광시각암호를 이용한 생체정보보호

이상이* · 류충상** · 이승현***
*국가보안기술연구소
**전파연구소
***광운대학교

Biometrical Information Security by Using Opticla Visual Cryptography

Sang-Yi Yi* · Chung-sang Ryu** · Seung-Hyun Lee***
*National Security Research Institute
**Radio Research Lab., Ministry of Information and Communication
***Kwangwoon University
E-mail : syyi@etri.re.kr

요 약

지문 데이터를 광시각암호에 적합하게 Secret Sharing하고 Share 데이터의 일부를 공개된 네트워크로 전송하고 지문의 소유자가 나머지 Share를 소유하고 있다가 필요 시 지문과 함께 Share를 제시하여 본인임을 인식시키는 광시각암호 기반의 생체정보보호 방법을 제안한다.

ABSTRACT

We propose a biometrical information security method based on Optical Visual Cryptography in that a fingerprint data is processed by Secret Sharing method taking into account the Optical Visual Cryptography and a part of shared data transmitted through an open network. Whenever necessary, the owner of the fingerprint can be authenticated by submitting his fingerprint with the other shared information.

키워드
광시각암호, 지문인식, Binary Computer Generated Hologram, Optical Correlator

Ⅰ. 서 론

개인인증을 위하여 이용하는 생체정보는 지문, 홍체, DNA 등 여러 가지가 주목받고 있다. 그중 지문은 모든 사람에게 형태에서 차이가 있어서 개인을 구분하는 데이터로 가장 널리 활용되고 있다. 지문 영상은 고유 주파수를 지니고 있기 때문에 지문 영상의 고유 주파수를 이용하여 광학적으로 패턴 정합을 시도하면 효과적인 광 지문 인식 시스템을 구성할 수 있다.[1] 지문 영상은 외형적으로는 형태가 복잡하여 주변 환경이나 입력 방법에 따라 정확한 데이터가 입력되지 않으므로 유사도로 사용자를 식별하므로 지문 기반의 개인인증 시스템은 데이터를 완전한 일치 보다는 유사도를 이용하여 본인을 판별한다.

광시각암호는 중요한 정보를 보호하기 위하여 복수 정보를 분산시킨 후 합의에 의하여 접근이 허가하는 평등한 Secret Sharing 방법인 시각암호를 광학으로 구현한 형태이다. 광시각암호는 여러 가지 장점이 있음에도 불구하고 암호화 과정에서 발생하는 백색 잡음으로 인하여 평문를 완벽하게 복구하지는 못하는 단점이 있다.

영상의 유사도를 이용하는 광 상관기와 백색 잡음과 함께 평문을 복호하는 광시각암호를 조합하면 정보보호 기능을 갖는 유사도 측정 시스템 구성이 가능해진다.[2] 여기에 지문 영상을 대상으로 두 시스템을 적절히 조합하고 유사도의 범위를 판정하는 기준을 만들면 지문정보를 대상으로 광시각암호기술이 적용된 새로운 생체정보보호 시스템이 구성 가능하게 된다.

따라서 이 논문에서는 광시각암호기술을 이용하여 생체정보시스템을 구성하고 지문데이터를 대상

으로 실험을 실시하여 타당성을 검증한다.

II. 본 론

중요한 비밀 정보를 개인이 관리하는 경우, 부주의와 개인의 악의 등에 의해 정보가 누설되고 나아가 악용될 가능성이 있다. 따라서 중요한 정보를 그룹의 복수 회원에게 분산시킨 후, 회원의 합의에 의해 접근이 허가되는 비밀 관리의 구조가 고려되어질 수 있다. 예를 들면, 수표발행을 위한 서명이나 핵무기의 발사 등의 응용이 있을 수 있다. 따라서 접근 구조가 대등한 회원을 갖는 동일 그룹의 경우에 있어서 평등한 비밀 분산법인 (k, n) 임계치 방식이 A. Shamir에 의해 제안된 후, 많은 연구가 수행되어졌다.[3] 단, 이들 방식에서는 비밀을 분산 및 복호하는 어느 경우라도 비밀의 안전성을 확보하기 위하여 복잡한 연산과 구성을 위한 고성능의 컴퓨터를 필요로 하였다.

