韓國컴퓨터情報學會 論文誌
第16卷 第2號, 2011. 2.

2011-16-2-4-2

혼돈신호의 동기화를 이용한 근거리 보안 전자액자 설계

김 홍 섭*, 임 거 수**

Design of a digital photo frame for close-range security using the chaotic signals synchronization

Hong-Sop Kim*, Geo-Su Yim**

요 약

디지털 디스플레이어의 보급과 발달로 인하여 기존의 인쇄용 액자보다 디지털 액자에 대한 관심이 높아지고 있다. 우리는 이런 디지털 액자를 정적인 자료 디스플레이용도 뿐만 아니라 CCD 카메라와 조합하여 감시용 모니터링 장비로 활용하기 위한 새로운 LCD 전자 액자를 개발하였다. 개발된 액자는 감시용 화상 데이터의 보안을 위해 기존의 양방향 통신 암호화를 대체하여 단방향 통신 암호화 방법으로 개발 하였다. 이 방법은 혼돈계의 단방향 동기화 현상을 이용한 것으로 일정 시간 동안 동기화를 진행 시키면 어느 시점에서든 암호화와 복호화를 시킬 수 있는 방법으로 양방향 통신 암호화와 같은 결과를 얻을 수 있다. 또한, 우리가 제시한 이 방법을 유비쿼터스 기기의 근거리 통신방법에 적용한다면 보다 효율적인 결과를 얻을 수 있을 것으로 생각된다.

▸ Keyword : 전자액자, CCD카메라, 근거리통신, 혼돈신호, 암호화, 복호화

Abstract

With the development and supply of digital displayers, there has been a heightened interest of late in digital photo frames, eclipsing the existing print frames. This digital photo frame was developed into a new LCD digital photo frame that can be used not only for data display but also as a surveillance monitoring equipment when combined with a CCD camera. The developed photo frame uses a one-way communication encryption method that replaces the existing two-way communication encryption method to ensure the security of the surveillance image data. This method uses the chaotic signal's one-way synchronization phenomenon, where synchronization is made for a certain amount of time, after which the synchronized data can be encrypted and decoded at any point. It can yield the same results as the two-way communication encryption method. Moreover, if the proposed method is applied to the close-range communication methods of ubiquitous devices, it will be able to obtain more efficient results.

• 제1저자 : 김홍섭 교신저자 : 임거수
• 투고일 : 2011. 01. 31, 심사일 : 2011. 02. 09, 게재확정일 : 2011. 02. 13.
*오산대학 멀티미디어정보과 (Dept. of Multimedia Information, Osan University)
** 배재대학교 과학기술학부 (Division of Science and Technology, Paichai University)
※ 이 연구는 2010학년도 오산대학 교내 연구비 지원에 의하여 이루어졌음.

▸ Keyword : Digital Photo Frame, CCD Camera, Cloase-range Security, Chaotic Signal, Encryption, Decryption

Ⅰ. 서 론

정보통신의 발달은 디지털 장비의 발달과 더불어 멀티미디어 장비에 대한 연구도 많이 이루어지게 하였다. 그 중 전자액자에 대한 관심은 액자 본연의 용도 보다는 응용성에 초점을 맞추어 많은 연구가 이루어지고 있다. [1-4]

