금융기관에서 사용하는 지문인식 기반 OTP 시스템 개발

한상훈*, 이채영O
*한경국립대학교 컴퓨터응용수학부,
O한경국립대학교 평택캠퍼스 컴퓨터공학과
e-mail: hansh0903@hknu.ac.kr*, clairech1119@naver.comO

Development of Fingerprint Recognition-Based OTP System for Financial Institutions

Sang-Hoon Han*, Chea-Young LeeO
*School of Computer Engineering & Applied Mathmetics, Hankyong National University,
ODept. of Computer Engineering, Hankyung National University Pyeongtaek Campus

● 요 약 ●

본 논문은 기존의 OTP(One-Time Password) 시스템의 한계와 약점을 해결하기 위하여 지문인식을 활용한 OTP 시스템에 대하여 연구를 진행하였다. OTP 시스템 자체가 높은 보안성을 가지고 있지만, 은행에서 발급하는 OTP는 생성 버튼만 누르면 비밀번호가 생성되기 때문에, 분실 및 도난 상황에서 2차 인증에 대한 보안이 허술해 질 수 밖에 없다. 본 연구에서는 지문인식 기반 OTP 시스템의 개발 방법을 마련하여 사회적으로 보안에 대한 인식을 높이고, 동시에 사용자의 편의성을 높이기 위한 방법을 제시하고자 한다.

키워드: 생체인식(biometric), 지문(fingerprint), 보안(security), 일회용비밀번호(One-Time password)

I. Introduction

4차 산업시대에 들어섬에 따라 현대 사회에서 정보 보안은 점점 더 중요한 이슈로 부각되고 있다. 최근 보이스 피싱과 스미싱 등의 금융 사기가 잇따르자 금융기관에서는 OTP 카드 사용을 추진하는 추세이며, 기존의 OTP카드는 무한으로 재 생성되는 인증번호 덕분에 안정성이 매우 우수하다는 평가를 갖고 있지만 누구든 접근이 가능하여 보안성이 약하다는 지적을 해결하기 위해 지문과 같은 생체 인식 기술을 활용하여 문제점을 해결하고자 지문인식 기반의 OTP 카드를 고려하였다. 지문인식 기반의 OTP를 통해 사회적으로 보안에 대한 인식을 강화시키며 사용자의 편의성을 동시에 해결하고자 한다[1].

OTP 시스템은 일회용 비밀번호를 생성하여 본인 확인을 수행하는 보안 시스템으로, 난수 발생기와 현재 시간을 이용하여 비밀번호를 생성한다. 이러한 OTP 시스템은 재사용이 불가능하며, 중간 과정에서의 데이터 유출 위험이 적다. 그러나 기존의 OTP 시스템은 누구나 접근이 가능하므로 보안성이 약한 측면이 있다. 이 런 문제를 보완하기 위해 지문인식 기술을 활용한 OTP 시스템을 연구하였다. 지문은 개인마다 고유한 패턴으로 구성되어 있으며, 지문인식은 이를 전자적으로 읽어 지문 데이터를 비교하여 본인 인증에 사용하는 기술이다. 따라서 지문인식을 통한 OTP 시스템은 개인의 신체적 특성을 활용하여 보다 안전하고 강한 보안성을 제공할 수 있다.

2장에서는 기존 연구에 대한 소개를 하고, 3장에서 제안 시스템에 대한 설명과 결과를 소개하고, 4장에서 결론을 맺는다.

II. Preliminaries

1. 지문인식 기술 및 적용 사례

지문인식은 개인마다 모두 다른 값을 고유하게 갖는 패턴으로 구성된 지문을 활용하여 인증을 수행하는 기술이다. 지문인식 기술은 지문을 전자적으로 읽어 입력된 데이터와 비교해 본인 여부를 확인한다. 지문인식 방식에는 정전식, 광학식, 초음파식이 있다[2,3,7]. 이를 분실 시 사용자의 개인 정보와 중요한 데이터가 도용될 수 있는 USB에 적용할 수 있다. 지문을 항상 사용자와 함께 있으며, 비밀번호를 기억할 필요 없이 USB 드라이브에 손쉽게 액세스 할 수 있다. 중요한 파일이 들어 있다면. 분실이나 도난 등에 의해서도 파일을 안전하게 보호 할 수 있을 것으로 본다. 그림 1에서 보는바와 같이 USB 장치에 지문인식 장치를 부착하여 보안성을 높이는 방향으로 제품들이 나오고 있다[4,5].

