LFSR과 2D CAT를 이용한 단계적 영상 암호화

남태희* · 김석태** · 조성진***

Gradual Encryption of Image using LFSR and 2D CAT

Tae-Hee Nam* · Seok-Tae Kim** · Sung-Jin Cho***

요 약

본 논문에서는 LFSR(Linear Feedback Shift Register)과 2D CAT(Two-Dimensional Cellular Automata Transform)를 단계적으로 적용한 영상 암호화 방법을 제안한다. 먼저 LFSR을 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 그런 다음, 생성된 수열을 원 영상과 XOR 연산하여 1단계로 암호화된 영상을 얻는다. 그리고, 게이트웨이 값을 설정하여 2D CAT 기저함수를 생성한다. 생성된 기저함수를 1단계로 암호화된 영상에 곱하여 2D CAT 방법으로 암호화를 한다. 마지막으로, 안정성 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음을 검증한다.

ABSTRACT

In this paper, we propose the gradual encryption method of image using LFSR(Linear Feedback Shift Register) and 2D CAT(Two-Dimensional Cellular Automata Transform). First, an LFSR is used to create a PN(pseudo noise) sequence, which is identical to the size of the original image. Then the created sequence goes through an XOR operation with the original image resulting to the first encrypted image. Next, the gateway value is set to produce a 2D CAT basis function. The created basis function multiplied with the first encrypted image produces the 2D CAT encrypted image which is the final output. Lastly, the stability analysis verifies that the proposed method holds a high encryption quality status.

키워드

CAT(Cellular Automata Transform), PN(pseudo noise) sequences, LFSR(Linear Feedback Shift Register), Gateway Values

* 동주대학 의료기공학과 교수

** 부경대학교 전자컴퓨터정보통신공학부 교수(교신저자)

*** 부경대학교 수리과학부 교수

접수일자 2009. 05. 29

Ⅰ. 서 론

유비쿼터스 환경은 사용자의 편의에 맞게 구성된 새로운 네트워크 환경으로 우리가 인식하지 못하고 있는 사이 우리의 생활 속에 서서히 스며들고 있다. 즉 유비쿼터스 환경은 누구든, 언제, 어디서나, 어떤 정보라도 쉽게 활용할 수 있게 한다. 한편 유비쿼터스 환경은 자유로운 정보 활용에 따른 정보의 변질, 무단도용, 등의 부작용에 대한 강력한 보안 기술을 요구하고 있다. 만일 보안의 취약성으로 주요 정보가 유출된다면 개인 프라이버시 침해나 저작권에 대한 심각한 문제가 발생할 수 있다. 특히 정보유통의 대부분을 차지하고 있는 영상에서의 보안기술은 대단히 중요한 테마이다. 최근에 영상정보의 보안에 관한 취약성을 사전에 예방하고 자유로운 컨텐츠 활용을 위해 영상 분야에서 암호화하는 방법이 다수 제안되어 있다[1-7].

이들 암호화 방법 중 Scharinger는 Kolmogorov flow map을 이용한 영상 암호화 기법을 제안 하였으며[8], Wong은 chaotic standard map을 기반으로 한 영상 암호화 방법을 제안하였다[9]. 또한 Pareek은 두 개의 chaotic logistic maps와 긴 키를 이용하여 영상을 암호화하는 방법을 제안하였다[10]. 제안한 방법들은 대부분 영상의 픽셀 위치를 discredited chaotic map을 이용하여 변환 시킨 다음, CBC(Cipher Block Chain) 모드로 픽셀 값을 변환하기 때문에 암호화 효과가 떨어지는 단점이 있다.

본 논문에서는 기존 방법과 달리 최대 주기를 갖는 LFSR(Linear Feedback Shift Register)과 2D CAT(Two-Dimensional Cellular Automata Transform)를 단계적으로 이용한 새로운 영상 암호화 방법을 제안한다.

암호화 방법은 먼저, LFSR을 이용하여 원 영상의 크기만큼 PN(pseudo noise) 수열을 생성한다. 생성된 PN 수열을 이용하여 LFSR 기저 영상을 만든다. 그 후 생성된 LFSR 기저 영상과 원 영상을 XOR 연산하여 LFSR이 적용된 1단계 암호화 영상을 구한다. 그 다음, 2D CAT의 게이트웨이 값을 설정하고 이를 이용한 2D 기저함수를 생성한다. 마지막으로, 이미 암호화된 LFSR 영상에 2D 기저함수를 곱하여 최종적으로 영상을 암호화한다.

