생성 과정

Fig 2는 영사식무아레를 통한 생체정보를 이용한 암호화 토큰 생성시 높은 보안을 제공하기 위해 인증 과정 자체가 한 보안토큰 내부에서 수행 되어지는 시스템인 Match-on- Token을 이용하여 사용자의 특징을 기반으로 작성된 인증 보안 토큰 시스템을 사용한다[10].

영사식 무아레를 이용한 얼굴인식 정보을 사용한 특징 기반의 인증 시스템은 사용자 인증과정과 사용자 등록과정을 수행한다[11,12]. 등록은 획득된 얼굴인식 정보상에서 특징 정보들을 추출하고, 인증 과정은 특징 정보가 입력된 영사식 무아레를 이용한 얼굴인식 정보영상에서 추출한 후 저장되어있던 특징점과 matching을 수행함으로써 저장된 지문과 입력된 정보가 동일한 정보인지를 판단하여 등록 처리과정을 거친다[13,14]. 이후 특징을 추출하는 과정을 호스트 컴퓨터에서 수행하고, 등록된 특징을 인증해 새로 입력된 특징 사이의 유사도를 측정하는 특징 매칭 과정을 보안 토큰 내부에서 수행한다[15]. 처리 과정과 특징 추출 과정은 많은 메모리 사용과 명령어 수를 요구 하여 보안 토큰과 같은 제한인 환경에서는 수행이 불가능하다.

정보보호를 위해 외부로 유출되지 않아야하는 영사식 무아레를 이용한 특징 정보는 등록 과정에서 보안 토큰에 저장된 특징 정보는 외부로 전달하지 않고 보안토큰 내부에서 정합 과정을 수행한 후 최종 인증 결과만을 호스트로 전송하여 고유한 개인의 생체 정보가 외부로 유출되지 않도록 한다.

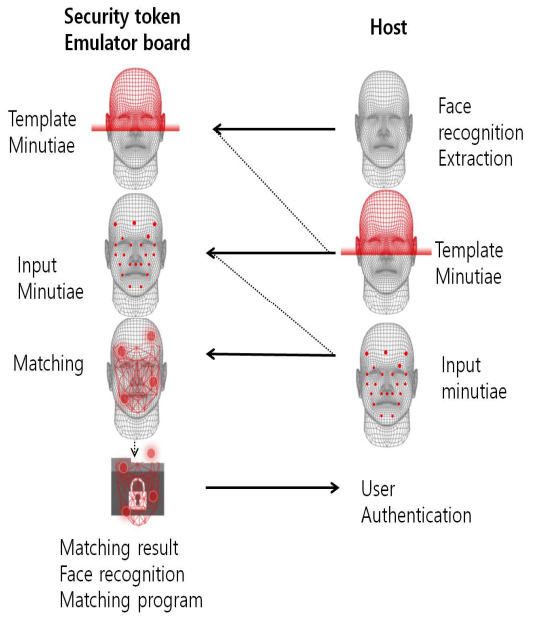

Fig. 2. Security Token System Actions

Fig 3에서 보안 속성 전파를 사용하면 보안 속성을 전송할 수 있다. WebSphere Application Server는 정적 속성이나 동적 속성을 조회할 수 있는 사용자 모듈에서 보안 속성을 가져올 수 있다. 동적 보안 속성은 연결에 사용할 인증 강도, 호출자의 정보 등을 포함한다. 보안 속성 전파는 Java직렬화 방법에 대한 규칙을 지정, 전파 서비스를 제공한다. 서로 다른 플랫폼 및 소프트웨어 버전을 처리할 때 문제가 발생할 수 있으므로 사용자 정의 직렬화 기능을 사용 가능하게 하는 프레임워크를 제공한다. 프레임워크는 만들어진 토큰의 고유성을 식별할 수 있다.