Fig. 1. 지문인식 USB

지문인식 USB외에도 카드에 생체인식을 넣은 생체인증 카드가 있다. 이 생체인증카드는 하드웨어적으로 구현된 보안 칩과 지문센서 그리고 보안 프로세서 기능을 통합하여 단일 칩으로 구성하였다. 하드웨어 보안 칩은 강력한 보안성을 확보하기 위해 지문정보를 암호화하였으며, 사용자의 안전한 결재를 위해서 비밀번호/PIN 번호 입력이 필요 없어진다. 생체정보(지문)를 통해 본인 인증을 하기 때문에 카드 도난이나 분실로 인한 피해를 효과적으로 예방할 수 있다. [6,8,9,10].

Fig. 2. 생체인증 카드

그림 2처럼 IC카드에 생체인식 방법 중 하나인 지문인식을 활용해 보안과 편의성을 모두 해결할 수 있다. 그림 2는 삼성에서 개발하고 있는 지문 인증 IC카드의 실제 예이다. 이렇게 OTP에도 이와같이 지문인식을 활용한다면 기존의 OTP보다 보안성이 뛰어난 OTP 시스템이 될 것으로 본다.

2. OTP의 기능 및 특징

OTP(One-Time Password)는 보안 시스템으로, 난수 발생기와 시간 동기화 알고리즘에 따라 매 시간마다 변경되는 일회용 비밀번호를 생성하여 예측하지 못하도록 하여 비밀번호 인증에 활용한다. 접속 시 필요한 비밀번호를 바로 생성하여 그 번호를 통해 본인 확인을 하는 방식이다. 주로 현재 시간을 활용하여 난수 발생기를 통해 OTP 비밀번호를 생성한다. OTP는 노출되더라도 재사용이 불가능하며, 서버와의 접속 없이도 생성이 가능하여 중간 과정에서 패킷 유출 등의 위험이 발생하지 않는다[11].

OTP는 크게 HOTP와 TOTP로 나뉜다. HOTP는 HMAC(Hash-based Message Authentication Code) 알고리즘을 사용하여 구현한다. HOTP는 counter 값을 기준으로 HOTP가 요청되고 검증될 때마다 증가한다. 생성된 코드는 다른 코드를 요청하고 인증 서버에서 유효성을 검사할 때까지 유효하다. OTP 생성기와 서버는 코드가 검증되고 사용자가 액세스 권한을 얻을 때마다 동기화가 된다. TOTP는 HOTP를 기반으로 만들어졌으며 HOTP와 마찬가지로 정적이지만 HOTP와는 다르게 시간(time)기반이라는 점이다. 이 알고리즘은 공유 비밀 키와 시간을 사용하여 일회성 비밀번호 값을 생성한다. 현재 많이 사용되고 있는 OTP는 대부분 TOTP를 기반으로 작동되고 있다.

III. The Proposed Scheme

현재 금융기관에서는 카드형과 토큰형 OTP를 주로 사용하고 있다. OPT 자체가 높은 보안성을 유지하고 있어서 매우 중요한 인증수단으로 사용되고 있다. 본 연구에서는 여기에 OTP의 도난 및 분실을 가정하여 보았다. 현재 OTP는 비밀번호를 생성하는 기능이 버튼을 누르면 바로 실행되고 6자리 번호를 얻을 수 있다. 타인이 나의 OTP를 이용한다면, 어떻게 될지 생각하여 본다면 좋은 상상은 아닐 것이다. 이런 관점에서 지문인식 장치를 OTP에 적용하여 비밀번호를 생성하는데 버튼이 아니라 사용자의 지문을 통하여 본인만 비밀번호를 생성할 수 있도록 하여 좀 더 높은 보안성을 유지 할 수 있을 것으로 본다.

1. 지문인식 기반 OTP의 설계

지문인식 기반 OTP 시스템은 콘트롤러, 지문인식기, 비밀번호 생성기로 구분할 수 있다. 본 연구에서는 실현가능성과 사용성을 제시하고자, 콘트롤러는 Arduino UNO, 릴레이모듈, 12C방식 LCD 제어기를 사용하였다. 아두이노 UNO는 ATmega328기반의 마이크로 컨트롤러 보드로 필요한 모듈들이 내장되어 있어서 간편하게 컴퓨터와 USB 케이블로 연결할 수 있다. 릴레이 모듈에서 릴레이는 전자석의 원리를 이용하여 전자기유도 원리를 이용한 것이다. 즉, 이 원리를 이용해 스위치 역할로써 사용을 한다. LCD는 2열 디스플레이 장치를 사용하였다.