전자액자를 단순한 디스플레이 장치가 아닌 스트리밍 서버를 이용한 미디어 디스플레이 장치 또는 유비쿼터스 기반으로 전자액자를 구성하는 결과가 많이 보고되고 있고, 우리는 이런 전자액자를 단순히 저장되어 있는 미디어 파일을 보는 장치에서 감시용 카메라로 활용할 수 있는 방법에 대한 연구를 진행 하였고, 연구 결과로 LCD 전자 액자는 제품으로 완성하였다. 감시용 전자액자는 무엇보다 전송 되는 화상 이미지에 대한 보안이 중요하다. 따라서 보안성과 경제적인 측면을 고려하여 단방향 암호화 방법을 구현 하였다. 우리가 구현한 단방향 암호화 방법은 혼돈계의 동기화 현상을 이용한 방법으로 CCD(Charge Coupled Device) 카메라의 혼돈 계와 LCD 전자액자의 혼돈계가 단방향 피드백으로 동기화 되어 CCD 카메라에서 암호화 시킨 데이터를 LCD 전자액자에서 손실 없이 복호화 할 수 있는 방법이다. 반면, 동기화가 되지 않은 다른 LCD 전자액자는 전송되는 이미지를 복호화 할 수 없게 된다. 그리고 이 단방향 방법은 기기 사용에 있어서 2개의 제약조건을 지니게 된다. 하나는 CCD 카메라에서 동기화 신호를 송신하면 LCD 전자액자에서 동기화 수신 버튼을 눌러야 하는 것이고, 둘째는 버튼을 누르고 동기화 될 때 까지 기다려야 하다는 것이다. 그러나 동기화 속도는 사람이 인지하는 시간 보다 매우 빠르기 때문에 버튼을 누르는 동시에 동기화가 이루어져 기기 사용에 큰 문제점은 없을 것이다. 그리고 이렇게 혼돈계로 구성된 단방향 암호화 방법이 근거리 통신을 주로 사용하는 유비쿼터스 장비에 적용 된다면 보안뿐만 아니라 경제적인 면에서도 큰 효과를 얻을 수 있을 것이다. 우리는 이런 연구 결과를 가시화 하기위해 디지털 전자액자의 외형 및 내부를 제시하고, 혼돈 계를 사용한 암호화 방법 중 동기화에 대한 설명과 암호화된 결과를 상관계수 계산법을 이용하여 암호화 정도를 수치적으로 나타낸다.

Ⅱ. 디지털 전자액자

1. 유비쿼터스의 전자액자

디지털 전자액자에 대한 연구 및 상품은 이미 기존의 시장을 점유하고 있는 상태이고 디지털 액자의 편의성 때문에 많은 호응을 받고 있는 상태이다. 이런 이유로 디지털 액자를 이용한 연구가 많이 이루어지고 있다. 디지털 전자액자를 단순한 뷰어 기능에서 센서 네트워크를 이용한 주변 환경의 조도, 온도, 습도 등을 모니터링 하는 유비쿼터스 장비로 활용하는 연구, 또는 스트리밍서버 및 웹서버에 접속 할 수 있는 미디어 재생 장치와 같은 연구가 이루어지고 있다. [1-4]

그림 1. CCD 카메라 모듈
Fig. 1. CCD Camera MOdule

우리는 지금 까지 단순한 기능의 저장된 멀티미디어 뷰어로 사용되는 전자액자를 근거리 지역의 보안이나 감시 목적의 모니터링 장비로 활용할 수 있는 방법과 그것에 필요한 보안에 대한 연구를 진행 하고 그 결과를 보인다. 그림 1. 은 감시 대상의 화상데이터를 전송하는 CCD 카메라 송신기 인쇄회로 기판(printed circuit board) 이며, 그림 2. 는 CCD 카메라에서 전송된 화상데이터를 디스플레이 하는 LCD 전자액자의 모습이다. 전자액자는 일반적인 전자액자 및 미디어 파일 재생과 같은 PMP(Portable Multimedia Player) 기능과 더불어 암호화가 적용된 모니터링 장비의 기능을 가지고 있다.

그림 2. LCD 전자액자
Fig. 2. LCD Digital Photo Frame

III. 화상 데이터 암호화 방법

무선 카메라 송신 모듈을 이용한 감시용 전자액자 개발에 있어서 가장 중요한 부분이 전송되는 화상데이터에 대한 보안의 문제점이다. 우리는 이 문제점을 해결하기 위해 화상 데이터의 보안을 위한 새로운 보안 알고리즘을 구성 하였다. 기존의 통신 암호화 방법은 대부분 양방향 통신으로 암호화가 이루어지고, 이후 암호화된 데이터가 송신 되는 방식이다. 그러나 우리는 혼돈계의 동기화를 이용하여 양방향 암호화를 대체할 수 있는 단방향 암호화 방법을 구성하고 그 내용을 LCD 전자액자로 구현 하였다.

