Journal of the Korea Industrial Information Systems Research Vol. 22 No. 6, Dec. 2017 :17-22
http://dx.doi.org./10.9723/jksiis.2017.22.6.017 ISSN:1229-3741

영상처리를 이용한 비밀번호 인식시스템 개발

(Implementation of OTP Detection System using Imaging Processing)

최 영 빈[1], 김 지 혜[2], 김 진 욱[3], 문 병 현[4]*
(Yeong-Been Choe, Ji-Hye Kim, Jin-Wook Kim, and Byung-Hyun Moon)

요 약 본 논문은 일회용 암호(OTP: One Time Password)와 같은 비밀번호의 입력 시 발생할 수 있는 비밀번호 훔쳐보기(Shoulder-Surfing)를 대비하고 비밀번호의 보안성을 높이기 위해 영상을 비밀번호로 대체하는 인식시스템을 개발하였다. 영의 인식율울 개선하기 위하여 영상처리 기술 중 하나인 모폴로지 기법을 사용하였다. 이미지의 인식율을 높이고 잡음을 제거하기 위하여 모폴로지 연산인 침식과 팽창 연산을 4회 실시하여 2진 영상의 잡음을 제거하였다. 도트매트릭스에 나타난 영상에서부터 비밀번호를 인식하는 앱을 개발하고 인식률을 측정하였다. 어두운 조명 환경(1 Lux이하)에서 2진 영상 비밀번호 인식율이 최소90% 달성됨을 확인하였다.

핵심주제어 : 훔쳐보기 공격, 일회용비밀, 영상처리, 모폴로지기법, 침식연산, 팽창연산

Abstract In this paper, a password recognition system that can overcome a shoulder-surfing attack is developed. During the time period of password insertion, the developed system can prevent the attack and enhance the safety of the password. In order to raise the detection rate of the password image, the mopology technique is utilized. By adapting 4 times of the expansion and dilation, the niose from the binary image of the password is removed. Finally, the mobile phone application is also developed to recognize the one time password and the detection rate is measured. It is shown that the detection rate of 90% is achieved under the dark light condition.

Key Words : Shoulder-surfing Attack, One Time Password, Image Processing, Mopology Techniques, Erosion, Dilation

1. 서 론

최근 IT기술의 발전으로 전자제품의 소형화와 이동성이 더욱 가속화되고 있고 스마트폰, 태블릿을 사용한 보안매체에 관한 기업들의 투자와 관심이 집중되고 있다. 특히 Non-ActiveX 등과 같이 고객들이 최대한 불편함을 느끼지 않게끔 하기 위해 다양한 방식으로 프로그램들이 개발되어지고 있다. 또한 기존보다 보안성은 한 단계 더 강조되고, 사용자들의 접근성은 더 간편해져야 한다고 생각되어진다. 이러한 무선기기의 보

* Corresponding Author : bhmoon@daegu.ac.kr
Manuscript received November 28, 2017 / revised December 13, 2017 / accepted December 22, 2017
+ 이 논문은 대구대학교 DU-리더스 학부생 연구지원 사업에 의해 진행된 연구임.
1) 대구대학교 정보통신공학과
2) 대구대학교 정보통신공학과
3) 대구대학교 정보통신공학과
4) 대구대학교 정보통신공학과, 교신저자

편적인 사용과 더불어 다양한 종류의 보안위협으로 인한 안전한 비밀번호의 입력시스템의 필요성이 증가하고 있다. 보안의 위협은 온라인 형태의 위협과 오프라인 형태의 위협으로 구분할 수 있다. 온라인 형태의 보안위협은 통신채널의 부당한 형태로 정보를 가로채거나, 정보를 위조나 변조하는 형태이다. 오프라인 형태의 보안 위협은 통신 채널을 이용하지 않는 상태에서 보안의 위협이 되는 행위이다. 대표적인 오프라인 형태의 보안위협이 비밀번호 훔쳐보기(Shoulder Surfing)이다. 특히, 아파트의 현관문에 설치된 비밀번호 입력시스템의 경우, 불법으로 설치된 영상기록장치에 의한 비밀번호의 노출이 발생할 수 있다. 이러한 공격에 대비하기 위한 비밀번호 대체용 이미지에 대한 연구가 필요하다. 본 논문에서는 비밀번호 이미지가 노출될 경우를 대비하여 동일한 이미지가 매번 다른 비밀번호를 나타내는 비빌번호 영상처리 시스템을 연구하였다.