또한 복호화 방법은 생성된 2D 기저함수가 직교성질을 갖고 있기 때문에 역 CAT로서 암호화된 영상은 LFSR 변환 영상으로 변환한다. 변환된 LFSR 변환 영상을 LFSR 기저 영상과 XOR 연산하여 무 손실 복원한다.

마지막으로 키 공간, PSNR(Peak Signal to Noise Ratio), 그리고 히스토그램 분석을 통하여 제안한 방법이 높은 암호화 수준의 성질을 가졌음이 실험을 통하여 확인한다.

Ⅱ. 제안 방법

본 논문에서는 LFSR과 2D CAT를 단계적으로 이용하여 영상 암호화 방법을 제안한다. 제안 과정은 먼저 LFSR을 이용하여 PN 수열을 생성한다. 생성된 수열을 이용하여 기저영상을 만든다. 그리고 생성된 기저영상과 원 영상을 XOR 연산으로 변환 영상을 구한다. 그 다음 게이트웨이 값을 이용해서 2D CAT 기저함수를 생성하여 변환된 영상을 암호화 영상으로 변환한다.

또한 복호화 방법은 생성된 2D 기저함수가 직교하는 성질을 갖고 있기 때문에 역 CAT로서 암호화된 영상은 LFSR 변환 영상으로 복원되고, 이를 LFSR 기저 영상과 XOR 연산하여 복호화 영상을 얻는다.

제안하는 암호화 과정의 흐름도는 그림 1과 같다.

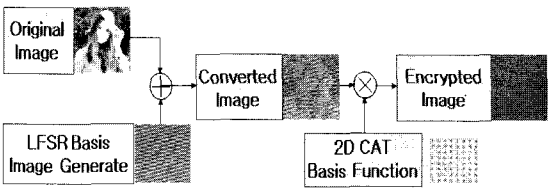


그림. 1 제안된 암호화 방법의 흐름도
Fig. 1. Flowchart of proposed encryption method

LFSR은 주기적 스트림 암호화에 이용되는 기법으로 주로 의사 난수를 발생시킨다[11,12]. 이것은 비트 단위로 암호화하므로 오류 확산 현상이 없고 블록 암호 알고리즘에 비해 빠르고 구현이 쉽다.

본 논문에서 제안된 LFSR 구조는 그림 2와 같다.

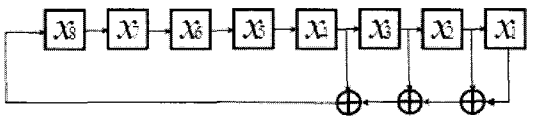


그림 2. 제안된 LFSR 구조
Fig. 2. Proposed LFSR structure

제안된 방법은 8비트와 귀환회로 XOR 연산자로 구성되어 최대 길이 사이클을 보여주며, 8,4,3,2에 탭을 가지고 있다. 이것은 식 (1)과 같이 특성다항식[13]으로 표현된다.

$$x^8+x^4+x^3+x^2+1 \tag{1}$$

또한 선형 귀환함수 f는 식 (2)와 같이 표현된다.

$$f(x_1,x_2,...,x_8)=x_8\oplus x_4\oplus x_3\oplus x_2\oplus x_1 \tag{2}$$

LFSR 기저영상의 생성은 식 (2)를 이용한다. 즉 생성된 기저영상과 원 영상을 XOR 연산으로 LFSR이 적용된 변환 영상을 구한다.