그래서 비밀 분산 방식의 새로운 형태로서 비밀정보로 영상을 이용하여 분산된 비밀 영상을 복잡한 암호적인 연산 없이 복호할 수 있는 암호화 방식이 M. Naor와 A. Shamir에 의해 제안되었는데, 이 시각암호화 방식은 A. Shamir에 의해 제안된 기존의 (k, n) 임계치 비밀 분산 방식을 영상 정보에 적용하여 시각적으로 복호할 수 있도록 변형한 것이다.[4] 즉, n명의 회원에게 미리 배포된 서로 다른 슬라이드 중에 임의의 k명 이상의 슬라이드를 중첩시키면 숨겨진 비밀 영상을 볼 수가 있으나, k명 미만으로는 숨겨진 비밀 영상에 관한 아무런 정보도 얻을 수 없도록 하는 것이다.

시각 암호화는 강력한 영상 암호 기능을 지니고 있음에도 불구하고 많은 제한점을 갖고 있다. 대상이 되는 영상은 이진화되어 있어야 한다. 일반적으로 이진화된 영상은 백화소 주변의 화소는 백화소일 가능성이 매우 높고 흑화소 주변의 화소는 흑화소일 가능성이 매우 높다. 이것은 안전성을 떨어뜨리는 요인이 된다. 또한 암복호 과정에 부화소의 더하기 과정만이 존재하므로 복호된 영상의 백화소 부분에는 각 화소당 하나 이상의 흑 부화소가 존재하여 신호대잡음비가 낮은 단점을 지니고 있다.

일반적으로 알려진 암호화 방법은 디지털 처리에는 적당하나 광학에 적용하기는 매우 비효율적이다. 기존의 알고리즘을 적용하기 위해서는 광 데이터를 디지털로 전환하여 저장하고 복호하여 다시 광 데이터로 전환해야 한다. 이것은 올바른 방법이 아니며 암호 알고리즘을 광 시스템에 적용하기 위해서는 광학적으로 복호하는 것이 필수적이다. 예를들어 CGH(computer generated hologram)에 저장되는 정보를 블록 암호, 스트림 암호, 공개키 암호 등과 같이 기존의 암호화에서 알려진 방법을 직접 적용하기에는 적당하지 않다. 따라서 암호화는 디지털적으로 이루어져도 복호는 광학적으로 수행될 수 있는 알고리즘이 요구고 있으며 시각암호가 한 가지 힌트이다.

BCGH(binary CGH)는 이진 값으로 구성되어 있어도 계조도의 영상을 표현할 수 있다. 특히 패턴인식에 이용되는 POF(phase only filter)는 백화소 주변의 화소가 백화소일 가능성은 약 50% 정도이며, 이것은 흑화소의 경우에도 동일하다.

BCGH는 시각 암호화에서 요구하는 입력 조건을 만족하고 있다. 따라서 BCGH에는 시각 암호화 기법을 적용할 수 있으며, 보호된 BCGH는 시각암호의 안전성을 보장한다.

광시각암호시스템은 시스템의 입력으로 입력 데이터를 직접 입력하지 않고 BCGH를 사용한다. 따라서 회색 준위를 갖는 영상에도 적용이 가능하며, 신호대잡음비도 개선된다.

광시각암호에 기반하여 지문인식에 적용되는 생체정보보호 시스템의 구성은 그림 1과 같다. 지문패턴을 대상으로 광시각암호 기술을 적용하고, 복호된 영상을 대상으로 광 상관기를 통하여 인증 하는 방법을 사용한다. 시스템 구성은 크게 두 부분으로 구성된다. 영상을 암/복호하는 전처리 단과 유사도를 판단하는 후처리 단으로 구성하였다. 즉, 전처리 단에서는 암호문을 암/복호하여 BCGH를 만들고 이를 퓨리에 변환하여 기록된 영상을 복원하면 후처리 단에서 암호문의 변조 여부를 확인한다.