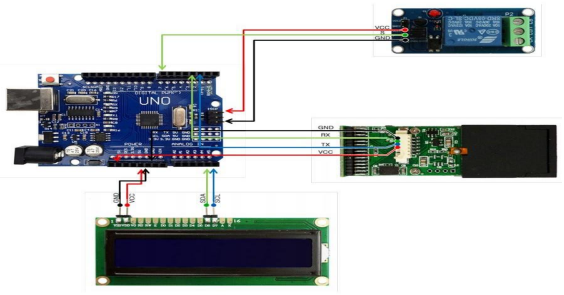

Fig. 3. 아두이노를 활용한 지문 OTP 회로도

그림 3이 아두이노를 활용한 지문인식 기반 OTP의 연결 회로도이다.

지문인식 모듈은 광학식 센서를 활용하여 가시광선에 의해 반사된 지문 영상을 획득하는 방식을 사용한다. 그림 3에서 우측 중앙에 있는 장치가 지문 인식 장치이다. 지문인식 장치에는 지문을 등록하고 등록된 지문을 인식하는 과정을 지원하고 있으며, 등록된 지문 사용자가 지문인식을 통하여 인증이 되었을 때 TOTP(Time-based OTP)에 의해서 비밀번호를 생성한다. 그림 4는 시스템의 전체적인 흐름도를 보여준다.

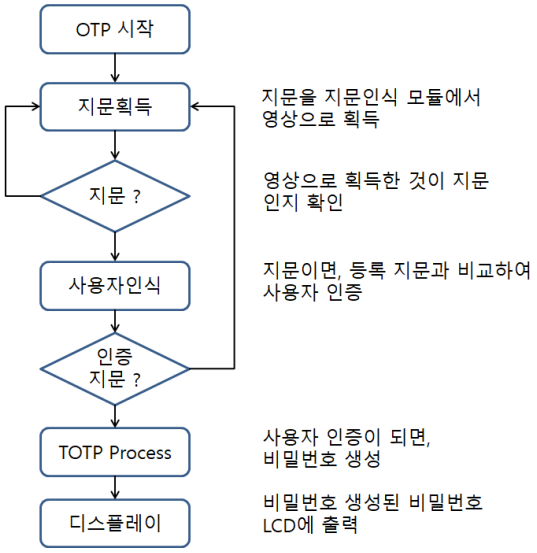

Fig. 4. 시스템 흐름도

그림 5는 아두이노를 활용해 지문을 등록하는 함수이다. finger.getImage()를 호출하여 지문 센서에 유효한 지문을 기다리고 getImage()의 결과 p를 확인하여 처리한다. FINGERPRINT_OK의 경우 이미지 캡처 성공 메시지를 출력한다. 이미지가 캡처된 후 finger.image2Tz(1)를 호출하여 이미지를지문 템플릿으로 변환하고 image2Tz()의 결과 p를 확인하여 처리한다. FINGERPRINT_OK의 경우 이미지 변환 성공 메시지를 출력한다. 그 후 변경된 지문 템플릿을 finger.storeModel(id)를 호출하여 지정된 ID에 저장한다. storeModel()의 결과 p를 확인하여 FINGERPRINT_OK의 경우에만 지문 템플릿 저장 성공 메시지를 출력한다.

```
uint8_t getFingerprintEnroll(uint8_t id) {
  uint8_t p = -1;
  //이미지 캡처를 위해 지문 센서에 유효한 지문을 기다린다
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
      case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
      //생략
      //이미지가 캡처되었으므로 이미지를지문 템플릿으로 변환한다.
      p = finger.image2Tz(1);
      switch (p) {
        case FINGERPRINT_OK:
        Serial.println("Image converted");
        break;
        //지문 템플릿을 저장한다.
        p = finger.storeModel(id);
        if (p == FINGERPRINT_OK) {
          Serial.println("Stored!");
        }
        //생략
}
```

Fig. 5. 지문인식 모듈에서 지문등록 함수

지문 등록 완료 후 ID입력을 하여 OTP 번호를 생성한다. 이때는 TOTP Process를 통하여 서버와 동기화를 통하여 시간을 기반으로 일회용 비밀번호를 생성한다. 본 연구에서는 TOTP를 구현하기 위해서는 서버 부분도 구현되어야 하기 때문에 난수 발생기를 이용하여 LCD에 출력할 수 있도록 6자리의 숫자를 생성하는 것으로 처리하였다.