또한 CAT는 동역학계를 해석하는 한 방법으로 시간과 공간을 이산적으로 다루는 시스템으로서 복잡한 자연현상을 시뮬레이션 하는데 유용한 도구이다[14]. 그 기본은 1D CA로서, 모든 셀들이 선형으로 배열되어 있는 3-이웃 CA이다.

$$a_{i,t+1}=f[a_{i,t},a_{i+1,t},a_{i-1,t}] \tag{3}$$

식 (3)은 상태전이 함수로서, f는 결합논리를 가지는 국소전이함수이며, 서로 다른 2^3 개의 이웃하는 배열상태가 존재한다. CAT는 2D 영상 공간이 $n\times n$ 셀일 경우, 기저함수는 $A_k\equiv A_{ijkl},(i,j,k,l=0,1,....,N-1)$이다. 또한 $f_{ij}(i,j=0,1,2,...,N-1)$의 2D CAT는 식 (4)와 같다.

$$f_{ij}=\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}c_{kl}Aijkl \quad (i,j=0,1,2,....,N-1) \tag{4}$$

본 논문에서는 영상 암호화를 위해 2D 기저함수를 생성한다. 2D 기저함수는 먼저 2D CA 공간 $a\equiv a_{ijt}(i,j,t=0,1,2,...,N-1)$에서 2D 기저함수 A_{ijkl}을 생성한다. 이것은 1D 기저함수 A_{ik}로부터 생성한다. 식 (5)는 2D 기저 함수식이다.

$$A_{ijkl}=A_{ik}A_{jl} \tag{5}$$

2D CAT 기저함수를 구하는 절차는 그림 3에 나타내었다.

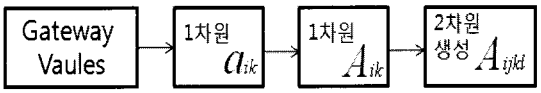


그림 3. 2D 기저함수 생성과정
Fig. 3. 2D basis function generation process

2D 기저함수는 표 1을 이용하여 생성한다.

표 1. 게이트웨이 값
Table 1. Gateway Values

Gateway	Values
Wolfram Rule	**14**
Number of Cells per Neighborhood	**3**
Number of Cells in Lattice	**8**
Initial Configuration	**01001101**
Boundary Configuration	**Cyclic**
Basis Function Type	$A_{ik}=2a_{ik}a_{ki}-1$

게이트웨이 값의 조건하에서 갱신되는 셀들의 상태전이함수식은 식 (6)과 같다.

$$a_{(r)(t+1)}=\left(\sum_{j=0}^{2^m-2}W_j\alpha_j+W_{2^m-1}\right)^{W_{2^m}}\bmod K$$
$$a_{(1)(t+1)}=(W_0a_{0t}+W_1a_{1t}+W_2a_{2t}+W_3a_{0t}a_{1t}+$$
$$W_4a_{1t}a_{2t}+W_5a_{2t}a_{0t}+W_6a_{0t}a_{1t}a_{2t}+W_7)^{W_{2^3}}\bmod K \tag{6}$$

식 (6)에서 $r=1$이고 $t+1$일 경우, 조건은 $0\le W_j\le 2$이다. α_j는 이웃 셀 상태들의 조합으로 이루어진다. 이것은 1D 3-이웃이다. 따라서 m=3으로 $W_{2^3}=W_8$의 값을 가진다. 여기서 셀들의 상태는 시간 t $(t=k)$에서 a_{0k},a_{1k},a_{2k}순으로 정의된다. 2D 기저함수는 1D 기저함수로부터 구할 수 있다. 기저 함수 타입를 이용하여 2D CAT 식 (7)를 구한다[15].

$$c_{kl}=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}f_{ij}A_{ijkl}\ (k,l=0,1,2,...,N-1) \tag{7}$$

식 (7)을 이용하여 영상을 암호화한다. 게이트웨이 값에 의해 생성된 2D 기저함수는 그림 4와 같이 나타내었다.

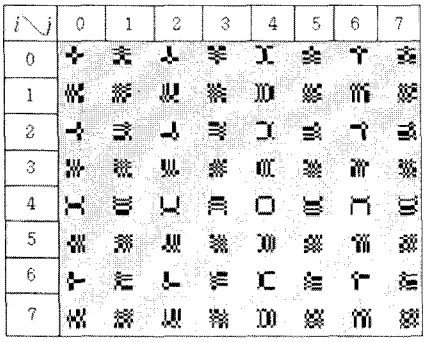


그림 4. 2D 기저 함수
Fig. 4. 2D basis function

Ⅲ. 실험 결과

실험에서는 256×256 크기의 8비트 그레이 레벨 영상을 이용하여 그 변화를 고찰 하였다.

본 논문에서는 100개의 영상들을 가지고 실험하였으며, 그 중 일부 영상들을 그림 5에 나타내었다.

