論文96-33B-11-4

물질전달함수를 이용한 영상 암호화 알고리즘

(An Encryption Algorithm of Images Using a Mass Transfer Function)

金 承 孫 *, 崔 炳 旭 *

(S. J. KIM and Byunguk CHOI)

요 약

본 논문에서는 물질전달함수(Mass Transfer Function: 이하 *MTF*)를 이용한 영상정보 보호 알고리즘을 제안한다. 제안한 암호화 알고리즘은 고인물에 떨어진 검은 잉크의 확산 현상을 영상 정보의 특성에 알맞게 수학적으로 해석하고, 해석된 결과를 암호화 함수(encryption function) 및 가중치 생성 함수(weight generation function)로 이용하여 정보를 보호한다. 즉, 영상정보의 암호화 과정을 일종의 물질전달현상이 발생했다고 보는 시각이다. 제안한 알고리즘의 시스템 구현으로 협대역 채널 통신에서 효율적인 정보 보호 서비스를 가능케 하고 중요한 정보의 전송에 있어서, 제 3자의 고의적인 교란이나 위협으로 부터 정보를 보호케 한다. 따라서, 개인 및 단체간에 안전한 정보의 유통을 가능케 한다.

Abstract

In this paper, we propose an encryption algorithm of image information using a mass transfer function(*MTF*). The algorithm is based on a diffusion phenomenon of black ink when black ink dropped in the stationary water. We mathematically analyze the phenomenon, in consideration of characteristics of image information, and apply the results of analysis to the security of image information. That is, we suppose that the security of image information is similar to a mass transfer phenomenon. The cryptosystem proposed in this paper enables the security services of information in narrow-band channel communication network to be provided. And in transmission of important information, it can secure against intentional disturbance and violation. Also, it can guarantee the safe flow of information.

Ⅰ. 서 론

영상 정보 보호에 대한 연구는 10년 이상 진행되어 많은 발전을 거듭해왔다. 초기에는 단순히 주사선 및 원영상 정보를 치환하거나 가산하는 형태의 암호화 방식이 제안되었고[1-4], 영상 정보의 방대성으로 인하여 처리 및 전송에 심한 오버헤드를 초래하면서 점차 압축을 고려한 암호화 방식이 제안되었다[5-7].

[1-4]에서 제안된 암호화 방식은 원영상의 계조값은 변화시키지 않고 위치 정보만을 혼합하여 원래의 화상을 알아 볼 수 없게 하는 방식이며, 혼합하는 단위에 따라 주사선 치환 방식, 주사선내 치환 방식, 주사선내 신호 절환 방식, 칼럼 치환 방식으로 나뉘어 진다. 그러나, [1-4]의 암호화 방식은 암호화 수행시 고속성을 유지하는 장점이 있지만, 다음과 같은 단점이 존재한다. 첫째, 치환된 영상은 원영상의 정보를 그대로 가지고 있기 때문에 히스토그램 정보를 이용하여 원영상을 추정할 수 있다. 둘째, 영상정보는 용장성(redundancy)이 크기 때문에 상관관계를 이용하여 해독

* 正會員, 漢陽大學校 電子通信工學科

(Dept. of Elec. Communications Eng., Hanyang Univ.)

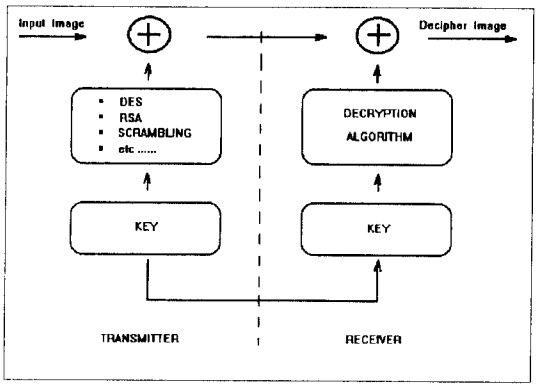
接受日子:1995年10月19日, 수정완료일:1996年11月11日

이 가능하다. 셋째, 치환된 영상은 계조값간의 상관관계가 없기 때문에 고주파 성분을 많이 포함하고 있어 DCT기반의 압축을 고려한 것에 적용하면 압축 효과가 거의 없다. [5]에서 제안된 암호화 방식은 영상 정보를 압축하면 자연발생적 혹은 인위적인 잡음에 대하여 민감한 반응을 보이기 때문에, 이러한 잡음 혹은 도청에 대처할 필요가 있다는 점을 감안한 오류정정 암호화 동시 부호화 방법이다. [6]에서 제안된 암호화 방식은 랜덤하게 발생된 SFC(Space Filling Curve)에 의하여 계조값을 재배열함으로써 위치 정보를 혼합하여 암호화 하는 것을 의미하는데, SFC의 특징은 인접 화소로만 위치 정보가 변하기 때문에 상관관계가 향상되어 DCT 기반의 압축방식에 적용하면 비월 주사의 방식보다 더 좋은 압축효과를 가져오지만, 이는 SFC를 취하는 영상의 크기가 비교적 클 경우에 해당되기 때문에 기본 블럭 단위로 처리를 하는 DCT 기반에서는 오히려 압축률 저하를 가져온다. [7]에서 제안된 암호화 방식은 위성을 통한 통신회의 프로토콜에서의 정보 보호를 다룬 암호 방식으로 DCT의 특성을 이용, 그 영상을 표현할 수 있는 정보의 대부분이 저주파 쪽으로 집중된다는 사실로 부터 주로 그 부분을 암호화하는 압축을 고려한 암호화 방식이다. 그러나, 기존의 영상 암호화 방식은 일반 텍스트(text) 및 음성 정보에 적용했던 암호화 방식을 단순히 결합한 형태로 영상정보에 이용되었기 때문에 영상 정보의 구조적인 특성과 용장성 및 압축율에 대해서 충분히 고려하지 않았다. 따라서, 다음과 같은 문제점이 존재한다.