비밀번호 훔쳐보기를 방지하기 위하여 다양한 연구가 진행되었다. 비밀번호를 입력할 때 숫자뿐만 아니라 색깔까지 암호로 취급하는 색깔핀을 사용하는 방법이 Alexander Luca에 의해 제시되었다[1]. 따라서 은행거래용 보안인증 매체인 보안카드는 시대에 뒤쳐져 점차 사라지고 있고 일회용 암호 생성기(OTP : One Time Password)의 중요성이 강조되어지고 관심이 높아지고 있다. 최근 안드로이드 기반의 이동통신기기에서의 은행업무용 애플리케이션은 점차 활용도가 높아기고 있는 실정이지만 안전하지 않은 점이 많다. 특히 비밀번호 훔쳐보기 공격은 비디오 영상을 통하여 발생하기도 한다. 이러한 비밀번호 훔쳐보기에 대응하기 위하여 그림을 사용한 보안시스템(Graphical Password Authentication)을 사용하는 연구되고 있다[2-5]. 또한, 인지심리학에 기초한 비밀번호 훔쳐보기로부터 안전한 기술인 역동 인증 체계(DAS)로 불리는 비밀번호 입력시스템의 설계 및 구현이 제안되었다[6]. 모바일 환경에서 훔쳐보기 공격과 무작위적 공격을 방어할 수 있는 스도쿠(Sudoku)퍼즐을 이용된 숫자배치법의 비빌번호입력시스템 제안되었다[7].

본 논문에서는 비밀번호의 입력 시 필요한 보안의 강화를 위하여 숫자에 해당하는 비밀번호에 대응되는 숫자를 표시하는 8X8 LED 매트릭스에 표시하고 해당되는 숫자에 점등된 패턴을 인식하는 앱을 개발하였다. 본 연구에서는 비밀번호 훔쳐보기에 대한 위협을 강화하고 인식율을 높이기 위하여 8X8 매트릭스의 랜덤한 열의 점등된 부분은 사용하지 않도록 하여 보안을 훔쳐보기 공격으로부터 강한 비밀번호 입력시스템을 구현하였다. 또한 개발된 앱에서는 숫자의 인식율을 높이기 위하여 모폴로지 기법을 이용하여 점등패턴의 잡음을 제거하고 비밀번호에 해당되는 비밀번호를 입력하는 앱을 개발하여 테스트하였다. 2절에서는 비밀번호를 발생시키는 하드웨어의 구성과 비밀번호를 나타낸는 원본영상과 2진화된 영상을 설명하고 2진화된 영상의 잡음을 제거하기 위하여 모폴로지 기법에 해당하는 침식연산과 팽창연산을 설명하였다. 이진 영상에서 비밀번호의 변환과정이 소개된다. 3절에서는 이진 영상을 핸드폰 앱으로 인식하고 성능을 평가하였다. 마지막으로 4절에서는 결론에 대하여 설명하였다.

2. 영상처리를 이용한 난수인식기

2.1 비밀번호 영상생성기

Fig. 1에서 보는 바와 같이, 아두이노 우노를 사용하여 숫자에 해당하는 비밀번호에 대응되는 숫자를 표시하는 8X8 LED 매트릭스에 표시하는 하드웨어를 설계하였다. 8X8 LED 중에서 핸드폰을 사용하여 획득한 영상의 정확한 위치를 정하기 위하여 8X8 LED 중에서 첫 번째 열과 1번째 행은 항상 꺼지도록 설계되었다. 또한 2번 째 열과 2번 째 행의 정해진 위치는 항상 점등되도록 설계하여 영상의 정확한 위치 선정에 도움이 되도록 하였다. 따라서 3번째 행에서 7번째 행의 3열에서 7열까지 총 20개의 LED를 사용하여 비밀번호를 나타내도록 설계되었다.