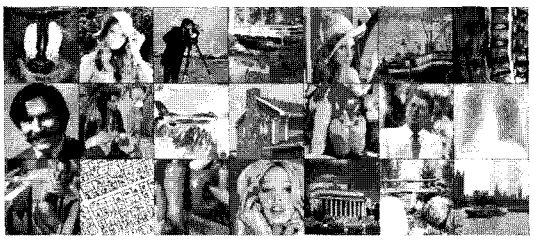


그림 5. 실험 영상들
Fig. 5. Experimental images

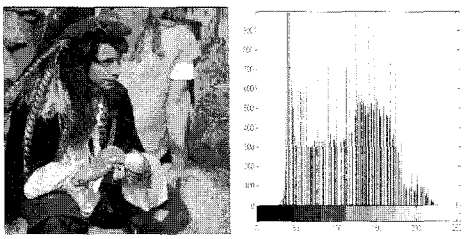
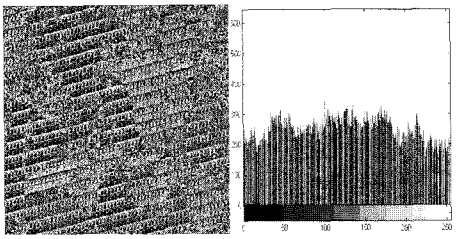
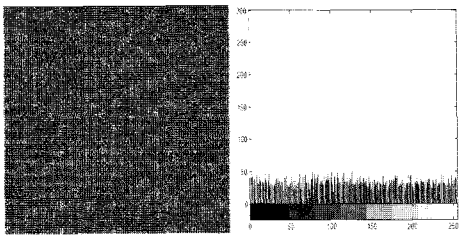


그림. 6 원 영상 "man"과 히스토그램
Fig. 6. Original image "man" and Histogram



PSNR of encrypted image(PSNR=+25.4380 dB)
그림 7. LFSR과 원 영상과의 XOR 연산에 의한 영상과 히스토그램
Fig. 7. Image and Histogram by XOR operation with LFSR and Original image



PSNR of encrypted image(PSNR=+23.6739 dB)
그림 8. LFSR과 2D CAT를 이용하여 암호화된 영상과 히스토그램
Fig. 8. Encrypted image and Histogram using LFSR and 2D CAT

LFSR에 의해 생성된 PN 수열과 원 영상을 XOR 연산하여 생성된 LFSR 변환 영상은 그림 7에 보였다. 또한 LFSR 변환 영상에 2D CAT 기저 함수를 곱하여 얻은 2D CAT 영상 암호화의 결과 영상은 그림 8에 나타내었다.

여기서 암호화된 영상을 분석하기 위해 PSNR을 사용하였다. PSNR은 원 영상과 잡음 영상의 비로서, 암호화된 그림 8은 +23.6739 dB로서 영상의 왜곡이 크다는 것을 확인하였다. PSNR은 그 값이 낮을수록 영상의 왜곡이 크다는 것을 의미하는데, 보통 PSNR<35 dB이면, 시각적으로 영상의 왜곡을 느낄 수 있다.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)[dB] \tag{8}$$

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(I_{ij} - K_{ij})^2$$

식(8)에서 255는 픽셀의 최대 값으로 8비트 잡음 또는

밝기를 나타내며 dB로 표현한다. 또한 MSE는 오차제곱 평균으로 i 와 j 값은 가로와 세로 영상을 의미하며, 두 개의 같은 양의 영상 데이터에 대해 동일한 위치의 분산을 계산한다.

다음은 실험한 영상의 일부 과정을 그림 9에 나타내었다.