1. 혼돈신호의 암호화

혼돈 계에 대한 연구는 이 공학뿐만 아니라 경제학에서도 많은 연구가 진행 되고 있다. 우리는 이런 혼돈계의 신호를 암호화에 적용 시키려고 한다. 혼돈신호는 그 결과가 잡음과 매우 유사하다. 그러나 잡음과 달리 이전 값을 알면 이후 값을 계산 할 수 있는 특성이 있다. 이것이 암호화된 데이터를 복호화 할 수 있는 특성인 것이다. 잡음은 혼돈 신호와 형태는 유사 하지만 이전 값으로 이후 값을 생산 할 수 없으므로 암호화 된 데이터를 복호화 할 수 없는 문제점을 가지게 된다. 현재 혼돈신호를 이용한 암호화 방법의 대표적인 방법은 CKBA(Chaotic key-based algorithm) 방법으로 혼돈 신호를 킷 값으로 하여 데이터를 암호화 하는 방법이다. [5-7]

이렇게 암호화에 사용되는 혼돈 계는 크게 Map 구조의 Logistic, Henon Map과, ODE 시스템으로는 Lorenz, Rossler 등이 있다. [8] 우리는 이 혼돈계 중 이후 전자회로 구현이 용이한 ODE 시스템 중 Lorenz 시스템을 암호화에 사용 하였다.

$$\begin{aligned}\dot{x}_1 &= \sigma(y_1 - x_1) \\ \dot{y}_1 &= x_1(\rho - z_1) - y_1 \\ \dot{z}_1 &= x_1 y_1 - \beta z_1\end{aligned} \quad \cdots\cdots (1)$$

위의 식 (1)은 Lorenz 식을 나타낸 것이다. 컴퓨터 시뮬레이션을 위해 시스템에서 매개변수 $\sigma = 10.0$ 이고 $\beta = 8/3$ 그리고 $\rho = 28.0$ 으로 설정하여 암호화에 사용하였다. [9]

2. 혼돈신호의 동기화

혼돈계 시스템의 특징 중 가장 대표적인 것이 시스템의 동기화 이다. 동기화란 초기 값에 의해 다른 궤적을 나타내는 두 개의 서로 다른 혼돈계가 외부의 영향에 의해 특정 시간 이후 같은 궤적을 그리게 되는 현상이다. 대표적인 예로는 '호이겐스의 시계' 를 들 수 있다. 네덜란드의 물리학자인 호이겐스는 같은 벽에 걸려 있는 시계들이 일정 시간이후에 시계추의 주기가 모두 같아지는 것을 발견 하였다. 이것은 시계추의 진동이 벽을 통해 다른 시계에 영향을 주었기 때문에 동기화가 된 것이다.

$$\begin{aligned}\dot{x}_2 &= \sigma(y_2 - x_2) + k(x_2 - x_1) \\ \dot{y}_2 &= x_2(\rho - z_2) - y_2 \\ \dot{z}_2 &= x_2 y_2 - \beta z_2\end{aligned} \quad \cdots\cdots (2)$$

우리는 이런 동기화를 단방향으로 구현 하기위해 2개의 Lorenz 시스템을 구축하고 두 번째 시스템을 식(2) 에 보인다.