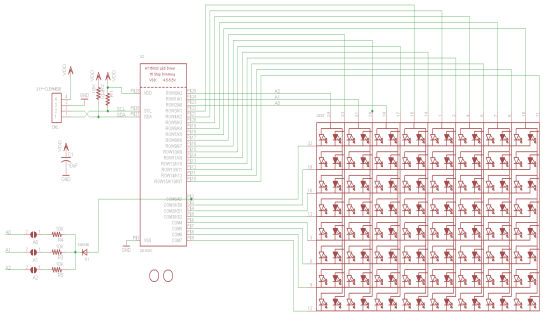


Fig. 1 LED Hardware for Password.

2.2 2진화 비밀번호 영상

Fig. 1에서 보는 하드웨어를 사용하여 비밀번호에 해당하는 원본 영상의 기본 색상 모델인 RGB 컬러 모델에서 HSV 컬러 모델로 변환 한다. Fig. 2 에서는 난수알고리듬에 의하여 생성된 8X8 도트매트릭스의 원본영상과 2진화된 영상을 보여준다. Fig. 3 은 이진화된 영상의 비밀번호에 해당하는 LED의 켜짐과 꺼짐을 구분하기 위하여 영상기준값을 127, 180 및 230으로 변경하여 영상을 관찰한 결과를 나타낸다. Fig. 2에서 보는바와 같이 기준값 127과 230에서의 차이를 확인할 수 있다.

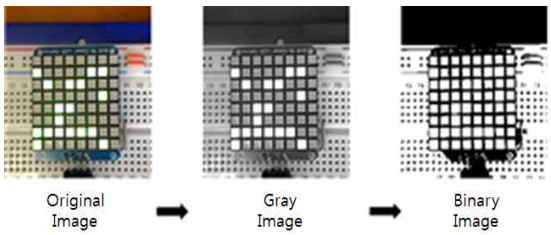


Fig. 2 Binary Image for a Password.

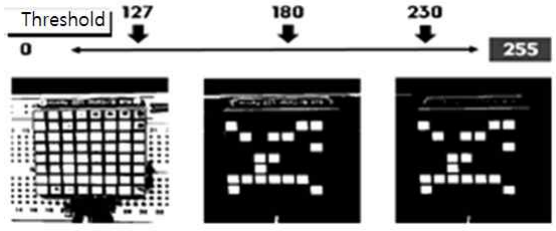
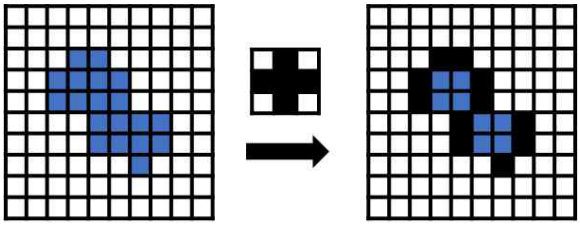


Fig. 3 Binary Image with Different Values of Threshold.

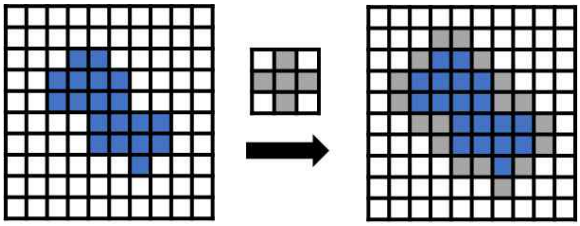
2.3 잡음제거를 위한 모폴로지 연산

Fig. 4는 모폴로지를 사용한 침식연산과 팽창연산의 예를 나타내었다. 이진 영상의 모폴리지 기법 사용했을 때 결과 영상에서 흰색 영역이나 검은색 영역이 원하는 의도보다 넓거나 좁게 얻어질 수 있다. 최적의 문턱값을 사용하면서 잘못된 분리 영역은 후처리 과정을 통하여 결과를 수정하는 기법을 많이 사용하는 데 이를 모폴로지 처리라고 한다. 모폴로지 처리는 대상 영역이 좁아지는 침식 연산, 대상 영역이 넓어지는 팽창 연산, 대상 영역에서 세부 영역이 제거되는 열림 연산, 빈틈이 채워지는 닫힘 연산이 있다. 일반적으로 대상 영역은 이진 영상에서 흰색으로 표시된 영역을, 회색조 영상에서는 밝은 영역을 가리킨다. 침식과 팽창 연산은 기본적인 연산에 해당하며 열림과 닫힘 연산은 침식과 팽창 연산의 조합으로 구성된다.