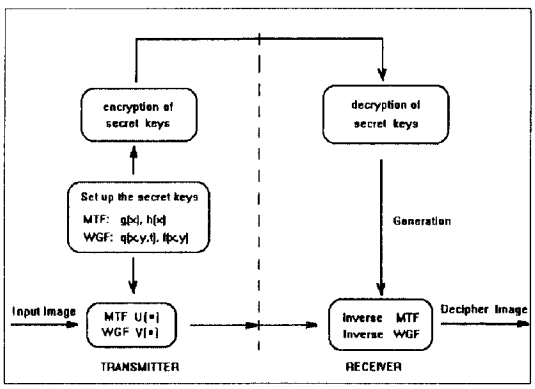
첫째, 영상 정보는 그 정보량이 방대하기 때문에 많은 계산량을 필요로 하는 암호화 방식에 적용이 어렵다. 즉, 빠른 암호화 처리를 요하는 영상 정보 전송에 지장을 초래한다. 둘째, 영상 정보는 용장성이 크기 때문에 암호 해독에 취약하다. 따라서, 정보의 기밀성을 유지하기 어렵고 정보의 가치가 크게 손상될 우려가 있다. 셋째, 영상 정보는 윤곽선 정보만으로도 전체 영상을 쉽게 파악할 수 있기 때문에 적은 정보의 해독이 의외로 많은 정보의 누출을 가져온다. 따라서, 동영상 전송에 있어서 효율적인 정보 보호를 위해서는 기존의 일반 텍스트 및 음성 정보에 적용했던 암호화 방식을 단순히 결합한 형태가 아닌 영상 정보의 구조적 해석과 자체의 특성을 고려하여 보다 빠르고 암호 강도가 높은 새로운 암호화 방식이 절실히 요구된다. 이러한 문제점을 해결하기 위해, 본 논문에서는 물질전달현상을 영상 정보의 특성에 알맞게 수학적으로 해석하고, 해석된 결과를 암호화 함수(encryption function) 및 가중치 생성 함수(weight generation function)로 이용하여 정보를 보호하는 암호화 알고리즘을 제안한다. 제안한 알고리즘의 암호화 함수 및 가중치 생성 함수는 상황에 적합한 미분방정식(differential equation)과 미분연산자(differential operator)를 정의하고 비밀키(secret key)의 역할을 하는 초기조건(Initial Condition: 이하 *IC*) 및 경계조건(Boundary Conditions: 이하 *BCs*)을 설정하고 미분방정식의 해(solution)를 구하여 얻는다. 한편, 기존의 영상 암호화 방식은 암호화 수행 단위가 주사선 혹은 블럭 단위, 즉 화소의 위치 정보에 대하여 암호화를 수행하는 것에 비하여, 제안한 암호화 방식은 화소 단위의 암호화를 수행한다. 따라서, 원영상의 계조값을 암호화 하는 방식이므로 암호 강도의 효율성을 향상시키며, 암호화에 쓰이는 비밀키는 임의의 함수로 표현되므로 비밀키의 전송이 용이하여 처리 및 전송에 지장을 초래하지 않는다.

영상 정보의 암호화는 압축률, 암호 강도, 처리 시간 사이의 trade-off인 관계가 있으며 암호 강도와 압축률과의 관계는 암호 강도가 크려면 이웃하는 화소들끼리의 상관도 및 화면과 화면사이의 용장성을 충분히 작게 해야한다. 그러나, 상관성을 작게하면 압축률 관점에서는 압축 효과가 거의 없다. 이는 한정된 대역폭에 많은 양의 영상 정보를 전송하려면 심한 오우버헤드를 초래하게 되며, 결국 영상 정보의 실시간 처리가 불가능 하게 된다. 암호 강도와 처리 시간과의 관계는 다음과 같다. 예를 들면 스크램블 방식은 처리 시간이 굉장히 빠르지만 암호화 강도가 약하다는 단점이 존재하고 RSA 방식은 암호 강도는 상당히 크지만 암호화 및 복호화 처리에 많은 시간이 걸림을 알 수 있다. 본 논문에서는 암호 강도, 압축률, 처리 시간에 대하여 이 모두를 적절히 만족할 수 있는 암호화 방식을 제안하였다. 즉, 암호 강도의 측면에서는 암호화의 수행 단위가 화소의 위치를 변경하지 않고 화소값을 변경하기 때문에 기존의 스크램블링 방식에 비하여 높은 암호 강도를 유지할 수 있고 압축률 측면에서는 화소의 위치를 변경하지 않기 때문에 이웃하는 화소들 끼리의 상관도를 유지할 수 있어 DCT 기반의 영상 전송 시스템에서 효율적이다. 처리 시간의 관점에서는 제안한 암호화 방식의 암호화 진행은 동심원의 형태로 수행되기 때문에 병렬처리가 가능하며 H/W 구성시 Transputer

및 Hypercube 등을 이용하면 빠른 처리 시간을 유지한다.



