이미지 합성을 이용한 인증에 대한 연구

김수희* · 박봉주**

요 약

본 연구는 이미지 합성을 이용하여 서버가 사용자를 인증하기 위한 알고리즘을 개발하고 이를 구현한다. 서버는 사용자가 소지하는 사용자카드를 랜덤하게 점을 찍어 생성하고, 각 사용자에게 배포된 사용자카드의 정보를 유지하고 관리한다. 한 사용자로부터 인증요청이 들어오면, 서버는 그 사용자의 사용자카드 정보를 기반으로 서버카드를 실시간에 생성하여 사용자에게 송신한다. 서버카드는 각 인증마다 다르게 생성되므로 원타임 패스워드 챌린지(challenge) 역할을 한다. 사용자는 본인이 소유하고 있는 사용자카드와 서버로부터 송신된 서버카드를 겹쳤을 때 생성되는 이미지를 판독하여 인증을 수행한다. 이 논문은 보안성을 높이면서 이미지를 선명하게 형성하는 기법을 제시하고 이를 구현한다.

A Study on Authentication using Image Synthesis

Suhee Kim* · Bongjoo Park**

ABSTRACT

This research develops an algorithm using image synthesis for a server to authenticate users and implements it. The server creates cards with random dots for users and distribute them to users. The server also manages information of the cards distributed to users. When there is an authentication request from a user, the server creates a server card based on information of the user's card in real time and send it to the user. Different server card is generated for each authentication. Thus, the server card plays a role of one-time password challenge. The user overlaps his/her card with the server card and read an image(eg. a number with four digits) made up from them and inputs the image to the system. This is the authentication process. Keeping security level high, this paper proposes a technique to generate the image clearly and implements it.

Key words : Authentication, Image Synthesis, Server Card, User Card, One Time Pass Word

* 호서대학교 컴퓨터공학부 컴퓨터공학전공

** 호서대학교 컴퓨터공학부 정보보호전공

1. 서 론

인터넷 망을 포함하는 전산망의 환경이 급격하게 발전하면서, 인터넷상에서 구축되어 네트워크를 통해 연결되는 사용자들을 대상으로 온라인서비스를 제공하는 서버의 수가 급증하고 있는 추세이다.

이러한 서버, 특히, 금융권(은행, 증권회사 등)에 의해 구축되는 서버는 네트워크를 통해 접속한 사용자가 자신의 재산을 온라인상에서 출금하는 기능을 제공하고 있기 때문에, 현재 네트워크에 접속한 사용자가 정당한 사용자인가를 정확하게 판단해야 함은 물론이고, 네트워크에 접속한 사용자로부터 출금이 요청되었을 때 안전성 확보를 위하여 사용자가 권한이 있는 사용자인가를 재차 판단하는 과정이 필요하다.

온라인상의 출금은 본인이 소유하는 은행계좌의 잔액을 타 은행계좌로 이체시키는 행위, 자신의 증권계좌에서 주식을 매도하는 행위, 또는 증권계좌의 잔액을 타 은행계좌로 이체하는 행위 등이 될 수 있다.

이를 위해, 인터넷을 통해 은행 업무를 처리하는 인터넷 뱅킹 또는 주식거래를 위한 사이버 트레이딩(cyber trading)을 제공하는 서버들은, 사용자들에게 인증서를 배포하고 이 인증서를 통해 사용자에 대한 인증을 행하고 있다. 금융거래뿐만 아니라 온라인상으로 중요한 정보를 제공하거나 유료사이트로 운영되는 곳에서는 모두 사용자의 인증을 요구하고 있다.

Shannon의 이론에 의하여 원타임 패드는 완벽한 암호시스템으로 알려져 있다[1]. 이 연구에서는 높은 보안성을 유지하면서 효율적인 인증을 하기 위하여, 원타임 패드와 유사한 원타임 패스워드의 개념과 이미지 합성을 이용하여 사용자들을 서버에서 인증하기 위한 알고리즘들을 개발하고 이들을 구현하여 그 성능을 평가하고 분석한다.