이진 영상의 침식연산은 입력한 이진 영상의 각 픽셀에 마스크를 놓았을 때 마스크가 255값을 가지는 모든 픽셀 위치에 대하여 입력 영상도 255 값을 가져야만 결과값이 255가 되는 연산이다. 만약 대상 위치에서 한 픽셀이라도 0 값을 가지면 결과값은 0이 되기 때문에 전체적으로 255값을 가지는 영역이 줄어드는 결과가 나타난다. 팽창 연산은 침식 연산과 반대로 마스크 영역 내 입력 영상 픽셀의 최댓값을 구하는 것이다. 입력 영상에서 마스크가 걸친 영역 가운데 가장 밝은 픽셀 값이 결과 픽셀로 저장되기 때문에 결과 영상은 밝은 영역이 확대되고 어두운 영역이 축소된다. 팽창 연산도 침식 연산과 마찬가지로 마스크에 값을 지정할 수 있는 데 팽창 연산에서는 마스크 원소 값을 입력 영상의 각 픽셀에 더하고 나서 더한 값의 최댓값이 결과 픽셀 값이 된다.



(a) Example of Erosion



(b) Example of Dilation

Fig. 4 Example of Erosion and Dilation.

Fig. 5에서는 핸드폰에서 획득된 영상에서 빨간색 박스로 표시된 잡음을 나타내었다. 이러한 잡음을 제거하고 원하는 영상을 얻기 위해서는 도트매트릭스 주변에 잡음을 제거해야한다. 이를 위해서 Fig. 4에서 설명된 침식연산과 팽창연산을 실시하였다.

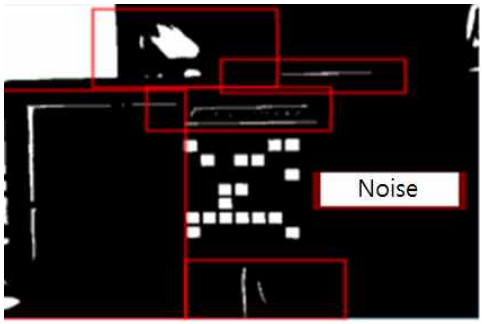


Fig. 5 Password Image with Noise.

Fig. 6에서는 침식연산을 통해 도트매트릭스 주변의 잡음을 제거하기 위하여 침식연산을 4번 실행하였다. 잡음이 제거된 침식된 영상에서 팽창연산을 4회 실시하여 개선된 비밀번호 영상을 보여준다.

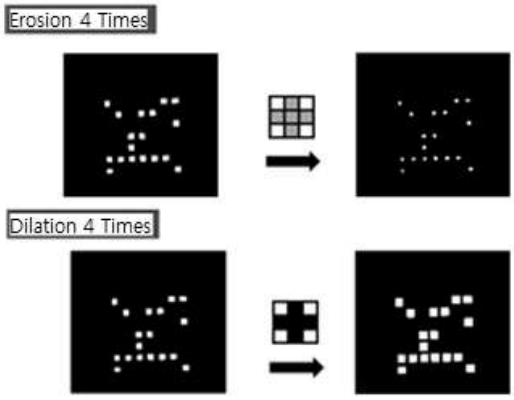


Fig. 6 Images with 4 Times of Erosion and Dilation.