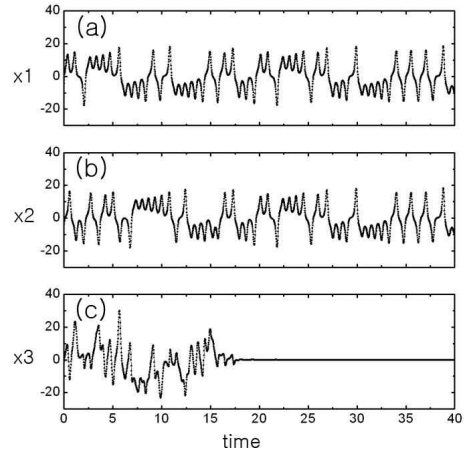

그림 3. 동기화 시계열
Fig. 3. Temporal behaviors of Synchronization

우리는 이런 혼돈계의 동기화를 단방향 암호화 통신에 응용하여 근거리 통신에 적용 시키는 연구를 진행 하였다. CCD 카메라와 LCD 전자 액자 사이의 근거리 통신 및 동기화 그리고 데이터 암호화에 대한 내용을 그림 4. 의 순차 UML 로 설명한다.

(a) 단계는 CCD 카메라와 LCD 전자액자의 혼돈 계가 초기화 되어 신호 값을 발생 하는 단계이다. CCD 카메라의 혼돈신호 X_a와 LCD 전자액자의 혼돈신호 X_b는 서로 다른 결과를 나타낸다. 그 이유는 서로 다른 초기 값으로 시작된 혼돈계 이기 때문에 신호가 서로 다른 것이다. 이런 현상이 혼돈의 특성중 하나인 초기치 민감성 이다. [11]

(b) 단계는 CCD 카메라에서 발생된 데이터 D_a 와 혼돈신호 X_a 가 $\oplus$ 연산으로 암호화 된 데이터 E_a 가 LCD 전자액자로 송신된 상태이다. E_a는 전자액자의 혼돈 신호 X_b와 $\oplus$ 연산을 수행하여 복호화 된 D_b를 생성 시키지만 D_a와 서로 다른 결과 값을 나타낸다. 이것이 동기화로 인증되지 않은 LCD 전자액자에서 나타나는 결과가 되는 것이다.

(c) 단계는 CCD 카메라에서 화상 데이터를 송신하지 않고 동기화를 위한 혼돈계의 신호를 송신 한다. LCD 전자액자에 수신된 데이터는 복호화 연산을 수행하지 않고, 동기화에 사용 된다. 이렇게 동기화가 완료되면 CCD 카메라와 LCD 전자액자는 같은 혼돈신호를 발생하는 혼돈계가 된다. 이 결과는 그림 3. 의 시계열에서 확인 할 수 있다.

(d) 단계 에서는 동기화 이후 CCD 카메라의 X_a와 LCD 전자액자의 X_b가 같기 때문에 화상 데이터 D_a와 D_b 역시 같아진다. 이것이 암호화된 데이터 E_a가 동기화된 LCD 전자액자 에서만 복호화가 되는 결과이다.

3. 암호화 결과

CCD 카메라와 LCD 전자액자의 단방향 암호화 통신 방법의 알고리즘을 프로그램으로 구현하여 실행한 결과를 그림 5. 에 보인다. [12-13]

그림 5.의 (a)는 CCD 카메라에서 송신된 화상 데이터 이다. (b) 는 그림(a)의 히스토그램으로 색의 분포가 특정 값에 편중 되어 있는 것을 확인 할 수 있다. 그러나 그림 (c) 는 암호화 이후 화상 데이터로 육안으로 식별하기 어렵고 그림 (d) 의 히스토그램 또한 일정 분포를 가지고 있어 원본 데이터를 복원하기는 불가능한 것을 확인 할 수 있다.