2. 인터넷 뱅킹 시스템

2.1 현황

현재 행해지고 있는 인증서를 이용한 인증방법에 의하면, 사용자가 서버에 의해 운영되는 사이트를 통해 웹상에 존재하는 인증기관으로부터 인증서를 발급받아 본인이 소유하는 컴퓨터의 하드디스크, 플로피 디스크 또는 USB 메모리 등에 저장하고, 인증서의 이용을 로그인하기 위한 인증서 비밀번호를 인증기관에 등록한다.

이렇게 등록을 한 후, 사용자가 사이트에 접속하여 인증이 필요한 특정 서비스를 요청하면, 저장매체에 저장된 인증서 정보와 인증기관에서 관리되고 있는 인증서의 정보를 비교하여 서로 일치하고, 사용자로부터 인증서 비밀번호를 입력받아 서버에 등록된 인증서 비밀번호와 동일하면, 성공적으로 로그인이 된다.

로그인을 한 후 사용자가 계좌이체 등 각종 서비스를 이용하기 위해서 서버는 또 다른 인증을 요청한다. 인터넷 뱅킹에서 계좌이체를 하고자 하는 경우, 서버에서는 통장 비밀번호 외에 계좌이체를 위한 비밀번호와 은행에게 발급한 비밀번호 카드(일명, 보안카드)의 특정 번호에 할당된 숫자의 입력을 추가로 요구한다.

한편, 비밀번호 카드는 서버(은행)로부터 오프라인으로 발급받는데, 이는 서버 측에서 실명확인을 행하여 실명확인이 된 고객에 대해서만 인터넷 뱅킹을 서비스하기위한 것이다. 계좌이체의 최종단계에서 비밀번호 카드에 기재된 특정 번호에 해당하는 숫자의 입력을 요구한다.

2.2 문제점

보안카드에는 번호별로 미리 정해진 숫자가 인쇄되어 있는데, 그 종류가 약 35개 내외에 불과하다. 즉, 전체 경우의 수가 적은 점을 감안할

때, 스니핑(sniffing)과 같은 해킹방법에 의해 보안카드에 대한 정보가 악의의 제 3자에게 노출될 수 있는 가능성이 다분히 있다[2].

또한, 컴퓨터에 저장된 사용자의 인증서 정보도 스푸핑(spoofing)과 같은 해킹방법에 의해 악의의 제 3자에게 노출될 수 있는 가능성이 있다[2]. 계좌번호 및 비밀번호가 불법 유출되면, 이 계좌 및 보안카드를 이용하여 더 이상 안전한 인증을 수행할 수 없다. 기존의 인증 방법보다는 사용자의 정보를 더 안전하게 관리할 수 있는 인증시스템이 절실히 요구되고 있는 실정이다.

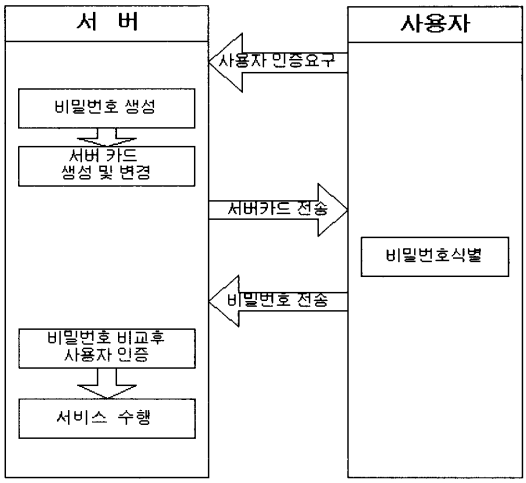
이미지 합성을 인증에 응용하면 매우 높은 보안을 유지할 수 있다. 이 연구에서는 이미지 합성을 이용한 인증에 필요한 요소기술을 개발하고자 한다. 또한, 효율적인 이미지 판독을 하기 위한 기법을 제시하고 구현을 통하여 실용성을 진단한다.