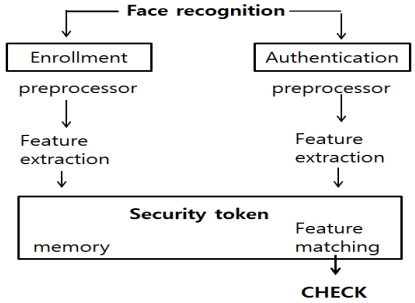

Fig. 3. Face recognition token system

사용자 정보(영사식 무아레를 이용한 얼굴인식 정보)를 인증한 후 원격 사용자 레지스트리를 호출하여 사용자 액세스 권한을 표시하는 보안 속성을 찾는 프로세스를 사용 전파 로그인은 사용자 정보의 유효성을 검증한 다음 WebSphere Application Server에 알려진 사용자 정의 오브젝트와 프레임워크를 구성하는 일련의 토큰 직렬화 해제한다. 사용자 정의 토큰의 직렬화 및 직렬화 해제는 구현을 통해 수행되고 사용자 정의 로그인 모듈에 의해 처리되며 접근의 여부를 결정하고자 한다.

3.2.2 수평전파

수평전파에서 직렬화된 보안속성(전파 토큰)에는 정적 속성과 동적 속성이 포함된다. SSO토큰은 수평 전파에 필요한 시스템 특정 정보를 저장한다. SSO 토큰에 포함된 정보는 위치와 해당 서버와 통신하는 방법을 수신 서버에 알려주며, 직렬화된 속성을 찾기 위한 키도 포함된다. 수평 전파를 사용하려면 SSO토큰 및 보안 속성 전파 기능을 구성해야 하며, 관리 콘솔에서 두 기능을 모두 구성할 수 있다.

수평 전파에서 보안 속성은 서버 간에 전파가 된다. 직렬화된 보안 속성(내용 및 전파 토큰)에는 정적 속성과 동적 속성이 포함되어있다. SSO 토큰은 수평 전파에 필요한 추가 시스템 특정 정보를 저장한다. SSO 토큰에 포함된 정보는 원래 서버가 있는 위치와 해당 서버와 통신하는 방법을 수신 서버에 알려준다. 또한 SSO 토큰에는 직렬화된 속성을 찾기 위한 키를 가지고 있으며, 수평 전파를 사용하려면 SSO 토큰 및 웹 인바운드 보안 속성 전파 기능을 구성해야 한다. 관리 콘솔에서 두 기능을 모두 구성할 수 있다.

주제에 추가된 사용자 정의 SSO토큰은 자동으로 응답에 쿠키로 추가되며 브라우저로 다시 전송되는 속성을 포함한다. 토큰 인터페이스 getName 메소드는 getVersion 메소드와 함께 쿠키 이름을 정의한다. 중요한 정보, 기밀 정보 또는 암호화되지 않은 데이터를 응답 쿠키에 추가하지 않아야 한다.

사용자는 SSO 토큰을 사용하여 한 번의 인증으로 여러 WebSphere Application Server의 자원에 액세스할 수 있다. 사용자 정의 SSO 토큰은 사용자 정의 처리를 SSO 시나리오에 추가하여 이 기능을 확장한다. SSO 토큰에 대한 자세한 정보는 웹 사용자 인증을 최소화하기 위해 싱글 사인온 구현의 내용을 참조할 수 있다.

4. 결론

전파를 직접적으로 이용 하는 사용자들이 급격히 늘면서 집단의 의해서가 아닌 개인 사용자들끼리의 전파 방해 간섭 교란 등 일어나면서 각종 사고들이 빈번하게 일어나고 있지만 개인 사용자들의 가이드라인이나 미흡하여 많은 문제를 야기하고 있다. 전파 교란과 교섭을 막기 위한 방안으로 백색광 광원과 투영격자와 광원으로 측정한 생성한 3차원 형상도를 이용한 생체정보인 영사식 무아레를 이용한 얼굴인식 정보를 이용한 암호화된 토큰을 만들어 토큰링을 통한 정보의 수신여부를 결정하여 인증 강도, 호출자의 정보 등을 포함한 동적 보안 속성을 가진 수평 전파를 전송하고 java직렬화와 직렬화 해제 기능을 사용하여 토큰의 고유성 여부를 확인함으로 인해 기존의 수평전파 교란으로 인한 송수신의 문제점을 보완할 뿐만아니라 다중보완의 간소화로 인한 전파송신의 속도 향상을 기대한다. 다양한 기기들의 각기 다른 전파의 위협을 모두 충족하기에 미흡한 부분이 있어 향후 연구를 통하여 좀더 세밀한 방안에 대한 연구가 필요하다.

REFERENCES

[1] G. G. Kim & D. S. Kim, (2001). An Analysis of Anti-jamming Capability of Frequency Hopping Satellite Communication Systems, *The Journal of Korean Institute of Communications and Information Sciences, 26(1),* 34-41.