(a) 기존의 암호화 방식



(b) 제안한 암호화 방식

그림 1. 기존의 암호화 방식과 제안한 암호화 방식의 블럭 다이어그램

Fig. 1. Block diagram of the existing and proposed encryption method.

제안한 암호화 알고리즘은 영상 정보를 2차원 평면상의 좌표로 가정하고 임의의 암호화 시작 화소가 주어지면 암호화 하고자 하는 범위까지 동심원의 형태로 물질전달현상이 발생하며, 암호화 함수 및 가중치 생성 함수에 의하여 주어진 범위내에 존재하는 모든 화소를 암호화 한다. 그림 1은 기존의 암호화 방식과 제안한 암호화 방식을 비교한 것으로 기존의 암호화 방식은 이미 정해진 비밀키와 암호화 함수를 이용하여 암호화가 수행된다. 반면에, 본 논문에서 제안한 암호화 방식은 암호화 함수 U(•) 및 가중치 함수 V(•)를 생성하기 위해 먼저, 비밀키들을 설정하고 설정된 비밀키에 의하여 각각의 함수들을 생성한다. 다음에는 생성된 암호화 함수 및 가중치 함수를 이용하여 입력 영상을 암호화 한다. 한편, 비밀키의 전송은 RSA 암호화 방식으로 수신측으로 전송하며, 수신측은 전송되어 온 비밀키를 복호화 한다. 복호화 된 비밀키를 이용하여 암호화 역함수 및 가중치 역함수를 생성하고 전송되어 온 암호화된 영상을 복원한다.

II. 물질전달함수를 이용한 암호화 알고리즘

물질전달현상은 우리 주변에서 흔히 볼 수 있다. 예를 들면, 커피용액속의 설탕이 용해되는 상태, 향수의 향이 공기중에 확산되는 상태, 고인물에 떨어진 검은 잉크가 확산되는 상태 등 자연계에 존재하는 거의 모든 현상들이 일종의 물질전달현상에 의하여 발생한다[18]. 본 논문에서는 고인물에 떨어진 검은 잉크의 확산현상을 영상 정보의 암호화에 응용한다.

일반적으로 물질전달현상은 편미분방정식(Partial Differential Equation: 이하 *PDE*)으로 표현되며, 주어진 상황에 적합한 미분방정식을 설정하고 적절한 *IC*과 *BCs*을 이용하여 미분방정식의 정확한 해를 얻으면 전달현상을 해석할 수 있다[9-17]. 그러나, 자연계에 존재하는 물질전달현상은 일반적으로 비선형성(Nonlinearity)을 띄고 있기 때문에 모든 상황을 고려하면 전달현상을 해석하기란 거의 불가능하다. 따라서, 물질전달현상을 영상 정보의 암호화에 응용하기 위해서는 상황에 적합한 선형성(Linearity)을 갖는 함수로 모델링(Modeling)하는 것이 필요하다. 즉, 영상 정보내에서 발생하는 물질전달현상은 좌우(Left & Right Direction) 및 전후(Forward & Backward Direction)로만 발생하며 외부 영향은 무시하는 가정이 필요하다. 이를 위해서는, 물질전달현상이 발생하는 영역에 대한 설정과 물질전달함수를 선형화 하기 위한 미분연산자를 정의해야 한다.

본 논문에서는 영상 정보의 암호화에 적합한 미분방정식을 설정하기 위해 라플라시안 미분연산자(Laplacian Differential Operator: 이하 *LDO*)를 정의한다. *IC*는 초기 상태를 의미하며 "0"으로 설정하고 *BCs*는 물질전달현상이 발생하는 영역을 의미하며 비밀키 $g(x), h(x)$로 설정한다. 설정된 조건들을 이용하여 미분방정식의 해를 구하고 얻어진 해에 대하여 시간을 의미하는 변수 t대신 가중치 생성 함수(Weight Generation Function: 이하 *WGF*)에 의해 생성된 가

중치를 변수로 하여 최종적으로 영상 정보를 암호화하는 암호화 함수가 얻어진다. 한편, *WGF*는 비밀키 $q(x,y,t)$와 *LDO*의 합으로 미분방정식을 설정한다. $q(x,y,t)$는 영상 정보의 암호화시 쓰이는 검은 잉크의 양을 기술한다. *IC*는 가중치가 생성되기 이전 상태를 의미하며 비밀키 $f(x,y)$로 설정하고 *BCs*는 "0"으로 설정한다. *MTF*는 위치와 가중치의 함수이며, 영상정보 내에서 위치에 따른 검은 잉크의 확산 현상을 기술하고 *WGF*는 위치에 따라 확산되는 검은 잉크의 양을 기술한다.

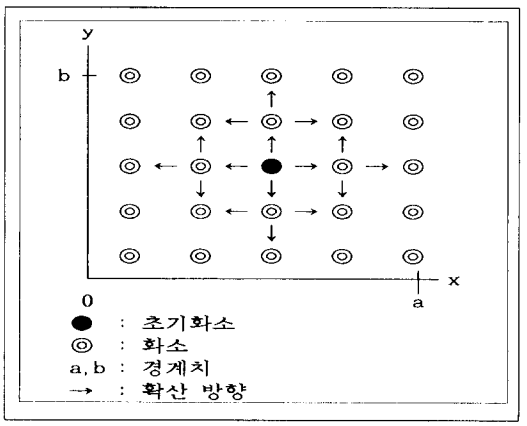


그림 2. 암호화 진행도
Fig. 2. The processing diagram of encryption.