3. 이미지 합성을 이용한 인증

3.1 이론적인 배경

두 개의 투명한 카드를 생성하고 이들의 임의의 위치에 50%의 밀도로 작은 점들을 찍는다. 두 카드를 겹쳐서 본다면 점이 찍힌 부분과 찍히지 않은 부분의 비율은 약 75 : 25가 된다. 그러나 각 카드가 50%의 비율로 점이 찍혀 있을지라도, 두 카드의 점이 서로 독립적이지 않도록 관련성을 부여한다면 두 카드를 합성하였을 때 특정한 문자 및 그림을 나타나게 할 수 있다. 예를 들어, 두 카드의 특정한 부분에서 점들의 위치가 모두 동일하면 두 카드를 합성하였을 때 그 부분은 약 50%의 밀도로 점들이 나타난다. 또한, 특정한 부분에서 두 카드의 점들의 위치가 모두 다른 경우, 두 카드를 합성하였을 때 그 부분은 약 100%에 가까운 밀도로 점들이 나타날 것이다.

이 방법을 이용하여 두 카드를 정확히 겹쳤을 때, 특정한 문자나 그림을 생성하도록 하여, 이를 비밀번호로 취급하여 인증시스템에 이용할 수 있다. 이미지 합성을 이용한 인증 시스템에서 서버와 사용자간의 인증과정은 (그림 1)과 같다.



(그림 1) 사용자 인증과정

사용자카드와 초기 서버카드를 랜덤하게 생성하기 위해 LFSR(Linear Feedback Shift Registers) 알고리즘 사용한다[4].

• LFSR을 이용한 난수의 생성

LFSR이라 불리는 선형 난수 발생기를 이용하면 주기가 긴 수열을 효율적으로 발생 시킬 수 있다. LFSR은 n비트의 초기값을 선형귀환 쉬프트 레지스터에 대입한다. 레지스터에 있는 n비트의 값을 선형귀환 함수에 대입하여 나온 결과값을 n개의 레지스터중 MSB에 삽입되고, 레지스터내의 값은 오른쪽으로 1비트 쉬프트된다. 이를 반복하면 레지스터값이 계속 변화하게 되고, 특정한 비트에서 출력되는 비트열을 발생시킬 수 있다.

이 때 초기값이 $(0, 0, \cdots, 0)$이면 선형귀환함수 값이 항상 0이 되어 주기가 1인 수열이 발생된다. 그러므로 초기값 투플은 0이 아닌 수이어야

만 한다. 레지스터가 n단이므로, 이 레지스터의 상태는 2^n가지를 가질 수 있으며, 모두 0인 상태를 제외하면 2^n-1개의 상태를 가질 수 있다. 이때 LFSR이 동작하면서 n개의 레지스터의 상태가 이전에 발생된 상태와 같을 경우 이후에 발생되는 수열은 이전 수열과 일치하게 된다. 그러므로 LFSR에 의해 생성되는 주기는 2^n-1보다 작거나 같게 된다.

이 이론에 입각하여 30비트의 LFSR을 사용하면 최대 $2^{30}-1$(약 10억개)의 주기를 갖는 수열을 얻을 수 있게 되고 이 수열의 마지막 비트들의 조합을 통해 일정 범위 안에서의 수를 생성할 수 있게 된다.

3.2 사용자카드 생성 알고리즘

투명한 카드의 임의의 위치에 검은 점을 찍으며, 그 밀도를 50%가 되도록 사용자카드를 생성한다. 각 사용자에게 고유한 사용자카드를 배포하기 위해 LFSR 알고리즘들을 조합하여 random 함수를 생성한다. 또한 이 random 함수가 통계적 특성을 분석하여 안전성을 평가한다[3]. 각 카드마다 유일한 고유번호를 할당하고, 그 고유번호를 seed로 사용하여 random한 수열을 발생시킨다. 이 수열을 이용하여 검은 점들을 찍을 위치를 결정함으로써 고유번호에 따른 유일한 카드가 생성된다. 이렇게 생성된 카드들을 사용자들에게 발급한다(예 : (그림 2)). 사용자카드는 인터넷 뱅킹에서 사용되는 보안카드에 해당한다.