2.4 이진화된 이미지에서 비밀번호 변환

Fig. 7에서는 비밀번호 영상을 나타내는 도트매트릭스를 나타내었다. 그림에서 보는바와 같이 푸른색으로 표시된 1행과 1열은 항상 LED가 꺼져있도록 설계되었다. 그리고 노란색으로 표시된 2행의 2, 4, 8열은 항상 LED가 켜져 있도록 설계되어 비밀번호 영상을 획득할 때 바른 위치를 선정하도록 설계되었다. 3행의 2열과 8행의 2, 7, 8열 또한 항상 LED가 켜져 있어 영상의 위치 선정에 도움이 되도록 설계되었다. 따라서 비밀번호에 해당하는 부분은 3행에서 7행까지 3열에서 7열까지의 20개 LED를 활용하여 비밀번호를 나타내도록 하였다. Fig. 7에서 나타난 바와 같이 “1”은 LED가 켜져 있는 부분을 나타내고 “0”은 LED가 꺼져 있는 부분을 나타낸다. Fig. 7의 좌측 영상은 영상을 인식하여 비밀번호 429289를 앱으로 나타낸 영상이다. Fig. 8 은 영상에서 비밀번호를 변환하는 테이블을 나타내었다. 비밀번호의 훔쳐보기 공격으로부터 보안강화를 위하여 아래와 같은 규칙을 정하였다. 첫째, 파란색으로 나타난 7번 째 행의 3열에서 7열까지의 5개 비트는 영상에서 사용하지 않는 부분으로 3열에서 7열까지 랜덤하게 위치 할 수 있도록 하였다. 둘째, 발간색으로 표시된 4행의 20개 비트 또한 영상이 발생될 때 마다 랜덤하게 행의 위치를 바꾸도록 하여 훔쳐보기 공격으로부터 보안을 강화하도록 하였다. 또한 영상에서 비밀전호로 변환할 때 켜

진 부분은 “0”으로 꺼진 부분은 “1”로 변환하여 10진수로 나타내도록 하였다.

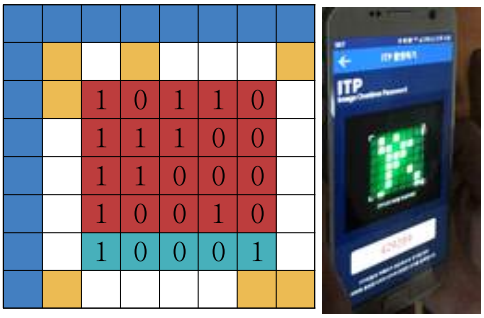


Fig. 7 A Password Image(Password: 429289)

Fig. 8은 2진 영상 “1”과 “0”에 해당하는 비트의 2진수의 지수를 나타내었다. 그림 7.에서 “1”로 표시된 부분은 LED가 켜진 부분으로 그림 8.에서 초록색으로 표시되어 있으며 “0”으로 표시된 부분은 LED가 꺼진 부분으로 Fig. 8 에서 회색으로 표시 되었다. 이진 영상을 비밀번호 429289로 변환시 에는 영상에서 켜진 부분은 “0” 꺼진 부분은 “1”로 변환하여 2진수로 MSB에서 시작하여 LSB로 5비트씩 나타내면 01101/00011/00111/01001로 표현되면 10진수로 429289를 변환되도록 하였다. Fig. 8 에서와 같이 2진수의 지수의 위치는 비밀번호가 생성될 때 마다 행의 위치가 무작위로 변화시켜 훔쳐보기 공격으로부터 안전하도록 설계하였다.

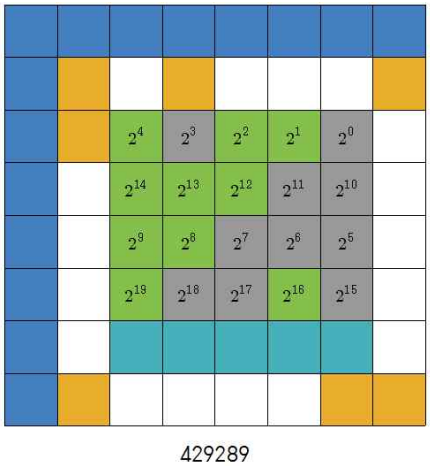


Fig. 8 Password Transformation Table (Password: 429289)

3. 성능 평가

Fig. 9와 같이 잡음이 제거된 영상의 비밀번호를 인식하기 위한 안드로이드 스튜디오를 사용하여 앱을 개발하였다. Table 1.은 다양한 환경에서 비밀번호를 100번 실시하여 올바르게 인식된 횟수를 나타내었다. Fig. 3에서 기준 임계값에 따라 획득된 영상을 사용하여 실내 조명이 아주밝음(70 Lux이상), 보통밝음(5-30Lux) 및 조명이 없는 상태(1 Lux 이하)에서 비밀번호를 인식하도록 하였다.