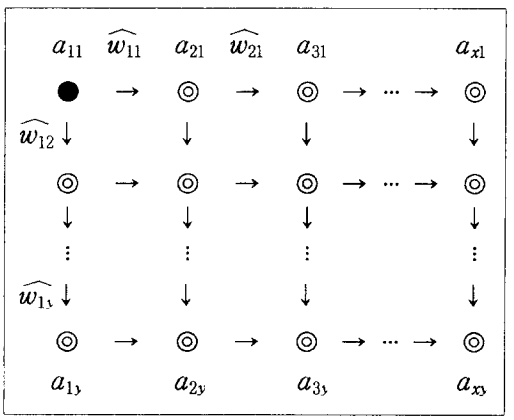


그림 3. 부분적인 암호화 진행도
Fig. 3. The processing diagram of partial encryption

1. 암호화

그림 2는 제안한 암호화 알고리즘의 진행도를 보이고 있으며 ●가 암호화 시작 화소이다. 암호화 진행은 시작 화소, 시작 화소와 연결된 가중치를 변수로 갖는 암호화 함수 $U(\cdot)$에 의하여 각 방향으로 확산되며 암호화가 진행된다. 가중치의 생성은 시작 화소, 이미 암호화된 화소값을 변수로 갖는 가중치 생성 함수 $V(\cdot)$에 의하여 생성된다[18-19].

그림 3에서 a_{xy}는 원화소를 의미하고 $\widehat{w_{xy}}$는 생성된 가중치를 각각 의미한다. 화소의 암호화는 *MTF* $U(\cdot)$에 의하여 진행되며 식(1)과 같다. 식(1)에서 $U(\cdot)$는 *MTF* 즉, 암호화 함수를 의미하고, $\widehat{a_{xy}}$는 암호화된 화소, $\widehat{w_{xy}}$는 생성된 가중치를 각각 의미한다. 암호화 함수의 생성은 다음과 같다.

$$\widehat{a_{xy}} = U(x, y, \widehat{w_{xy}}), \quad \widehat{w_{xy}} = V(x, y, a_{xy}) \tag{1}$$

2. 암호화 함수의 생성

본 논문에서 제안한 암호화 함수 $U(\cdot)$는 식(2)와 같이 편미분방정식을 설정하고 설정된 미분방정식의 해를 얻기 위해 식(3) 및 식(4)와 같이 *IC* 및 *BCs*을 설정하여 생성한다.

$$PDE: \frac{\partial u}{\partial t} = k\nabla^2 u \tag{2}$$

$$\begin{aligned} BCs: \; & u(x,0,t) = g(x) \\ & u(x,b,t) = h(x) \\ & u(0,y,t) = 0 \\ & u(a,y,t) = 0 \end{aligned} \tag{3}$$

$$IC: \quad u(x,y,0) = 0 \tag{4}$$

식(2)~(4)에서 x, y, t의 범위는 각각 $0<x<a$, $0<y<b$ 및 $t>0$ 이며 식(2)에서 ∇^2는 물질전달현상을 선형화하기 위한 미분연산자의 역할을 하며 2D-*LDO*이다. 식(3)은 암호화 범위를 의미하는 경계조건으로서 그림 4와 같이 사각형의 각 변에 해당 한다. 즉, $y=0$일 때 $0<x<a$인 구간에 대해서는 $g(x)$, $y=b$일 때 $h(x)$로 설정하고 $x=0$일 때 $0<y<b$인 구간에 대해서는 0, $x=a$일 때 $0<y<b$인 구간에 대해서는 0으로 각각 설정하면 그림 4와 같이 경계조건들이 사각형 형태로 표현된다. 이는, 암호화 범위를 결정하는 데 있어서 중요한 요소로 작용할 뿐만아니라 미분방정식의 해, 즉 암호화 함수를 경계조건으로 둘러싸인 내부에서 정의하고자 함이다.

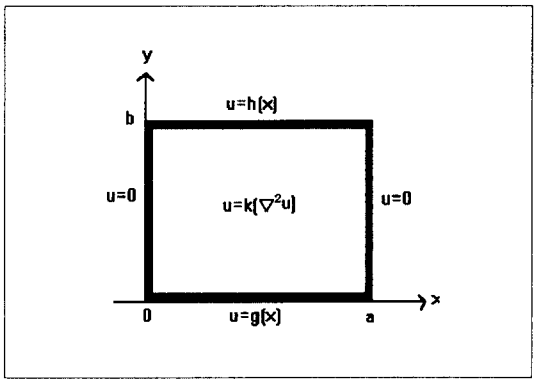


그림 4. *BCs*의 기하학적인 의미
Fig. 4. Geometric analysis of *BCs*

설정된 *BCs*와 *IC*를 이용해 주어진 미분방정식의 해, $u(x,y,t)$를 구하는 과정은 다음과 같다. 먼저, y를 고정 변수(fixed parameter)라 하고 식(2)의 해 $u(x,y,t)$를 주어진 구간 $0\le x\le a$에서 1계 및 2계 미분(first & second derivatives)은 연속(continuous)이라고 가정하자. 그러면, 주어진 구간의 끝에서 $u(x,y,t)$는 0이기 때문에 uniform convergence theorem[20]에 따라 $u(x,y,t)$는 식(5)와 같이 Dicrete Fourier Sine Series로 표현된다. 식(5)에서, summation하는 구간을 a까지 취한 이유는 a가 정수이기 때문이며 $u_m(y,t)$는 식(6)과 같이 표현된다.