3.3 서버카드 생성 및 변경 알고리즘

사용자카드를 생성하는 방법과 동일하게 임의의 고유번호를 이용하여 초기의 서버카드를 생성한다(예 : (그림 3)). 그 다음으로, 인증하여야 할 사용자의 사용자카드와 생성한 서버카드를 겹쳤을 때, 서버에서 의도하는 비밀번호(숫자와 문자의 조합)가 형성될 수 있도록 서버카드를 변경한다(예 : (그림 4)).

초기의 서버카드를 변경하기 위한 알고리즘을 예를 들어 설명하면 다음과 같다. (그림 5)와 같이 비밀번호는 5368이며 이를 생성하고자 하는 위치를 결정하였다면, 5368이 표시되는 부분은 서버카드와 사용자카드를 겹쳤을 때 검은 부분이 100%에 가깝게 되도록 서버카드의 점들을 국부적으로 이동한다. 이렇게 생성된 인증용 서버카드를 사용자에게 전송한다.

이 최종 서버카드는 인증마다 서로 다르게 생성되므로 원타임 패스워드 인증에서 챌린지(challeng) 역할을 한다[1]. 서버카드 자체로는 비밀 번호에 대한 정보를 알아 낼 수 없고 사용자카드와 합성하였을 때만 비밀번호를 알아낼 수 있다.

• 서버카드 변경 알고리즘

단계1 : i = 0, j = 0

단계2 : (i, j) 위치에 사용자카드와 서버카드 점 확인함.
(i, j) 위치가 숫자의 내부이고 사용자카드에 점이 없을 경우 서버카드에 점을 삽입.
(i, j) 위치가 숫자의 내부이고 사용자카드에 점이 있을 경우 서버카드에 점을 삭제.

단계3 : j와 카드 세로크기 비교함.
세로 크기보다 작으면 j = j +1, 단계2로 감.
세로 크기와 같으면 j = 0, 단계4로 감.

단계4 : i와 카드 가로크기 비교함.
가로크기 보다 작으면 i = i + 1, 단계2로 감.

단계5 : 종료함.

위 알고리즘에서는 서버카드에 점을 삽입하거나 삭제하여 서버카드와 사용자카드를 겹쳤을 때 숫자가 기록된 영역에 점의 빈도를 100%로 만드는 알고리즘이다. 점을 삽입만하고 삭제를 하지 않았을 경우 서버카드만을 볼 경우 글자의 모양이 나타날 수 있으므로 삭제를 통하여 서버카드만 볼 경우 숫자의 모양이 나타나지 않게 한다.

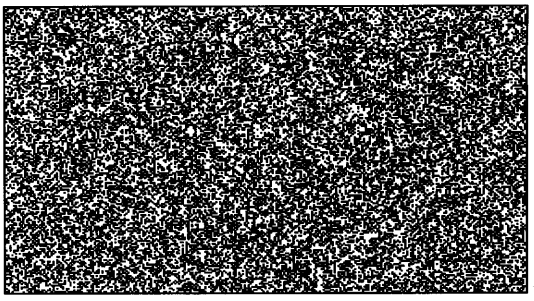
3.4 인증방법

사용자는 자신의 사용자카드와 서버로부터 송신된 인증용 서버카드를 합성한다. 합성된 카드에서는 비밀번호가 저장된 부분에서는 약 100%의 밀도로 검은 부분이 나타나고, 그 외의 영역에서는 평균적으로 약 75%의 밀도로 검은 부분이 나타나게 되며, 이 밀도의 차이로 비밀번호를 식별할 수 있다(그림 5). 이렇게 식별된 비밀번호를 사용자가 키보드와 같은 입력 장치를 이용하여 서버로 다시 전송하고 서버는 이를 확인하여 그 번호가 동일할 때 사용자를 정상적인 사용자로 인정한다.

