한국사물인터넷학회논문지 Vol. 2, No. 1, pp. 23-27, 2016 http://dx.doi.org/10.20465/KIOTS.2016.2.1.023

무아레 무늬를 이용한 참 난수 생성 방법

강혁[1*], 이근호[2]
[1]워싱턴 대학교 컴퓨터 공학과, [2]백석대학교 정보통신학부

True Random Number Generation Method by using the Moire Fringe

Hyeok kang[1*], Keun-Ho Lee[2]**
[*1]Department of Computer Science & Engineering, University of Washington
[2]Department of Information and Communication, Baekseok University**

요 약 빛의 물리적 성질 중의 하나인 파동의 회절 현상을 설명하는 프레넬 회절과 간섭에 의해 생성되는 무아레 무늬가 있다. 본 논문에서는 무아레 무늬에서 생성되어지는 값들을 암호 시스템에서 사용되는 키로, 의사 난수 발생기에서 생성한 난수가 아닌 참난수로 만들어 사용할 수 있음을 제안한다.

주제어 : 키 생성, 무아레 무늬, 참 난수, 간섭, 회절, 탈봇 효과, 프레넬 회절.

Abstract There is Generated Moire fringe by fresnel diffraction that explains one of light's physical phenomenon and interference. In this paper, we propose to generate true random numbers by Moire fringe should be used by not pseudo-random number in cryptosystem.

Key Words : Key generation, natural random number, Interference, diffraction, Fresnel diffraction.

1. 서론

난수는 정보보안 및 암호시스템 등 일상 생활에 다양하게 활용되고 있다. 우리가 주로 사용하는 난수는 수학적 알고리즘에 의해 생성된 의사난수로서 컴퓨터 장비의 발달과 해킹 기술의 발전으로 위험에 노출되어 있다. 난수성(randomness)은 많은 정보보안을 위한 암호 알고리즘을 설계하는데 있어서 가장 기본적인 항목이며 중요하다. 난수 생성의 기술은 모든 암호 시스템에서 없어서는 안되는 필요한 것이다. 난수 발생기에서 생성되는 난수는 예측 불가능성(unpredictable), 무 편향성(unbiased), 숫자간 무관성(uncorrelated) 의 세가지 조건을 만족해야 한다.

난수를 얻는 방법에는 크게 둘로 나눌 수 있는데 물리적 현상의 랜덤성을 이용하여 예측이 불가능하고 편향되지 않으며 독립적인 이상적인 비결정론적 난수발생기와 결정론적 알고리즘에 짧은 길이의 초기값을 입력하여 훨씬 더 긴 길이의 난수를 생성하는 결정론적 난수발생기가 있다. 전자에 의해서 만들어진 수를 참난수라하고, 후자에 의해서 생긴 수를 의사 난수라고 한다.[5]

본 논문의 구성은 2 장에서는 빛의 물리적 현상인 간섭과 회절에 대하여 간략하게 기술하고 무아레 무늬에 대한 배경과 내용을 기술하며, 3 장에서는 간섭과 회절에 의해 생성되는 무아레 패턴 무늬에서 참난수를 생성할 수 있음을 제안한다. 4 장에서는 본 연구에 대한 결론을 맺고 향후 과제를 제시한다.

교신저자 : 강혁(kanghyeok74@gmail.com)
접수일 : 2015년 12월 8일, 수정완료 : 2016년 2월 17일, 최종게재확정 : 2016년 3월 17일

2. 빛의 간섭과 회절 및 무아레 무늬

2.1 간섭(Interference)

두 개 혹은 그 이상의 파동이 중첩할 때, 부분적으로 또는 전체적으로 파동이 다른 파동성분보다 증가하거나 상쇄하는 영역이 있다. 중첩 이후에 개개의 파동들은 중첩 이전의 파동들에 의해서 영향을 받지 않고 완전히 독립적으로 진행하는 중첩의 원리(principle of superposition)에 따른다. 즉 간섭이란 두 빛 혹은 여러 빛이 중첩되었을 때 밝고 어두운 무늬가 나타나는 현상을 말한다. 빛의 간섭이론을 간단하기 알아보면, 전자기파의 선형중첩 원리에 기초를 두고 있으며 제일 간단한 경우로 알아보면 위상과 진동수가 동일한 두 파장을 중첩시키면, 중첩된 파동의 전장 진폭은 각각의 진폭의 합 $E=E_1+E_2$ 이 되며 파동의 세기는 $I \propto (E_1+E_2)^2$와 같은 진폭합의 제곱에 비례한다. 동일한 진동수와 위상이 서로 다른 두 파동을 중첩시켜 보면,

$\vec{E}(1)=\vec{E_1}\exp i(\vec{k_1}\cdot\vec{r}-wt+\phi_1)$

$\vec{E}(2)=\vec{E_2}\exp i(\vec{k_2}\cdot\vec{r}-wt+\phi_2)$ 와 같이 표현된다.