$$u(x,y,t)=\sum_{m=1}^{a} u_m(y,t)\sin(\frac{m\pi x}{a}) \tag{5}$$

$$u_m(y,t)=\frac{2}{a}\int_0^a u(x,y,t)\sin(\frac{m\pi x}{a})dx \tag{6}$$

미지 계수(unknown coefficients) $u_m(y,t)$를 구하기 위해서는 식(6)을 t에 관해 미분하면 얻을 수 있고 식(7)과 같이 표현된다. 식(7)의 우변에 있는 두 항을 x에 관해 적분하면 각각 식(8), (9)를 얻을 수 있으며, 이를 이용해 식(7)을 다시 표현하면 식(10)은 식(7)과 서로 equivalent함을 알 수 있다.

$$\begin{aligned}\frac{\partial u_m}{\partial t}&=\frac{2}{a}\int_0^a k\nabla^2 u\ \sin(\frac{m\pi x}{a})dx\\&=\frac{2}{a}\int_0^a k(\frac{\partial^2 u}{\partial x^2}+\frac{\partial^2 u}{\partial y^2})\ \sin(\frac{m\pi x}{a})dx\\&=\frac{2}{a}\int_0^a k(u_{xx}+u_{yy})\ \sin(\frac{m\pi x}{a})dx\end{aligned} \tag{7}$$

$$k\frac{2}{a}\int_0^a u_{yy}\sin(\frac{m\pi x}{a})dx=k\frac{\partial^2 u_m}{\partial y^2}, \tag{8}$$

$$k\frac{2}{a}\int_0^a u_{xx}\sin(\frac{m\pi x}{a})dx=-(\frac{m\pi}{a})^2\ ku_m \tag{9}$$

$$\frac{\partial u_m}{\partial t}=k\left(\frac{\partial^2 u_m}{\partial y^2}-(\frac{m\pi}{a})^2\ u_m\right) \tag{10}$$

한편, 식(6)에서 $y\to 0$라 놓으면 식(3)의 *BCs*을 이용해서 식(11)과 같이 $u_m(0,t)$를 얻을 수 있고 $y\to b$라 놓으면 식(12)와 같이 $u_m(b,t)$를 얻을 수 있다. $u_m(y,0)$을 구하려면 식(6)에 *IC*을 적용하여 $t\to 0$으로 놓고 식(4)의 *IC*을 적용하면 식(13)과 같이 $u_m(y,0)$를 얻는다.

$$u_m(0,t)=\frac{2}{a}\int_0^a g(x)\ \sin(\frac{m\pi x}{a})dx=g_m \tag{11}$$

$$u_m(b,t)=\frac{2}{a}\int_0^a h(x)\ \sin(\frac{m\pi x}{a})dx=h_m \tag{12}$$

$$u_m(y,0)=0 \tag{13}$$

여기에서, 식(10)~(13)은 최초에 설정한 미분방정식과 *IC* 및 *BCs* 모두를 만족한다. 따라서, 식(10)~(13)을 이용하여 식(14)~(16)과 같이 표현되는 미분방정식과 *IC* 및 *BCs*을 설정할 수 있고 설정된 조건들을 이용하여 식(10)의 미분방정식의 해를 얻으면 미지 계수 $u_m(y,t)$를 결정할 수 있다. 식(14)~(16)에서 y,t의 범위는 각각 $0<y<b,\ t>0$이다.

$$PDE:\ \frac{\partial u_m}{\partial t}=k\left(\frac{\partial^2 u_m}{\partial y^2}-(\frac{m\pi}{a})^2\ u_m\right) \tag{14}$$

$$BCs:\ u_m(0,t)=g_m\ ,\ \ u_m(b,t)=h_m \tag{15}$$

$$IC:\quad u_m(y,0)=0 \tag{16}$$

식(14)의 해는 식(17)과 같이 정상상태(steady-state)의 해와 천이상태(transient-state)의 해의 합으로 표현되며, 그림 5와 같은 기하학적인 의미를 갖는다. 즉, 정상상태의 해는 *BCs* $g(x)$와 $h(x)$ 사이에서 정의되는 해를 의미하고 천이상태의 해는 *IC*을 만족하는 해를 의미한다. 식(17)에서 w_m과 v_m은 각각 식(18)~(19) 및 식(20)~(22)를 만족한다.

$$u_m(y,t)=w_m(y)+v_m(y,t) \tag{17}$$

$$DE:\ \frac{d^2 w_m}{dy^2}-(\frac{m\pi}{a})^2\ w_m=0 \tag{18}$$

$$BCs:\ w_m(0)=g_m,\quad w_m(b)=h_m \tag{19}$$

$$PDE:\ \frac{\partial v_m}{\partial t} = k\left(\frac{\partial^2 v_m}{\partial y^2} - \left(\frac{m\pi}{a}\right)^2 v_m\right) \tag{20}$$

$$BCs:\ v_m(0,t)=0,\quad v_m(b,t)=0 \tag{21}$$

$$IC:\ v_m(y,0)=-w_m(y) \tag{22}$$

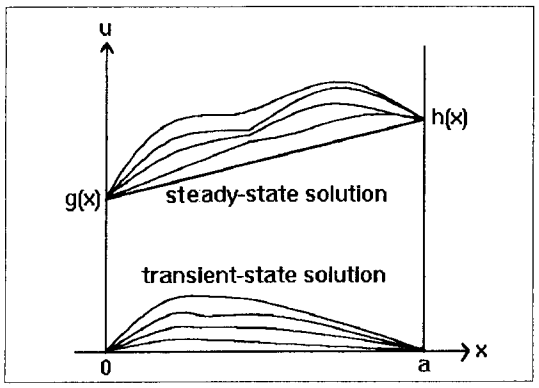


그림 5. 정상상태와 천이상태 해의 기하학적인 해석
Fig. 5. Geometric analysis of steady-state and transient-state solution