[2] K. S. Kang & C. S. Kim. (2017). Mutual Coupling Compensation and Direction Finding for Anti-Jamming 3D GPS Antenna Array ,*The Korean Institute of Communications and Information Sciences,* 723-730.
DOI : 10.7840/kics.2017.42.4.723

[3] D. W. Lim. (2013). Case Study of Incidents by GPS Interferences and Trend for Monitoring Techniques,*Current Industrial and Technological Trends in Aerospace, 11(1),* 169-176.

[4] E. J. Kang & B. J. Park. (2009). A Study on Enhancing the Performance of Detecting Lip Feature Points for Facial Expression Recognition Based on AAM ,*PKorea Information Processing Society)* , 299-308.
DOI : 10.3745/KIPSTB.2009.16-B.4.299

[5] W. J. Ryu, Y. J. Kang, H. M. Rho & D, H. Lee. (2005). A Study on 3-D Shape Measurement and Application by using Digital Projection Moiré (Ⅰ), *Journal of the Korean Society for Precision Engineering, 22(7),* 88-93.
DOI : 10.1016/j.ijleo.2006.12.016

[6] W. J. Ryu, Y. J. Kang, H. M. Rho & D. H. Lee. (2007). A Study on 3-D Shape Measurement and Application by Using Digital Projection Moiré (Ⅱ), *Journal of the Korean Society for Precision Engineering, 24(5),* 62-67.

[7] W. J. Ryu & Y. J. Kang. (2005). Shape Measurement Method by using Moiré Phenomenon, *Journal of the Korean Society for Precision Engineering, 22(4),* 7-12.

[8] C. R. Seo, J. P. Lee, K. H. Lee, Y. B. Jeon & J. S. Park, (2017), A Proposal for Improvement of Detection of User Based on Facial Authentication Using Digital Projection Moire, *KIPS_C2017B0117,* 366-367.

[9] P. S. Jeong & Y. H. Cho, (2018). User Authentication System based on Auto Identification and Data Collection, *Journal of the Korea Institute of Information and Communication Engineering , 22(1),* 75-82 .
DOI : 10.6109/jkiice.2018.22.1.75

[10] Y. W. Moon, D. S. Pan & S. B. Seo. (2011). A Practical Implementation of Fuzzy Fingerprint Vault, *KSII Transactions on Internet and Information Systems, .5(10),* 1783-1798
DOI : 10.3837/tiis.2011.10.006

[11] S. H. Han. (2008). A Study on certification plan on Radio Frequency Identification for Airplane Use, *Aerospace Engineering and Technology, 7(1),* 236-244.

[12] S. P. H & S. J. Han, (2012). Wireless LAN System based on IEEE 802.1x EAP-TLS Authentication Mechanism, *The Korea Institute of Information and Commucation Engineering, 16(9),* 1983-1989.
DOI : 10.6109/jkiice.2012.16.9.1983

[13] Y. J. Kim, D. S. Moon, S. B. Pan, Y. W. Chung & K. I. Chung. (2003). Implementation of Embedded Biometrics Technologies: A Case of a Security Token for Fingerprints, *The Institute of Electronics Engineers of Korea - Computer and Information, 40(6),* 39-46.

[14] B. K. Lee, M. S. Kim & J. H. Seo. (2015). Design and Implementation of The Capability Token based Access Control System in the Internet of Things, *Journal of the Korea Institute of Information Security & Cryptology, 25(2),* 439-448.
DOI : 10.13089/JKIISC.2015.25.2.439

[15] S. A. Park, C. J. Chae, H. J. Cho & J. K. Lee. (2012). Public Key Infrastructure of Electronic Bidding System using the Fingerprint Information, *Journal Of The Korea Contents Association, 12(2),* 69-77.
DOI : 10.5392/JKCA.2012.12.02.069

이 수 연(Lee, Su Yeon) [학생회원]

・2014년 3월 ~ 현재 : 백석대학교 정보통신학부
・관심분야 : 정보보호
・E-Mail : lsuy0530@naver.com

이 근 호(Lee, Keun Ho) [종신회원]

・2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
・관심분야 : 블록체인, 이동통신 보안, 융합 보안, 개인정보보호, IoT 보안
・E-Mail : root1004@bu.ac.kr