Table 1 Password Detection Rate.

기준 임계값	아주밝음 (70LUx 이상)	보통밝음 (5-30 Lux)	어두움 (1 Lux 이하)
127	0	0	0
180	0	0	33
230	21	62	90

Fig. 9의 좌측 영상에서는 비밀번호 에서 나타난 바와 같이 8X8 도트매트릭스에 나타난 영상은 번호 572470으로 인식되어 잡음을 제거하고 생성된 비밀번호를 영상으로 표현하였고, 영상에 해당하는 비밀번호를 성공적으로 앱에서 인식하여 비밀번호로 사용 가능함을 보였다.

Fig. 9 Image of Password Detection

4. 결 론

본 연구는 훔쳐보기와 같은 비밀번호 공격을

대비하여 영상처리 기술을 이용해 보안 인증 가능한 연구모델을 제시하였다. 비밀번호에 해당하는 영상을 생성하고 영상처리 기술의 방식 중 모폴로지 기법을 통해 이미지의 침식, 팽창연산을 통해 영상의 인식률을 높이도록 하였다. 핸드폰 앱을 개발하여 획득된 영상을 1 Lux 이하의 어두운 환경에서 비밀번호 인식률이 90% 가능함을 보였다. 향후 밝은 실내조명에서 인식률을 높일 수 있는 추가적인 연구가 필요하다.

References

[1] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hussmann, "Vibrapass: Secure Authentication Based on Shared lies," *Proc. of CHI,* 2009, pp. 913-916.

[2] Gurav, Shraddha M., Leena S. Gawade, Prathamey K. Rane, and Nilesh R. Khochare, "Grahphical Password Autherntication: Cloud Securing Scheme, " IEEE Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2016, pp. 479-483.

[3] T. S. Wu, M. L. Lee, H. Y. Lin and C. Y. Wang, "Shoulder-Surfing-Proof Graphical Password Authentication Scheme," International Journal of Information Security, Vol. 13, 2014, pp. 245-254.

[4] N. H. Zakaria, D. Griffiths, S. Brostoff and J. Yan, "Shoulder Surfing Defence for Recall-Based Graphical Passwords," in Proceedings of the Seventh Symposium on Usable Privacy and Security, p. 6, 2011.

[5] B. Kang, B. Kim and K. Kim, "Securing the Private Key in the Digital Certificates Using a Graphic Password, " The Journal of Society for E-business Studies, vol. 16, No. 4, 2011, pp. 1-16. Usable Privacy and Security, p. 6, 2011.

[6] N. H. Zakaria, D. Griffiths, S. Brostoff and J. Yan, "Shoulder Surfing Defence for Recall-Based Graphical Passwords," in Proceedings of the Seventh Symposium on Usable Privacy and Security, p. 6, 2011.

[7] B. Kang, B. Kim and K. Kim, "Securing the Private Key in the Digital Certificates Using a Graphic Password, " The Journal of Society for E-business Studies, vol. 16, No. 4, 2011, pp. 1-16. Usable Privacy and Security, p. 6, 2011.

최 영 빈 (Yeong-Been Choe)

- 학생회원
- 대구대학교 통신공학전공

김 지 혜 (Ji-Hye Kim)

- 학생회원
- 대구대학교 통신공학전공

김 진 욱 (Jin-Wook Kim)

- 학생회원
- 대구대학교 통신공학전공

문 병 현 (Byung-Hyun Moon)

- 1985년 6월 : Southern of Illinois University 전자공학과 (공학사)
- 1987년 6월 : University of Illinois(Urbara-Campaign) 전자공학과 (공학석사)
- 1990년 12월 : Southern Methodist University 전자공학과 (공학박사)
- 1991년 9월~현재 : 대구대학교 정보통신공학부 교수
- 관심분야: 통신이론, 무선통신