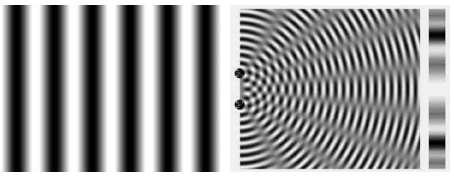
여기서 ϕ_1과 ϕ_2는 두 파동의 초기 위상을 나타낸다.

두 파동을 중첩시켰을 때, 중첩된 파동의 세기는

$I=[\vec{E}(1)\cdot\vec{E}(2)]\cdot[\vec{E}(1)^*\cdot\vec{E}(2)^*]$

$=I_1+I_2+2Re\,\vec{E_1}\cdot\vec{E_2}\exp i[(\vec{k_1}-\vec{k_2})\cdot\vec{r}+\phi_1-\phi_2]$

여기서 θ 는 $(\vec{k_1}-\vec{k_2})\cdot\vec{r}+\phi_1-\phi_2$ 이다. 위 식에서 보는 것과 같이 각 파동의 세기를 단순하게 합산해 놓은 값으로 바탕 세기(background intensity)가 되며, 실제 간섭항은 세 번째 항으로 바탕 세기를 중간 값으로 하여 이보다 더 밝은 부분과 어두운 부분이 연속적으로 생성된다. 이것을 간섭 무늬라고 한다.



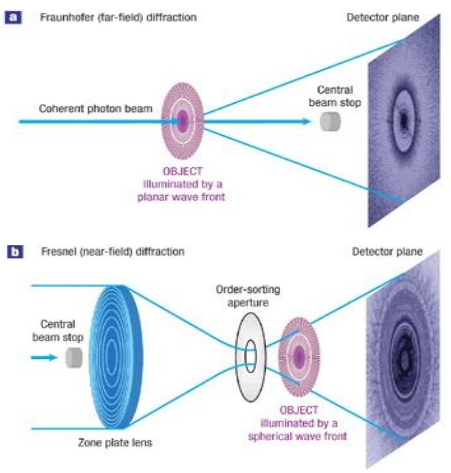
[Fig. 1] Interference patterns

간섭 무늬를 관찰하기 위해서는 무늬가 나타나는 곳에 눈이나 카메라 또는 망원경 등과 같은 검출기의 초점을 맞추는 것이 매우 중요하며, 간섭 무늬의 종류는 실무늬(real fringes)와 허무늬(virtual fringes)로 나누거나, 또는 국지화 되지 않은 무늬(nonlocalized fringes)와 국지화된 무늬(localized fringes)로 구분된다.

2.2 회절(diffraction)

불투명한 물체가 점광원과 스크린 사이에 놓이게 되면 스크린 위에 기하학적 그림자와는 달리 그림자 가장자리에서 밝은 선과 어두운 선이 교차로 나타나게 되는데 이처럼 물체의 가장자리에서 빛이 직진 경로에서 벗어나 진행하는 현상을 회절(diffraction)이라고 한다. 회절은 모든 파동에 있어서 진행하는 파면의 일부가 차단 혹은 방해받았을 때 발생하는 파동 현상의 일반적인 특징이다.[9]

회절은 프라운호퍼 회절(Fraunhofer diffraction)과 프레넬 회절(Fresnel diffraction)으로 구분되어진다. 불투명한 평판 위에 작은 구멍을 하나 뚫어 놓고, 광원에서 평행광선이 입사되는 경우, 관측 면이 평판과 충분히 가까이 접근하면 관측 면에는 명확한 구멍의 상이 나타나며, 상의 가장자리에는 몇 개의 회절 무늬가 희미하게 나타난다. 이 관측 면을 평판에서 조금씩 멀리 이동시키면 구멍의 상은 여전히 뚜렷하지만, 회절 무늬가 분명하게 생겨서 구멍의 상의 뚜렸한 동심원 구조를 갖게되는데 이 현상을 프레넬(Fresnel) 회절 혹은 근거리 회절이라고 한다. 또한 관측 면을 더욱 멀리 천천히 이동시키면, 회절 무늬도 연속적으로 변하게 되고 구멍의 크기보다 넓게 퍼지게 되는데 무늬 모양은 변하지 않고 그 크기만 변하게 되는데 이것을 프라운호포(Fraunhofer) 회절 혹은 원거리 회절이라고 한다.[9]



[Fig. 2] Fraunhofer diffraction and Fresnel diffraction[10]