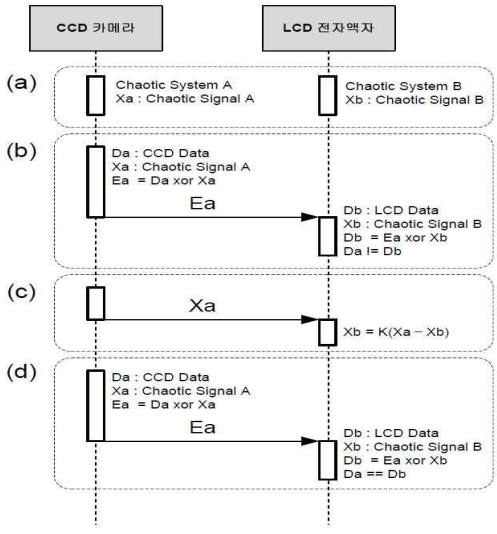

그림 4. 단방향 암호화의 순차 UML
Fig. 4. Sequence UML of Unidirectional Encryption

4. 암호화 방법의 성능평가

우리가 제시한 암호화 방법의 효율성을 육안이 아닌 수치적으로 평가하기 위해 원본데이터 그림 5. 의 (a) 와 암호화된 데이터 (b)의 상관계수를 측정 하였다. 상관계수는 식 (3) 을 이용하여 계산 하였다. [14]

$$\rho_{xy} = \frac{cov(r_x, r_y)}{\sigma_x \sigma_y} \quad \cdots\cdots (3)$$

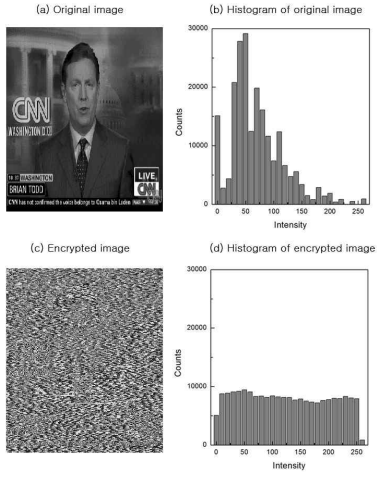

그림 5. 이미지 암호화 결과
Fig. 5. Result of Image Encryption

식 (3)에 나타낸 공분산 $cov(r_x,r_y)$ 과 표준편차 σ_x, σ_y 는 식 (4), 식 (5), 식 (6) 에 보인다.

$$Cov(r_x,r_y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y}) \quad \cdots\cdots (4)$$

$$\sigma_x=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2 \quad \cdots\cdots (5)$$

$$\sigma_y=\frac{1}{N}\sum_{i=1}^{N}(y_i-\bar{y})^2 \quad \cdots\cdots (6)$$

상관계수를 측정하기 위해 원본과 암호화된 데이터의 좌표를 무작위로 추출하고 그 좌표의 값을 x_n으로 정하고 그 값으로부터 가로, 세로 그리고 대각선 좌표의 값을 y_n으로 설정하고 계산을 수행 하였다.

표 1. 암호화된 이미지의 상관계수
Table 1. Correlation coefficient of encrypted Image

Direction of Adjacent pixels	Images	
	(a)	(b)
Horizontal	0.770	0.539
Vertical	0.922	0.001
Diagonal	0.741	0.003

계산을 수행 한 후 획득한 결과 값을 표 1. 에 보인다. 암호화된 데이터 (b)의 상관계수 값이 가로 값은 0.539 이고 세로 값은 0.001, 대각선은 0.003의 값을 나타내고 있다. 상관계수 값이 0.01 이하이면 근접한 두 값은 독립적이라고 판단 한다.

가로 값이 크게 나타난 이유는 Lorenz 혼돈계가 연속계라서 나타는 현상이다. 그러나 세로와 대각선은 0.01 이하의 값으로 암호화된 이미지에서 원본 이미지를 역으로 생성하기는 불가능 하게 된다. 결과 적으로 암호화가 효과적으로 이루어진 것을 확인 할 수 있다.

IV. 결 론

우리는 기존의 LCD 전자액자를 화상 디스플레이 장비에서 근거리 모니터링 장비로 활용 될 수 있는 방법을 연구 하였다.