식(18)은 상미분방정식(ordinary differential equation)이기 때문에 식(23)과 같이 쉽게 해를 구할 수 있고 식(20)의 해는 식(24)와 같이 Fourier sine series의 형태로 표현된다. 식(24)에서 $\lambda_{m,n}$은 고유값(eigenvalues)을 의미한다.

$$w_m(y) = g_m\frac{\sinh\left(\frac{m\pi(b-y)}{a}\right)}{\sinh\left(\frac{m\pi b}{a}\right)} + h_m\frac{\sinh\left(\frac{m\pi y}{a}\right)}{\sinh\left(\frac{m\pi b}{a}\right)} \tag{23}$$

$$v_m(y,t) = \sum_{n=1}^{b} C_{m,n} e^{-\lambda_{m,n} kt}\sin\left(\frac{n\pi y}{b}\right) \tag{24}$$

$$\lambda_{m,n} = \left(\frac{m^2}{a^2} + \frac{n^2}{b^2}\right)\pi \tag{25}$$

$$C_{m,n} = -\frac{2}{b}\int_0^b w_m(y)\sin\left(\frac{n\pi y}{b}\right)dy$$

$$= \frac{2n\pi}{b^2\lambda_{m,n}}\left(g_m - (-1)^n h_m\right) \tag{26}$$

최종적으로 식(2)를 만족하는 해는 식(27)과 같이 얻어지며 식(27)에서 시간을 나타내는 변수 t대신 가중치 생성 함수에 의해 생성된 가중치로 대치하면 암호화 함수(MTF)가 얻어진다.

$$u(x,y,t)$$

$$= \sum_{m=1}^{a} w_m(y)\sin\left(\frac{m\pi x}{a}\right) + \sum_{m=1}^{a} v_m(y,t)\sin\left(\frac{m\pi x}{a}\right)$$

$$= \sum_{m=1}^{a} g_m\frac{\sinh\left(\frac{m\pi(b-y)}{a}\right)}{\sinh\left(\frac{m\pi b}{a}\right)}\sin\left(\frac{m\pi x}{a}\right) +$$

$$\sum_{m=1}^{a} h_m\frac{\sinh\left(\frac{m\pi y}{a}\right)}{\sinh\left(\frac{m\pi b}{a}\right)}\sin\left(\frac{m\pi x}{a}\right) +$$

$$\sum_{m=1}^{a}\sum_{n=1}^{b}\frac{2n\pi}{b^2\lambda_{m,n}}\left(g_m-(-1)^n h_m\right)\times$$

$$e^{-\lambda_{m,n}kt}\sin\left(\frac{m\pi x}{a}\right)\sin\left(\frac{n\pi y}{b}\right). \tag{27}$$

3. 가중치 생성 함수의 생성

가중치 생성 함수 $V(\cdot)$는 위치와 시간에 따라 확산되는 검은 잉크의 양을 기술하며 식(28)과 같이 생성된다. $V(\cdot)$는 가중치 생성 함수, $\widehat{w_{xy}}$은 생성된 가중치를 각각 의미하며 암호화 함수 $U(\cdot)$에 의하여 화소의 암호화가 진행되는 동안, 병행하여 가중치 생성 함수 $V(\cdot)$에 의하여 자체적으로 가중치를 생성함을 알 수 있다. 따라서 보다 높은 암호화 강도를 유지하게 한다.

$$\widehat{w_{xy}} = V(x, y, a_{xy}) \tag{28}$$

가중치 생성 함수 $V(\cdot)$는 식(29)와 같은 편미분방정식을 설정하고 식(30), (31)과 같은 BCs 및 IC를 설정하여 생성한다. 여기에서, x, y, t의 범위는 암호화 함수의 생성시와 각각 같다.

$$PDE:\ v_t = k\nabla^2 v + q(x,y,t) \tag{29}$$

$$BCs:\quad v(x,0,t)=0,\quad v(x,b,t)=0,\quad v(0,y,t)=0,\quad v(a,y,t)=0 \tag{30}$$

$$IC:\quad v(x,y,0)=f(x,y) \tag{31}$$

식(29)에서 $q(x,y,t)$는 확산이 진행되는 동안 검은 잉크의 양을 기술하고 식(31)의 $f(x,y)$는 IC를 의미하며 이들은 모두 비밀키로서 이용된다. 식(29)의 해를 $v(x,y,t)$라고 가정하면, $v(x,y,t)$는 식(32)와 같이 고유값과 고유함수 $\phi_{m,n}=\sin\left(\frac{m\pi x}{a}\right)\sin\left(\frac{n\pi y}{b}\right)$로서 표현된다.

$$v(x,y,t)=\sum_{m=1}^{a}\sum_{n=1}^{b} B_{m,n}(t)\ \phi_{m,n}(x,y) \tag{32}$$

$$B_{m,n}(t)=\frac{4}{ab}\int_0^b\int_0^a v(x,y,t)\ \phi_{m,n}(x,y)\,dxdy \tag{33}$$