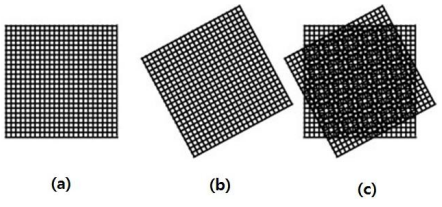
2.3 무아레 무늬(Morie Fringe)

2.3.1 무아레 무늬 역사

무아레 무늬에 대한 연구는 1874년 Lord Rayleigh경이 두 개의 동일한 회절 격자를 거의 평행하게 겹침으로써 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 진행되어져 왔다. 무아레 현상은 물체의 3차원 형상을 측정하는데 응용되어질 수도 있고, 지문의 분석에도 이용될 수 있음이 밝혀지면서 이 분야에 대한 많은 연구가 진행되고 있다[1][9]

2.3.2 무아레의 정의 및 현상

백색광 하에서 공간적으로 주기성을 갖는 반사판 또는 투과판을 서로 겹쳐 놓을 때 발생하는 물질 형태의 간섭무늬를 무아레 간섭무늬라고 하는데, 이 방법은 회절 격자를 사용하며 광학적인 간섭을 이용하여 변형에 관한 정보를 얻어낼 수 있는 방법이다. 모기장 같은 망사 두 장이 겹쳐있을 때 망사를 이루는 세밀한 직물의 격자 간격보다 훨씬 크고 변화가 다양한 얼룩무늬를 볼 수 있으며, TV 안에서 줄무늬 셔츠를 볼 때에도 무늬를 볼 수 있다. 이렇게 주기적인 무늬를 무아레 무늬(Moire Fringe)라 한다. 이 Moire는 프랑스 말로 '물결 무늬'의 뜻을 가지고 있다[6]



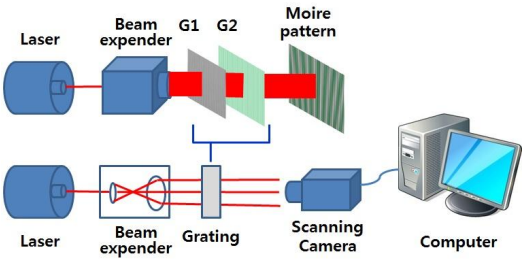
[Fig. 3] (a) pattern 1, (b) pattern 2, (c) moire pattern created as the patterns of two grids are combined

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[6]

3. 무아레 무늬 실험

3.1 무아레 무늬의 실험

[Figure 4]는 무아레 무늬를 생성하기 위한 실험 장치도이다. 무아레 무늬를 생성하기 위한 과정을 살펴보자. 보통의 무아레 무늬는 비간섭성 광원, 즉 보통의 태양 빛이나 현광등, 백열전등의 빛으로도 무아레 무늬는 생성된다. 그러나 더 정확한 무늬를 생성하기 위하여 레이저를 사용하였다. 이 레이저의 빛은 beam expander 안의 작은 구멍은 통하여 확산된다. 이 확산된 빛은 미리 준비해둔 서로 다른 두 개의 격자들를 통과하면서 간섭을 일어나 무아레 무늬가 생성된다. 이때 생성되는 무늬를 CCD 카메라가 촬영하고 이 영상을 컴퓨터에서 분석을 한다. 무아레 무늬를 나타내는 데이터는 컴퓨터의 스캐닝 무아레 해석모듈에 의해서 구할 수 있다.



[Fig. 4] Experiments For Moire Pattern

실험에는 원형형태의 격자를 사용하였으며 원형 격자를 통과하는 물체 영역은 직각좌표계(x,y,z) 또는 원통좌표계(ρ,ϕ,z)로 표현되며 격자에 의한 회절된 빛의 영역의 거리 $z'=\frac{2p_0^2}{\lambda}$ 의 정수배에서 자체의 상을 만들어 낼 수 있으며 물체를 A(x,y)와 거리z를 두고 측정하면 회절면 A'이 결정된다.

$$A'(x',y',z')=C\int_{-\infty}^{\infty}dx\int_{-\infty}^{\infty}dyA(x,y)\exp(i\pi\frac{(x'-x)^2+(y'-y)^2}{\lambda z'})$$

여기서 $C=\exp(i2\pi z'/\lambda)/(i\lambda z')$ 이다.

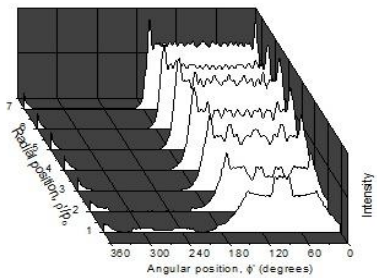
위 식을 원통 좌표계 (ρ,ϕ,z)로 변환하면 다음과 같이 된다.

$$A'(\rho',\phi',z')=C'\int_0^{2\pi}d\phi\int_0^{\infty}d\rho A(\rho,\phi)\exp(i\frac{\pi\rho^2}{\lambda z'})\exp(-i\frac{2\pi\rho'\rho}{\lambda z'}\cos(\phi-\phi'))$$

여기서 $C'=Cexp(i2\rho^2/\lambda z')$ 이다.