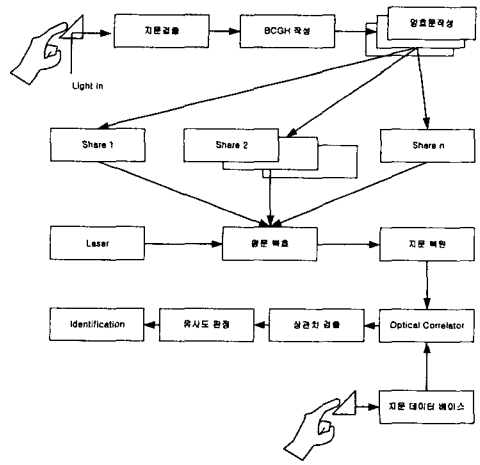

그림 1. 시스템 구성

광시각암호 시스템에 기반하여 구성되는 생체정보보호 시스템 역시 영상 자체를 그대로 이용한다. 입력된 지문을 BCGH를 사용하여 홀로그램으로 작성하고. 원하는 수만큼 share를 작성한다. 각각의 share는 여러 가지 경로를 통해 다시 모이게 되고 평문으로 복호될 것이다. 복호된 평문을 광학적으로 퓨리에 변환하면 지문 영상이 복원될 것이다. 그리고 이것을 확인하기 위하여 최종 확인자가 자신의 지문을 입력하거나 데이터베이스에서 데이터

를 읽어 복원된 지문과 광학적으로 상관을 발생시킨다. 그리고 서로간의 상관도를 판단하여 암호문이 정확한 데이터인가를 확인한다. 만일 share에 대한 위조가 있는 경우 기본적으로 BCGH가 구성되지 않기 때문에 복호된 평문을 퓨리에 변환하면 어떠한 형태의 지문도 나타나지 않는다. 또한 어떠한 형태의 지문이 입력되는 경우 이 지문이 허위로 작성된 것이라면 상관도 판정을 통과하지 못할 것이다.

III. 실험 및 고찰

원본을 가장한 가짜 지문에 대한 실험을 위하여 그림 1과 같은 지문을 시스템 입력으로 사용하였다. 그림 2(a)는 암호화하여 보호하고자 하는 지문 영상이며, 그림 2(b)는 가짜 지문 영상으로서 원래 지문과 가능한 유사한 지문을 선택하였다. 사용한 가짜 지문은 원래 지문을 약간 오른쪽으로 옮긴 듯한 형태로 무늬의 방향이나 골의 모습이 표적 지문과 유사한 무늬를 가지고 있어서 적지 않은 유사도를 나타낼 것으로 유추할 수 있다.

(a) 암호를 위한 지문 (b) 가짜 지문
그림 2. 실험을 위한 입력 영상

생체정보보호 시스템의 실험 및 평가를 위하여 Secret share를 4장으로 구성한 후 세 가지 경우에 대한 가정을 하였다. 첫 번째는 암호문을 복호한 결과가 표적으로 삼고 있는 원래 지문과 동일한 경우이다. 두 번째는 복호한 결과가 표적과 다른 지문으로 복원된 경우로서 신분을 위장하기 위하여 광시각암호 제작 알고리즘에 따라 가짜 지문을 이용하여 제작한 암호문이 복호 후에 정상적으로 복원되었을 때이다. 마지막으로 암호문이 위조된 경우로서 Secret share중 임의의 한 장에 대하여 30% 변조를 발생시킨 경우를 실험하였다.

그림 3과 그림 4에서 'A'는 원 지문과 복호된 지문간의 상관결과를 나타내는 광상관 평면이다. 그림 1의 'B'는 원본과 다른 가짜 지문이 복호된 것에 대한 상관으로 원 지문과 다른 가짜 지문이 입력되어 낮은 상관도를 나타내었다.