식 (32)에서 미지 계수(unknown coefficients) $B_{m,n}(t)$를 구하기 위해서는 식(33)을 t에 관해 미분하면 식(34)와 같이 얻을 수 있고 식(34)에서 우측의 두 번째 항을 $Q_{m,n}(t)$라 하고 우측의 첫번째 항을 x와 y에 관해 적분하면 식(36)과 같이 표현된다.

$$\frac{dB_{m,n}}{dt}=\frac{4}{ab}\int_0^b\int_0^a\frac{\partial v}{\partial t}\phi_{m,n}\,dxdy$$

$$=\frac{4}{ab}\int_0^b\int_0^a k(\nabla^2 v)\phi_{m,n}\,dxdy+$$

$$\frac{4}{ab}\int_0^b\int_0^a q\phi_{m,n}\,dxdy \tag{34}$$

$$Q_{m,n}(t)=\frac{4}{ab}\int_0^b\int_0^a q(x,y,t)\ \phi_{m,n}(x,y)\,dxdy \tag{35}$$

$$\frac{4}{ab}\int_0^b\int_0^a k(\nabla^2 v)\phi_{m,n}\,dxdy=-\lambda_{m,n}k\frac{4}{ab}\int_0^b\int_0^a v\phi_{m,n}\,dxdy \tag{36}$$

식(36)의 좌변은 Green's formula에 의해서 $\nabla^2\phi_{m,n}$이 $-\lambda_{m,n}\phi_{m,n}$으로 변환되었음을 알 수 있고 식(36)의 우변을 $B_{m,n}(t)$로 표현하면 식(37)과 같다. 따라서, 위의 결과를 종합하면 식(34)는 식(38)과 같이 표현된다.

$$\frac{4}{ab}\int_0^b\int_0^a k(\nabla^2 v)\phi_{m,n}\,dxdy=-\lambda_{m,n}kB_{m,n}(t) \tag{37}$$

$$\frac{dB_{m,n}}{dt}=-\lambda_{m,n}kB_{m,n}(t)+Q_{m,n}(t) \tag{38}$$

식(38)에서 $Q_{m,n}(t)$는 알려진 함수이고 $B_{m,n}(t)$는 미지 함수이기 때문에 주어진 BCs와 IC를 이용해 $B_{m,n}(t)$를 구하면 식(29)의 해를 구할 수 있다. 즉, 식(33)에서 t를 0으로 놓고 식(31)의 IC을 적용하면, $B_{m,n}(t)$는 식(39)와 식(40)과 같이 표현된다. 이를 이용해 식(38)의 양변을 t에 관하여 적분하면 식(41), (42)와 같다.

$$B_{m,n}(0)=A_{m,n} \tag{39}$$

$$A_{m,n}=\frac{4}{ab}\int_0^b\int_0^a f(x,y)\phi_{m,n}(x,y)\,dxdy \tag{40}$$

$$B_{m,n}(t)=A_{m,n}e^{-\lambda_{m,n}kt}+C_{m,n}(t) \tag{41}$$

$$C_{m,n}(t)=\int_0^t e^{-\lambda_{m,n}k(t-\tau)}Q_{m,n}(\tau)\,d\tau \tag{42}$$

최종적인 해 $v(x,y,t)$는 식(43)과 같이 식(41)의 결과를 $B_{m,n}(t)$로 대치하면 얻을 수 있으며, 이렇게 얻어진 해에 대하여 시간을 나타내는 변수 t대신 암호화하고자 하는 화소값으로 대치하면 위치에 따라 확산되는 검은 잉크의 양을 기술하는 가중치 생성 함수가 식(44)와 같이 얻어진다. 이상에서 언급한 암호화 함수 및 가중치 생성 함수에 의하여 암호화되는 전체적인 과정의 수식적인 해석은 식(45)와 같다.

$$V(x,y,t)=B_{m,n}(t)\phi_{m,n}(x,y)$$

$$=\sum_{m=1}^{a}\sum_{n=1}^{b}\{A_{m,n}e^{-\lambda_{m,n}kt}+C_{m,n}(t)\}\phi_{m,n}(x,y) \tag{43}$$

$$\widehat{w_{xy}}=V(x,y,a_{xy})$$

$$=\sum_{m=1}^{a}\sum_{n=1}^{b}\{A_{m,n}e^{-\lambda_{m,n}ka_{xy}}+C_{m,n}(a_{xy})\}\phi_{m,n}(x,y) \tag{44}$$

$$\widehat{a_{xy}} = U(x,y,V(x,y,a_{xy})) \tag{45}$$

본 논문에서 제안한 암호화 알고리즘의 비밀키는 가중치 생성 함수의 생성을 위해 쓰이는 $q(x,y,t)$, $f(x,y)$와 암호화 함수를 생성하기 위해 쓰이는 $g(x)$, $h(x)$이며 각각의 비밀키에 대한 key space는 다음과 같다.