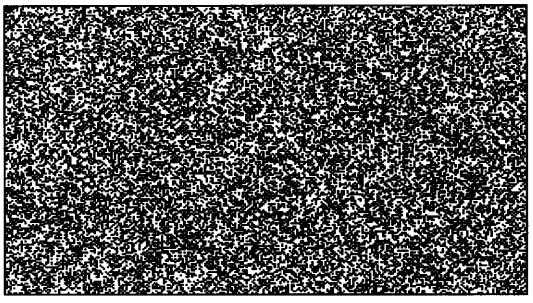
4. 카드 구현 및 검증

3.2절과 3.3절에서 서술한 카드 생성방법을 이용하여 사용자카드와 초기 서버카드 생성 모듈을 개발하였다. (그림 2)와 (그림 3)은 구현한 카드생성 모듈을 이용해 생성한 샘플카드들이다.

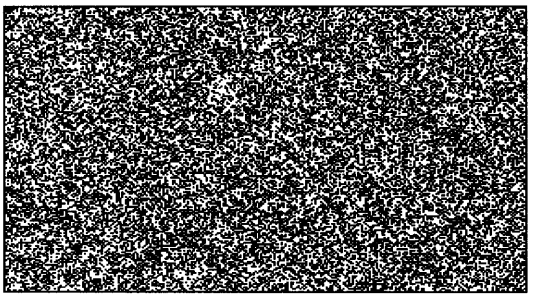
(그림 3)과 같이 초기 서버카드를 생성하고, 특정 사용자 카드와 합성하여 서버가 의도하는 비밀번호를 특정 위치에 형성하기 위하여 초기 서버카드를 변경한다. (그림 4)는 (그림 2)의 사용자카드와 합성하여 5368라는 비밀번호를 형성하기 위하여 카드 변경 알고리즘을 이용하여 (그림 3)의 초기 서버카드를 변경한 것이다. (그림 2)의 사용자카드와 (그림 4)의 인증용 서버카드를 겹쳐보면, (그림 5)가 된다. (그림 5)에서 우리는 5368이라는 비밀번호가 형성된 것을 식별할 수 있다. 참고로, (그림 2)의 사용자카드와 (그림 3)의 초기 서버카드를 겹쳐보면 전혀 어떤 이미지가 형성되지 않는다. 또한, (그림 6)의 제3의 사용자카드를 (그림 4)의 인증용 서버카드와 겹쳐보면 역시 어떠한 이미지도 생성되지 않는다((그림 7) 참조).



