2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

무아레 무늬를 이용한 암호 기법

강혁*, 이병래, 김태윤
고려대학교 컴퓨터학과
e-mail:paranblue@netlab.korea.ac.kr

Data Encryption Using The Morie Fringes

Hyeok kang*, Byung-Rae Lee, Tai-Yun Kim
Dept of Computer Science, Korea University

요약

본 논문은 물리학적 현상 중 무아레 무늬를 이용해 통신 중에 사용되는 데이터 암호화 기법을 제안한다. 먼저 무아레 무늬에 대한 기본적인 이론과 기존에 사용되어지는 데이터 암호화 기법에 대해 고찰하고 무아레 무늬를 이용한 데이터 암호화를 제안하고 마지막으로 제안된 무아레 현상을 이용한 데이터 암호화와 기존에 사용되는 암호화 기법을 비교 문제점과 해결 방안을 제안한다.

1. 서 론

무아레 현상은 1874년 Lord Rayleigh에 의해서 최초로 과학적인 도구로써 사용이 제안된 이후로 다양한 분야에서 연구가 되어지고 있는데 그 중 무아레 무늬는 공간적으로 주기적인 또는 준 주기적인 구조를 서로 겹치거나 다른 하나에 투영시켜 얻을 수 있는 강도 간섭에 의해 얻어지는 무늬로 물체형상측정, 열팽창 측정기 제작, 지문감식 등으로 사용이 가능하다. 이 무아레 무늬(Moire Fringe)를 또 다른 가능한 쓰임에 대하여 생각할 수 있다[1].

본 논문은 독특한 무아레 무늬를 데이터 암호화 체계에 적용하는 것에 대한 연구의 실현 가능성을 논의한다. 본 논문의 구성은 2 장에서는 무아레 현상에 대한 이론적인 배경을 기술하며, 3 장에서는 무아레 현상을 이용한 데이터의 암호화를 제안한다. 4 장에서는 본 연구에 대한 결론을 맺고 향후과제를 제시한다.

2. 이론적 배경

1.1 Moire의 역사

무아레 무늬에 대한 연구는 1874년 Lord Rayleigh경이 두 개의 동일한 회절 격자를 거의 평행하게 겹침으로서 평행한 막대 모양의 무아레 무늬들이 생기는 것을 발견하고, 이 현상을 회절 격자의 검사에 이용할 수 있음을 제안함으로써 시작되었다. 이후로 다양한 계측 분야로의 응용에 대한 연구가 진해되어져 왔다. 1963년 Theocaris는 무아레 간섭법에서 일반적으로 사용되어왔던 직선격자 대신에 두 원형 격자를 사용하여 병진 운동 시 상대적 이동거리를 측정하였고, 1964년 Nishilima와 Oster는 이러한 원형격자의 응용성을 복굴절물질의 편극에 따른 분산 특성의 측정하였다. 특히 1970년에 이르러 Meadow와 Takasaki등에 의해서 무아레 현상이 임의의 현상을 가지는 물체의 3차원 형상을 측정하는데 응용되어질 수 있음이 밝혀지면서부터 이 분야에 대한 많은 연구가 진행되어지고 있다[2].

1.2 Moire의 정의 및 현상

백색광 하에서 공간적으로 주기성을 갖는 반사판 또는 투과판을 서로 겹쳐 놓을 때 발생하는 물질 형태의 간섭무늬를 무아레 간섭무늬라

고 하는데, 이러한 무아레 현상은 비간섭성 광원을 사용하는 강도(intensity)간섭 효과로 이해될 수 있다. 무아레 무늬는 주기적인 무늬가 겹쳐 나타나는 현상이다. 모기장 같은 망사 두 장이 겹쳐있을 때 망사를 이루는 세밀한 직물의 격자 간격보다 훨씬 크고 변화가 다양한 얼룩무늬를 볼 수 있다. 또한 머리 빗 두 개를 겹쳐서 보면 간격이 빗살보다 넓은 새로운 어두운 그림자를 볼 수 있다. 이렇게 주기적인 무늬를 무아레 무늬(Moire Fringe)라 한다. 이 Moire는 프랑스 말로 '물결 무늬'의 뜻을 가지고 있다[1.2].

무아레 무늬는 공간적으로 주기적인 또는 준주기적인 구조를 서로 겹치거나 다른 하나에 투영시켜 얻을 수 있는 강도 간섭에 의해 얻어지는 무늬로 무아레 간섭법은 무늬를 얻는 방법에 따라 그림자식과 영사식, 반사식으로 나누어진다. 이때 얻어지는 무아레 무늬는 격자의 미소 변화를 증폭하여서 미소 변형 측정 또는 접촉식 방법으로 측정이 곤란한 물체의 형상 측정, 이동하고 있는 물체 등에 대한 정보를 얻는데 이용된다.