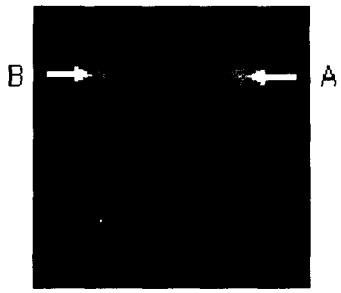

그림 3. 다른 지문이 입력된 경우

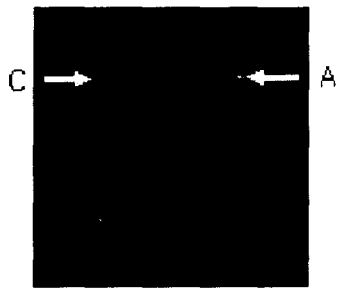

그림 4. 암호문이 변조된 경우

'C'는 암호문이 위조된 경우이다. 상관 결과 변조된 암호문에 의한 결과는 상관 첨두치를 전혀 발생시키지 못하였다. 이는 변조된 암호문이 BCGH를 정확히 복호하지 못하데 기인하는 것으로 상관에 참여한 지문 영상은 실제로는 잡음과 같은 형태로서 지문의 형태를 갖추지 못하였다.

이상의 실험 결과는 암호문의 변조는 다른 영상에 의한 결과 보다 검출하기 쉽다는 것을 알 수 있다. 이는 변조된 암호문이 BCGH를 손상시키고 이로 인하여 지문이 복원되지 못하기 때문이다. 그러나 CGH 특성상 CGH의 일부만이 남아 있더라도 반복 수행에 의하여 지문을 복원해 낼 수 있다. 따라서 암호문이 변조가 아니라 손상이라면 복원해 낼 수 있다. 그러나 광시각암호 시스템의 비도는 시각 암호 시스템의 암호 강도와 같으므로 이러한 홀로그램의 데이터 복원 특성을 이용하여 암호문을 해독하는 것은 시각 암호를 해독하는 것과 유사한 난이도를 갖는다.

광시각암호 시스템은 암호화 과정에서 발생하는 백색 잡음으로 인하여 평문을 완벽하게 복구하지는 못한다. 그러나 기본적으로 지문인식 시스템은 데이터를 완전하게 정합시킬 필요가 없으며, 환경이나 지문입력 방법에 따라 정확한 데이터가 입력되지 않으므로 유사도를 통하여 사용자를 효율적으로 식별할 수 있었다. 따라서 광시각암호 시스템을 지문을 대상으로 적용하여 생체정보보호 시스템에 구성하는 것은 생체기반의 개인인증을 위하여 적합한 것으로 해석된다.

V. 결 론

광시각암호 시스템은 암호화 과정에서 발생하는 백색 잡음으로 인하여 평문을 완벽하게 복구하지는 못한다. 그러나 기본적으로 지문 데이터와 같은 생체정보는 측정하는 환경에 따라 적으나마 변화가 발생한다. 따라서 완전하게 정합시킬 필요가 없으며 유사도를 통하여 사용자를 효율적으로 식별할 수 있다. 따라서 광시각암호 시스템을 생체정보 시스템에 적용하는 것은 타당한 것으로 판단된다.

참고문헌

[1] K. H. Fielding, J. L. Honor, and C. K. Makekau, "Optical fingerprint identification by binary joint transform correlation," Opt. Eng., vol.30, no.12, pp.1958-1961, 1991.

[2] S. Yi, C. Ryu, D. Ryu, and S. Lee, "Evaluation of Correlation in Optical Encryption by using Visual Cryptography", Proc. of SPIE, vol.4387, pp.238-246, 2001.

[3] M. A. Shamir, "How to Share Secret", CACM, Vol.22, pp.612-613, 1979.

[4] M. Naor and A. Shamir, "Visual Cryptography", Proc. Eurocrypt'94, vol.950, pp. 1-12, 1995.