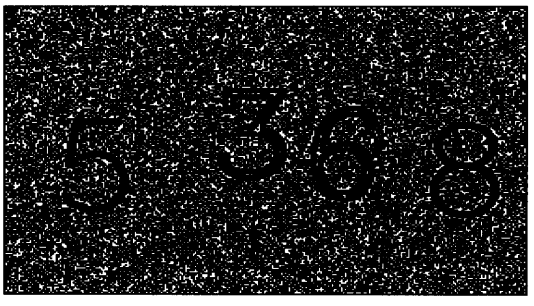
(그림 2) 사용자카드



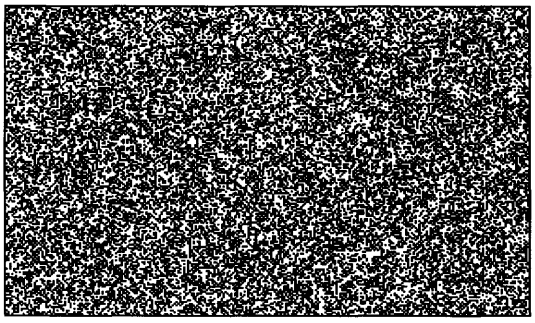
(그림 3) 초기 서버카드



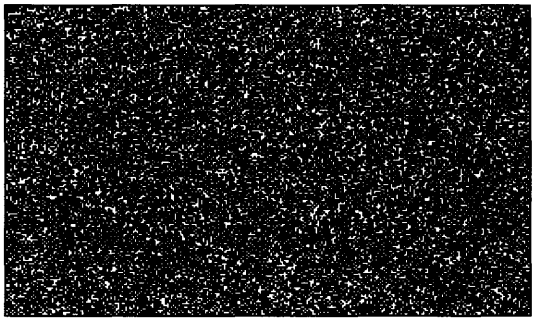
(그림 4) 최종 인증용 서버카드



(그림 5) (그림 2)와 (그림 4)의 합성



(그림 6) 제 3의 사용자카드



(그림 7) (그림 4)와 (그림 6)의 합성

5. 보안성

서버카드를 생성하는 기본 틀은 생성할 때 마다 다른 모양의 카드를 생성하는 것이고, 결과적으로 사용자가 받게 되는 서버카드의 모양은 계속적으로 변화한다.

비밀번호의 조합은 키보드로 입력받을 수 있는 대부분의 문자를 이용할 수 있어 매우 많은 비밀번호의 종류를 만들어 낼 수 있고, 비밀번호가 같더라도 문자의 크기 및 위치 폰트의 종류 등에 따라 서버에서 전송되는 인증용 서버카드의 모양은 계속적으로 다른 모습의 카드로 나타나므로 서버와 사용자 사이에서 전송되는 정보만으로는 비밀번호를 알아내기는 매우 어렵다.

서버를 해킹하여 고객의 정보를 안다 하여도, 고객정보에는 비밀번호에 대한 정보가 없기 때문에 고유번호를 이용한 카드 생성 방법을 알아내지 못하면 고객의 사용자카드를 알아낼 수 없다.

제 3의 사용자카드(그림 6)를 이용하여 인증용 서버카드(그림 4)와 합성하였을 때 (그림 7)과 같이 어떠한 글자나 비밀번호가 나타나지 않으므로 정당하게 발급된 사용된 사용자카드를 사용하였을 때에만 비밀번호를 판독할 수 있다.

6. 결론 및 향후 연구방향

이미지 합성을 이용한 인증 시스템을 도입함으로써 악의적인 제 3자에 의하여 네트워크나 저장매체를 통하여 유출될 수 있는 비밀정보를 좀 더 안전하게 보호할 수 있다. 사용자카드와 서버카드를 합성하는 단계가 사용자에게 다소 번거로울 수 있고 섬세함과 정확한 조정을 필요로 할 수 있다.

향후 연구방향은 합성된 카드에서 비밀번호를 보다 명확하게 식별할 수 있도록 서버카드를 변형하는 알고리즘을 개선하고, 이러한 인증시스템을 실제 활용하기 위하여 사용자 및 사용자카드를 관리할 수 있는 시스템과 비밀번호를 생성하고 확인할 수 있는 시스템을 구축하고자 한다.

참 고 문 헌

[1] Douglas R. Stinson, "Cryptography theory & Pratice," CRC Press.

[2] Bruce Schneier, "Applied Cryptography," John Wiley & Sons.

[3] Henry Beker and Fred Piper, "Cipher-Systems," Northwood.

[4] Solomon W. Golomb, "Shift Register Sequence," Aegean Park Press.

김 수 희

1986년 University of Georgia 전산학과 (MS)
1988년 University of Georgia 수학과 (MA)
1993년 University of South Carolina 전산학과(Ph.D.)
1993년~1994년 Benedict College 조교수
1994년~현재 호서대학교 컴퓨터공학부 컴퓨터공학전공 교수

박 봉 주

1982년~1986년 서강대 수학과
1986년~1988년 서강대 대학원 수학과 석사
1995년~2000년 서강대 대학원 수학과 대수(암호)전공 박사 졸업
국방과학연구소 선임연구원
전자통신연구원 부설 국가보안기 술연구소 선임연구원
2001년~현재 호서대 컴퓨터공학부 정보보호전공 조교수