무아레 간섭무늬의 형성은 이론적으로 공간상의 맥놀이 현상으로 설명될 수 있다 두 개의 유사한 공간상의 주기를 갖는 격자가 겹쳐진 상태를 공간상의 주파수 영역에서 살펴보면 원래의 격자들이 갖고 있던 고유의 주파수 성분들과 격자 주기의 합과 차에 해당되는 주파수 성분으로 분리할 수 있게 된다. 이때 격자 주파수의 차에 해당되는 저주파수 성분을 무아레 간섭무늬라 한다[1.4].

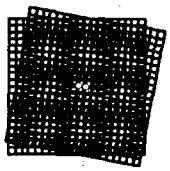
3. 제안한 무아레 무늬를 이용한 암호화

3.1 무아레 무늬를 이용한 암호화의 필요성

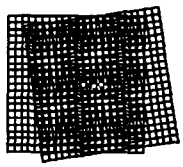
기존에 사용되어 왔던 암호화 방법에는 기원전 5세기경 고대 그리스인들이 쓰던 최초의 암호문 사이테일부터 비밀키를 사용하여 암호문을 작성하는 DES, 계산하기 힘든 소인수분해를 이용, 비밀키와 공개키를 생성하여 데이터를 암호화시키는 RSA까지 여러 가지의 방법들이 있다. 그러나 요즘 급격히 발전하는 과학의 발달에 의해서 기존에 사용해오던 여러 가지의 암호화 방법들이 해독될 수 있음이 증명되었다. 따라서 해독이 불가능한 암호의 필요성에 의거해 현재 사용되어지는 다른 것에 비해 보다 견고한 암호화를 위한 무아레 무늬(Moire Fringe)를 이용한 암호문을 제시한다.[2]

3.2 무아레 무늬를 이용한 암호화에 따른 원리

주기성을 갖는 동일한 격자들에서 겹쳐질 때 만들어지는 물결형태의 간섭 무늬가 그림 1과 그림 2에서와 같이 중심 거리에 따라 무아레 무늬의 모양이 바뀌는 성질을 이용하여 암호문내의 같은 문자에 대해서 다른 모양을 주어서 동일성을 없앨 수 있을 것이다. 즉 무아레 무늬의 특성을 이용한 해독 불가능한 암호를 만들 수 있다.



<그림 1>

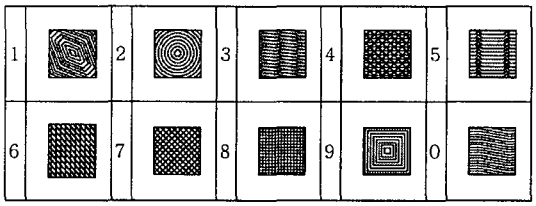


<그림 2>

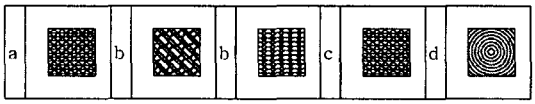
3.3 무아레 무늬를 이용한 암호화의 방법

무아레 무늬를 이용하여 암호화하는 방법에는 우선 문자를 격자화 시키는 문제가 있는데 영문자 A에서 Z까지, 숫자 0에서 9까지 각각에 대해 격자를 만들게 되면 총 36개의 격자를 만들어야 하는 문제가 생긴다. 그래서 이 논문에서는 ACSII 코드표처럼 두 개의 0에서 9까지의 숫자 조합으로 모든 문자를 나타낼 수 있으므로 0에서 9까지의 10개의 격자만을 사용하여 영문자와 숫자를 암호화시키는 것으로 제안하였다. 제작하는 격자는 소스격자와 덮침 격자를 제작한다. 소스격자에 덮침 격자를 겹치면, 고

유의 무아레 무늬가 나타난다. 여기서 소스 격자는 제작과정의 표현상의 문제로 비교적 단순한 격자로 제작하였고 모양에는 아무런 제한이 없다. 덮침 격자는 1개에서 n개까지 제작할 수 있지만 여기선 5개만 제작하였다.



<소스 격자>



<덮침 격자>

3.4 무아레 무늬를 이용한 암호화의 과정

무아레 무늬를 이용하여 컴퓨터 "갑"과 "을"이 "ABCD" 이라는 문자를 암호화하여 통신하는 과정을 살펴보자.

① 컴퓨터 "갑"은 입력받는 "ABCD"이라는 단어를 ASCII 코드표의 코드에 의거하여 숫자로 전환시 킨다.(여기서 "ABCD"이라는 문자는 ASCII 코드표에 의해서 "65666768"의 숫자로 전환된다.)

② 전환된 숫자를 해당되는 소스격자로 전환시킨다.