위 식을 통하여 생성되어지는 값(ρ',ϕ',z')들을 무아레 무

늬는 [Figure 5]에서 나타는 것 같이 3차원의 축으로 이루어진 값들로 Radial position의 값, Angular position의 값, 그리고 빛의 intensity 값으로 측정할 수 있으며, 이 값들은 격자들의 위치와 각도의 변화에 따라 변하는 값들로 빛의 간섭과 회절의 성질을 이용하여 생성되어진 값이기 때문에 아주 미세한 실험 조건의 변화에 의해서도 같은 결과 값을 절대로 같지 못하게 되며, 완벽하게 실험 조건이 일치해야만 같은 결과의 값을 얻을 수 있다. 3차원 축으로 측정된 값들의 데이터는 매우 작은 수들로 이루어져 있기 때문에 그 결과 중에 특징이 되는 곳의 일부를 선택하여 참난수로 사용한다. 이때 만들어진 난수들은 암호 시스템에 필요한 키 값들로 다시 만들어서 사용한다. 예를 들어 결과로 얻어진 난수들을 XOR 이나 블록 암호 알고리즘 기반의 난수 발생 알고리즘을 이용하여 실질적으로 암호 시스템에 사용될 키 값들로 형성할 수 있다.



[Fig. 5] Analysis Data Graph of Moire Pattern Experiment

3. 결론

본 논문에서는 물리적 현상의 무아레 무늬에 생성된 결과 값들을 가지고 참난수로 사용할 수 있음 제시하였다. 결과로 나온 난수들을 어떻게 이진 함수의 수로 결정을 지을 것인지와 이 난수들을 암호 알고리즘에 어떻게 실제적으로 사용할 수 있을지 연구와 테스트가 필요할 것이며, 탈봇-라우 간섭계와 같은 다른 간섭 무늬와 회절을 이용하여 보다 정교한 측정값을 참난수로 사용할 수 있는 연구가 필요할 것이다. 그리고 앞으로 모바일의 카메라 즉 CMOS를 이용하여 무아레 무늬를 측정, 그 카메라를 이용한 눈동자 속에서 발생하는 무아레 무늬를 측정, 보다 경량화되고 실용화된 측정 방법 연구와 현재 이슈가 되고 있는 양자 암호와의 다른 방식의 암호화를 기대해본다. 또한 무아레 무늬를 이용한 간편하고 저렴하며 보안성이 강조된 3차원 안면인식기술에 적용 및 응용될 수 있음을 기대해본다.

REFERENCES

[1] C.A. Sciammarella, “The moire method - A Review’, Experimental Mechanics, 1982.
[2] Isaac Amidror, “The Theory of the Moiré Phenomenon”, Springer, 2002.
[3] Tong Tu, Wooi-Boon Goh, “Moire patterns from a CCD camera”, VISAPP 2009 -Proceedings of the Fourth International Conference on Computer Vision Theory and Applications, Lisboa, Portugal, February 5-8, 2009.
[4] 강종성, “늘인 원형격자의 프레넬 결상 분석”, 2003.
[5] 송정환 외 4명, “국산 블록 암호알고리즘 등을 이용한 난수 발생 연구”, KISA, 2011.
[6] 김일환, 육근철, 조재홍, 장수, "두 원형 격자의 무아레 간섭 무늬를 이용한 회전각 측정", 새물리 32, 674 - 678 (1992).
[7] 이금분, 조범준, “가상광학에 기반한 강인한 디지털 워터마킹”, 한국정보통신학회논문지, 1073-1080 (2011)
[8] 장수, 조재홍 외, “광학”, 도서출판사 대웅
[9] 한국광학회 대구경북지회, “광학의 기초” (2003)
[10] http://functionspace.com/topic/116

강 혁(Hyeok Kang) [정회원]

- 2001년 2월 : 고려대학교 물리학과 졸업
- 2003년 6월 : 고려대학교 대학원 졸업 (전산학 석사)
- 2008년 3월 ~ 2013년 2월 : 워싱턴 대학교 대학원 수료 (컴퓨터공학 박사과정)
- 2015년 3월 ~ 현재 : 백석대학교 정보통신학과 강사

<관심분야>
양자암호, 암호키 키 생성, 사물인터넷, 무아레 현상

이 근 호(Keun ho Lee) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC 연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야>

M2M 보안, 이동통신보안, 융합보안, 개인정보보안