근거리 모니터링 장비는 무엇 보다 송수신되는 화상 데이터의 보안이 중요하다. 이런 보안을 위해 기존의 양방향 암호화 방법을 대체 할 수 있는 단방향 암호화 방법을 연구 하게 되었다. 단방향 암호화 방법은 경제적인 면에서 효율적이지만 암호화 코드 송수신 시점을 일치시키기 어렵다는 문제점이 있다. 이러한 문제점을 해결하기 위해 혼돈계의 단방향 동기화 방법을 이용하였고, 그 결과를 컴퓨터 시뮬레이션을 통해 상용화 될 수 있는 장비로 개발 하였다. 이 방법은 특정 시간에 암호화 코드를 송수신 하는 방법이 아니라 송신되고 있는 암호화 코드를 일정시간동안 수신 하게 되면 동역학 적으로 두 시스템이 동기화가 되어 시점에 대한 문제점을 해결 할 수 있는 것이다.

본 논문에서는 이 방법을 감시용 전자액자에 적용 시키고, 그 결과를 보였지만, 보안이 중요시되는 Bluetooth 나 Zigbee 같은 근거리 유비쿼터스 통신에 적용하다면 경제적인 측면의 효과뿐만 아니라 많은 연구 성과도 얻을 수 있을 것으로 생각된다.

참고문헌

[1] J. S. Park, D. h. Kim, J. S. Park, J. G. Choi, S. H. Lee, "Implementation of a Multimedia frame service using UPnP," Conference of KIISE, Vol. 33, No. 2(A), pp. 253-256, 2006.

[2] J. W. Kim, Y. T. Joe, C. M. Park, H. G. Lee, I. B. Jung, "Implementation of the Digital Photo Frame based on Ubiquitous," Conference of KIISE, Vol. 33, No. 2(D), pp. 450-455, 2007.

[3] W. H, N. H, C. Park, D. Seo, I. Jung, "Design and Implementation of Network Adaptive Streaming Media Service for Digital Photo Frame," Conference of KIISE, Vol. 34, No. 2(D), pp. 477-481, 2007.

[4] J. S. Park, D. H. Kim, J. S. Park, S. H. Lee. J. K. Choi, "Design and Implementation of a Multimedia frame service using UPnP based on OSGi," Conference of KIISE, Vol. 33, No. 1(A), pp. 271-273, 2006.

[5] G. S. Yim, H. S. Kim, "Chaos-based Image Encrypt-ion Scheme using Noise-induced

Synchronization," Journal of the Korea Society of Computer and Information, Vol. 13, No. 5, pp. 155-162, 2008.

[6] G. S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System." Korea Information Assurance Society, Vol. 8, No. 3, pp.57-64, 2008.

[7] G. S. Yim, "Analysis of the Encoding Degree According to the Characteristics of Chaotic Signals." Korea Institute of Information Technology, Vol. 7, No. 6, pp. 167-171, Dec. 2009.

[8] List of Chaotic maps, *http://en.wikipedia.org/wiki /List_of_chaotic_maps*

[9] E. Ott, "Chaos in dynamical systems," Cambridge, pp. 57-59, 1993.

[10] T. Kapitaniak, "Controlling Chaos," Academic Press, pp.12-16, 1995.

[11] G. L. Parker, J. P. Gollub, "Chaotic Dynamics," Cambridge, pp.41-43, 1996.

[12] A. Stanoyevitch, "Introduction to numerical ordinary and partial differential equation using matlab," Wiley-Interscience, pp. 386-389, 2005.

[13] S. Lynch, "Dynamical systems with applications using matlab." Birkhauser, pp. 284-286, 2004.

[14] S. Behnia, A. Akhshani, S. Ahadpour, H.Mahmodi, A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," Physics Letters A, Vol. 366, pp.391-396, 2007.

저 자 소 개

김 홍 섭

2008 : 동국대학교 컴퓨터공학 박사.
현 재 : 오산대학 멀티미디어정보과 교수
관심분야 : 분산운영체제, 임베디드시스템, 유비쿼터스 컴퓨팅
Email : khs@osan.ac.kr

임 거 수

2004 : 배재대학교 물리학과 이학사.
2004 : 배재대학교 물리학과 이학석사.
2004 : 서강대학교 물리학과 이학박사.
현 재 : 배재대학교 과학기술학부 전임강사
관심분야 : 신호처리, 비선형 시계열 분석
Email : lomac@pcu.ac.kr