③ 각각의 소스격자에 따른 숫자코드를 결정하기 위해서 랜덤하게 정수를 3개씩 선택한다. (여기서 숫자코드를 이용하는 이유는 같은 문자에 대한 규칙성을 없애자는 것으로 고안한 것, 숫자코드는 각각의 덮침 격자를 결정하고, 그 격자에 대한 특성을 부여하는 것이다.)

④ 결정된 숫자코드에 따라 덮침 격자를 소스코드에 씌우면 고유의 무아레 무늬가 보이며 컴퓨터 "갑"에서의 암호화 작업은 완료되었으며 컴퓨터 "을"에게 전송한다.

⑤ 컴퓨터 "을"은 컴퓨터 "갑"이 보낸 데이터를 수신하고, 컴퓨터 "갑"의 역과정으로 전송된 데이터에서의 숫자코드대로 그 숫자코드와 동일한 격자를 수신된 데이터에서 벗겨내면 소스 격자만 남게 된다.

⑥ 찾아낸 소스 격자를 숫자화 시키고 ASCII 코드에서 데이터를 문자화시킨다.

위의 과정에서 사용되는 동일한 소스 격자를 사용하여도 숫자코드를 이용함으로서 나중에 나타나는 무아레 무늬가 전혀 다르게 나타나므로 해당 격자의 숫자 코드가 무엇인지 알지 못하는 한 전혀 데이터를 해독하지 못하게 된다. 여기서 사용되어지는 숫자코드를 이용하는 의미는 같은 문자에 대한 규칙성을 제외시키자는 취지에서 고안한 것으로 예를 들어 설명하면, 숫자코드 531에서 5는 정사각형 격자를 뽑은 것이고, 3은 줄 사이 간격, 1은 줄의 굵기를 나타내는 것이다. 즉 숫자 코드는 각각의 덮침 격자를 결정하고, 그 격자에 대한 특성을 부여하는 것이다.

3.4 무아레 무늬를 이용한 암호기법의 한계점

무아레 무늬를 이용한 암호기법에 사용되는 무아레 무늬는 물질에 대한 광학적 실험에서 생성된 무늬를 전송하는 것이기 때문에 RSA과 같은 문자나 숫자를 전송할 때보다 전송 시간이 오래 걸린다는 한계점을 보인다.

예를 들어 흑백격자(2cm×2cm)를 1kbyte 정도라고 가정하더라도 문자 200자를 암호화 시켜 보낸다고 하면, 문자 1개당 격자가 각각 2개가 필요하게 된다. 일반 문자 200자를 기준으로 사용시 약 0.39kbyte가 필요하게 되는데 반해 무아레 무늬를 사용시 400kbyte가 필요하게된다. 이렇듯 데이터 공간을 많이 차지하게 되므로 전송시간이 늦어지는 한계를 보인다. 그러나 광학적 현상에 발생되는 무아레 무늬를 이용하

여 암호화는 방식으로 무아레 현상에서 생성되는 고유한 무늬를 이용한 방식이므로 보다 견고하다는 장점이 있다.

4. 결론 및 향후 연구과제

본 논문에서는 무아레 무늬를 사용하여 데이터를 암호화하는 것을 제안하였다. 앞에서 이야기 된 바와 같이 같은 문자에 대해서도 각 격자에 대한 해당 숫자코드를 부여함으로서 규격화된 격자 코드를 모르는 한 제 3자가 데이터를 해독하지 못하게 된다는 장점이 있다. 그러나 데이터 전송시 무아레 무늬를 이용할 경우 약간의 시간이 걸린다는 문제 문제를 안고 있다. 그러나 문제에 의한 암호화 방식은 과학의 발달로 점점 해독이 가능해 지고 있는 시점에서 본 논문에서 제안한 무아레 무늬를 이용한 암호화는 가치가 있는 것으로 생각된다.

5. 참고 문헌

[1] 김봉진, 송종섭, 김지택, 조재홍, 장수, 육근철, "회전각 측정용 Matched Radial-Parallel 격자가 만든 무아레 무늬의 해석", 새물리, 36, pp.577-583,(1996)

[2] L. Rayleigh, " On the manufacture and theory of diffraction gratings", Philos. Mag. 47, pp.81-93, (1874)

[3] 문일규, 육근철, "Maychedd Radial-Parallel Grating의 무 아레 무늬를 이용한 직선 도선의 자기장 측정에 관한 연구", 연구논총, 제 2집, pp. 223-242,(1997)

[4] http://my.dreamwiz.com/mnmn84

[5] http://myhome.shinbiro.com/~kmste2

[6] P. Szwaykoski and K. Patorski,"Moire fringes by evolute gratings" Appl. Opt. 3, 28, pp. 4679-4681 (1989)cGraw Hill