2. 지문인식 기반 OTP의 구현

그림 6에서는 본 연구에서 구현한 지문인식 기반의 OTP 시스템을 보여주고 있다. 개별 모듈의 크기는 크지 않으나 팩킹하는 과정에서 크기는 조금 커졌지만, 시스템의 기능에는 문제가 없음을 확인하였다.

OTP를 사용하기 위해서는 먼저, 지문 등록의 과정을 거친다. 이때는 사용자가 한명이기 때문에 사용되는 저장공간이 클 필요가 없다. 그리고, 지문 등록 후에 일회용 비밀번호를 얻기 위해서는 자연스럽게 지문인식을 통해서 등록된 지문과 일치하는 경우에 비밀번호를 생성하여 보여주도록 되어있다.

여기서, 좀 더 구현해야 할 부분이 있는데 다음과 같다.

1) 지문인식 데이터의 암호화
2) 저장공간의 파티션 단절
3) 크기의 소형화

등록된 지문데이터를 암호화하여 보관하는 기능과 지문인식에 인증을 통과하지 못하면, 데이터 파티션이 보이지 않도록 파티션을 단절 시킨다면, 분실된 경우에도 안전하게 폐기를 시킬 수 있을 것으로 본다. 마지막으로 크기를 작게하여 토큰형이나 카드형에 사용할 수 있도록 하는 부분이 남아있다.

Fig. 6. 아두이노를 활용해 만든 지문인식 기반의 OTP

IV. Conclusions

본 논문에서는 현대 사회에서 발생하는 보안 이슈에 대한 조금이나마 해결책을 제시하기 위해 지문인식 기반의 OTP 시스템을 연구하고 구현하였다. 아두이노 키트를 사용하여 실험실 버전을 개발하여 보았으며, 안전하고 신뢰성 있는 인증 방식을 제공함으로써, 기존의 비밀번호 기반 인증 시스템의 취약점을 보완하고자 하였다.

본 논문에서는 아두이노를 사용하여 지문인식 OTP 시스템을 개발하였지만, 보안성 측면에서 아직 부족한 점이 있다. 실제로는 TOTP 방식으로 서버부분과 함께 개발하여 제대로 동작하는 지문인식 기반의 시스템을 개발할 수 있도록 개선해야 할 것이다.

지문인식 기반의 OTP 시스템을 실제로 개발할 때에는 아두이노 외의 보안 기술과 암호화 알고리즘을 활용하여 일반 OTP와 같은 카드 형태의 지문인식 OTP를 구현할 수 있기에 미래에는 기존의 OTP 카드 형태를 취하는 지문인식 OTP 시스템의 개발이 가능할 것이라 생각한다. 이를 통해 보다 강력한 보안성을 갖춘 지문인식 기반의 OTP 시스템을 구현하고, 정보보안을 더욱 강화할 수 있을 것이다.

REFERENCES

[1] 정현희, 신동렬, “OTP를 이용한 사용자 계정 로그인 정보 관리 시스템 구현”, 한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호, 2014, 1, pp. 263-265.

[2] 구하성, “지문인식시스템”, 대한전자공학회지 제26권 제11호, 1999.11, pp. 24-31.

[3] 김원준, “지문 인식 및 위변조 검출에 관한 최신 기술동향”, 전자공학회지 제46권 제8호, 2019.8, pp. 31-38.

[4] 이규환, “지문인식 기술 및 응용제품”, 한국퍼지 및 지능시스템학회 2007년도 춘계학술대회 학술발표논문집 제17권 제1호, 2007. 4, pp. 273-273.

[5] 염기철, 노동건, “지문인식과 OTP정보를 이용한 이중 채널 인증 전자투표 시스템”, 2016년도 한국통신학회 동계종합학술발표회 논문집, 2016.01, pp. 466-467.

[6] 반성범, 정용화, 김호원, 박영수, “IC 카드를 이용한 생체인식 기술 개발 동향”, 정보과학회지 제19권 제7호, 2001.07, pp 14-21.

[7] https://news.samsungdisplay.com/18221

[8] https://www.etnews.com/20190625000254

[9] http://btbl.co.kr/products/

[10] https://semiconductor.samsung.com/kr/newsroom/tech-blog/biometric-card-ic- that-will-change-the-way-we-pay/

[11] http://directotp.com/WhatIsOTP.html