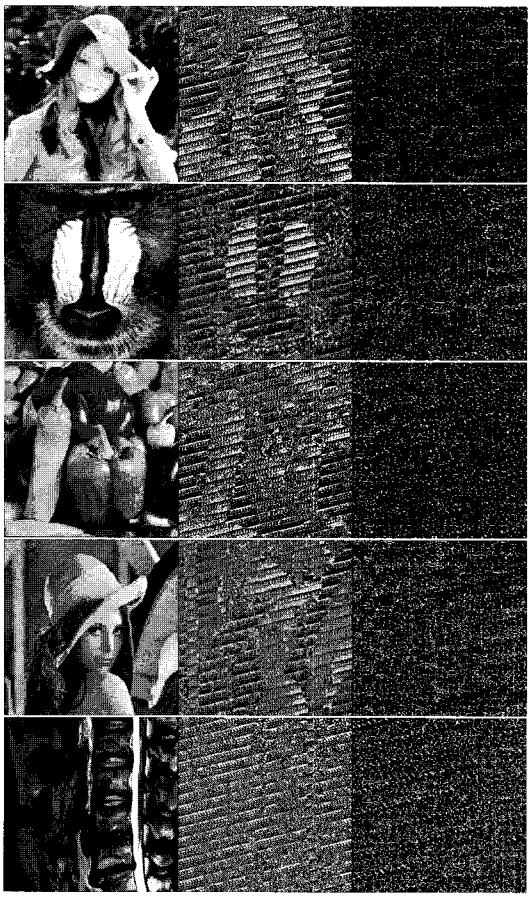


그림 9. 원 영상들, LFSR 변환된 영상들, 2D CAT에 의한 암호화된 영상들
Fig. 9. Original images, LFSR converted images, Encrypted images by 2D CAT

실험 결과를 통해서 원 영상과 비교 했을 때 각 픽셀 간의 연관성을 전혀 예측 할 수 없도록 고르게 출력됨을 그림 9에서 확인할 수 있었다.

Ⅳ. 안정성 분석

2D CAT를 이용하여 키 공간을 분석할 수 있는 주요 키는 CA 규칙, 셀 당 최대 상태의 수, 이웃 셀 수, 초기 구성, 경계 형상, 기저함수 타입 등이 있다. 큰 범위의 키 공간은 영상의 암호화 수준을 높인다.

본 논문에서 제안된 조건은 8-셀, 2-상태, 5-이웃이다. 따라서 2D CA는 $N_T^2 = K^{k''+3(N+M)+2T} = 2^{96}$ $(2^{2^7+3(8+8)+2\times 8})$가지의 키를 생성한다. 이것은 일반 CA 키를 이용한 영상 암호화 수준보다 훨씬 향상된 결과이다. 또한 LFSR은 1D 주기적 수열을 갖는 스트림 암호화 방법으로서 서로 다른 2^n가지의 키를 가진다.

따라서 본 논문에 제안된 영상 암호화 방법은 총 $2^{8+96} = 2^{104}$가지의 일정한 키를 생성할 수 있기 때문에 충분한 암호화 수준을 확보할 수 있다.

그러나 일반적인 CA 적용은 일정한 규칙에 의해 변환되기 때문에 영상이 매우 민감하게 반응한다. 따라서 허용되지 않는 일반적인 외부 키를 적용하면, 원 영상으로 전혀 복원할 수 없음을 그림 10에서 보여준다.

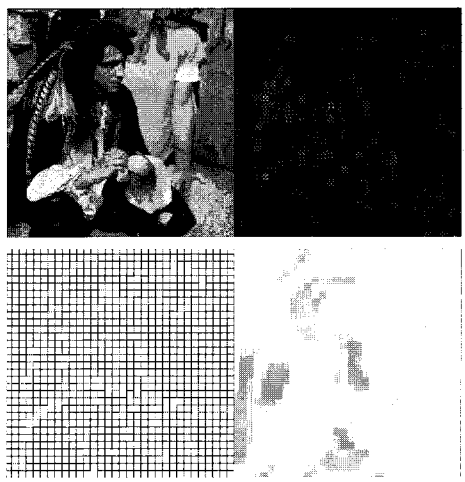


그림. 10 정상적인 복원 영상과 허용되지 않는 키에 의한 복원 영상들
Fig. 10. Restoration images by impermissible key with normal restoration image

V. 결 론

본 논문에서는 원 영상을 암호화하기 위해 LFSR과 2D CAT 방법을 단계적으로 적용하였다. LFSR은 주기적인 난수 발생으로 영상 암호화에 매우 유용하다. 또한 2D CAT는 시간과 공간을 이산적으로 다루는 시스템으로서 매우 랜덤성이 강한 성질을 가지고 있다. 본 논문에서는 이러한 성질을 단계적으로 암호화에 적용해 암호화의 수준을 높였다.

제안한 암호화 방법은 Java 프로그램과 Matlab으로 실험하였으며, 약 100개의 영상을 실험 대상으로 사용하였다. 또한 키 공간, PSNR, 그리고 히스토그램 분석을 통하여 본 제안방법이 높은 암호화 수준의 성질을 가졌으며 외부 공격에 대해 강인한 특성이 있음을 확인하였다.

향후 연구 과제로는 2D CAT 기저함수의 성질을 분석하여 이를 다른 분야에 응용하는 방법 혹은 랜덤성을 가진 다른 방법과의 결합을 통해 고효율의 영상 암호화 방법을 개발해야 할 것으로 생각된다.

참고문헌

[1] 박진, 나철훈, "디지털 컨텐츠의 보호기술에 관한 기술동향 분석", 한국해양정보통신학회논문집, pp. 1094-1097, May. 2005.

[2] 송학현, 김윤호, 류광렬, "영상 콘텐츠 지적재산권 보호 워터마킹 기술", 한국해양정보통신학회논문집, pp.144-148, May. 2004.

[3] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, Oct. 1996.

[4] 이지범, 고형화, "인터리빙과 랜덤 셔플링을 이용한 디지털 영상의 암호화 방법", 한국통신학회논문지. Vol. 31, No. 5C, pp. 497-502, May. 2006.

[5] A. Uhl, Image and Video Encryption, Springer Science, 2005.

[6] 박성호, 최현준, 서영호, 김동욱, "DCT-기반 영상/비디오 보안을 위한 암호화 기법 및 하드웨어 구현", 전자공학회논문지, Vol. 42, SP No. 2, pp. 27-36, Mar. 2005.

[7] 남태희, 김석태, 조성진, "90/150 NBCA 구조를 이용한 영상 암호화", 한국해양정보통신학회, 2009년도 춘계종합학술대회, Vol. 13, No. 1, pp. 152-155, May. 2009.

[8] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov Flows", J Electron Image, Vol. 2, No. 2, pp. 318-325, Apr. 1998.

[9] K.W. Wong, S.H. Kwok, and W.S. Law, "A fast image encryption scheme based on chaotic standard map", Physics Letters A, Dec. 2007.

[10] N.K. Pareek, V. Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Feb. 2006.

[11] H.Y. Song, "Feedback Shift Register Sequences", Encyclopedia of telecommunications, edited by G. J. Proakis, John Wiley & Sons, New York, Dec 2002.

[12] 남태희, 김석태, 조성진, "LFSR과 CAT을 이용한 영상 암호화", 한국해양정보통신학회, 2009년도 춘계종합학술대회, Vol. 13, No. 1, pp. 164-167, May. 2009.

[13] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S.H. Heo, "New synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata", IEEE Transactions on computer-aided design of integrated circuits and systems, Vol. 26, No. 9, pp. 1720-1724, Aug. 2007.

[14] O. Lafe, "Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, Jan. 2000.

[15] 박영일, 김석태, "다해상도 특성을 갖는 2D 셀룰러 오토마타변환을 이용한 디지탈 워터마킹", 한국통신학회논문지, Vol. 34, No. 1, pp. 105-112, Jan. 2009.

저자소개

남태희(Tae-Hee Nam)

1996년~부경대학교 전자공학과 박사수료
1993년~현재 동주대학 의료기공학과 교수

※관심분야 : Cellular Automata, 영상처리, 의료정보

김석태(Seok-Tae Kim)

1983년 8월 광운대학교 전자공학과 공학사
1988년 8월 Kyoto Institute of Technology, 전자공학과 공학석사
1991년 8월 Osaka대학교 통신공학과 공학박사
1999년 Univ. of washington, USA 방문교수
2006년 Simon Fraser Univ., Canada 방문교수
1991년~현재 부경대학교 전자컴퓨터정보통신공학부 교수

※관심분야 : 영상처리, 패턴인식, 워터마킹, Cellular automata.

조성진(Sung-Jin Cho)

1979년~ 강원대학 수학교육과 이학사
1981년~ 고려대학교 수학과 대학원 이학석사
1988년 고려대학교 수학과 대학원 이학박사
1988년~현재 부경대학교 자연과학대학 수리과학부 교수

※관심분야 : Cellular Automata론, ATM, Queueing론