먼저, $g(x)$, $h(x)$는 상수를 포함하여 임의의 모든 함수로 설정할 수 있으나, x에 따라 $0\le g(x),h(x)\le 255$인 범위내에 존재해야 한다. 왜냐하면, 암호화 함수의 해는 영상 정보의 계조값 표현 범위인 0부터 255 사이에서 존재해야만 하기 때문이다. 다음에는 $q(x,y,t)$를 살펴 보면, $q(x,y,t)$는 확산이 진행되는 동안 검은 잉크의 양을 기술하며 경계조건과 마찬가지로 $0\le q(x,y,t)\le 255$인 범위에 존재해야 하며 초기값을 의미하는 $f(x,y)$도 $q(x,y,t)$와 같은 범위내에 존재해야 한다. 따라서, 암호화 함수 및 가중치 함수의 생성에 필요한 비밀키의 key space는 x,y 및 t에 따라 0부터 255사이의 값으로 표현되는 모든 함수 공간으로 생각할 수 있다.

비밀키의 전송은 메시지의 인증 및 디지틀 서명이 가능하며, 안전성 측면에서도 그 우수성이 널리 인정된 RSA 공개키 암호 방식으로 암호화 하여 수신측에 전송한다. 수신측은 송신측으로 부터 전송되어온 암호화된 영상과 비밀키로 다음과 같이 복호화 한다.

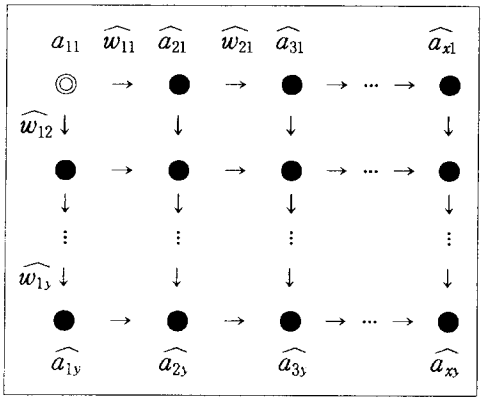


그림 6. 부분적인 복호화 진행도
Fig. 6. The processing diagram of partial decryption

4. 복호화

그림 6에서 $\widehat{a_{xy}}$는 암호화된 화소를 의미하고 $\widehat{w_{xy}}$은 가중치 생성 함수의 역함수에 의해서 생성된 가중치를 의미한다. 복호화 과정의 수식적인 해석은 식(46), (47)과 같으며, 구체적인 설명은 다음과 같다. 먼저, 식(46)과 같이 암호화 함수의 역함수 $U^{-1}(\cdot)$를 이용하여 가중치를 복호하고 복호된 가중치로 식(47)과 같이 가중치 생성 함수의 역함수 $V^{-1}(\cdot)$에 의하여 원화소를 복호화 한다.

$$\widehat{w_{xy}} = U^{-1}(\ x,\ y,\ \widehat{a_{xy}}\ ) \tag{46}$$

$$a_{xy} = V^{-1}(\ x,\ y,\ \widehat{w_{xy}}\ ) \tag{47}$$

5. 암호화 역함수 $U^{-1}(\cdot)$의 생성

가중치의 복호화는 암호화 역함수에 의하여 수행된다. 암호화 역함수의 생성은 전송되어 온 비밀키 $g(x), h(x)$를 이용하여 생성한다. 먼저, 식(27)의 암호화 함수에서 $\widehat{a_{xy}}$은 다음과 같이 $u(x,y,t)=u(x,y,\widehat{w_{xy}})$으로 표현되므로 복호화 과정은 식(48)과 같이 표현된다.

$$\widehat{a_{xy}} = u(x,y,t) = u(x,y,\widehat{w_{xy}}) \tag{48}$$

식(48)에서 $\widehat{a_{xy}}$는 식(27)의 결과를 이용하여 얻는다. 먼저, 식(27)의 우변 첫째항과 둘째항을 좌변으로 이항하면 식(49)과 같고 $P(x,y)$, $p(m,n)$은 각각 식(50), (51)과 같이 표현된다.

$$\widehat{a_{xy}} - u(x,y,\widehat{w_{xy}}) = P(x,y) \tag{49}$$

$$P(x,y) = \sum_{m=1}^{a}\sum_{n=1}^{b} p(m,n)\ \sin(\frac{m\pi x}{a})\sin(\frac{n\pi y}{b}) \tag{50}$$

$$p(m,n) = \frac{2n\pi}{b^2\lambda_{m,n}}(g_m-(-1)^n h_m)\ e^{-\lambda_{m,n}k\widehat{w_{xy}}} \tag{51}$$

식(50)은 직교(orthogonal) 특성을 만족하므로 역변환을 수행하여 $p(m,n)$을 구하고 $p(m,n)$과 식(51)을 같게 놓으면 식(52)와 같이 가중치 $\widehat{w_{xy}}$를 복호화 할 수 있다.

$$\widehat{w_{xy}} = -\frac{1}{k}\ \ln\frac{b^2}{2n\pi(g_m-(-1)^n h_m)} \times \left(\sum_{x=1}^{a}\sum_{y=1}^{b} \alpha P(x,y)\ \sin(\frac{m\pi x}{a})\sin(\frac{n\pi y}{b})\right) \tag{52}$$

6. 가중치 생성 함수의 역함수 $V^{-1}(\cdot)$의 생성

가중치 생성 함수의 역함수의 생성은 전송되어 온 비밀키 $f(x,y)$, $q(x,y,t)$와 복호된 가중치를 이용하여 생성한다. 즉, 식(32)의 가중치 생성 함수는 식(53)과 같이 표현되므로 암호화 역함수에 의해 복호된 가중치 $\widehat{w_{xy}}$을 이용하여 원영상 정보 a_{xy}를 구한다.

$$\widehat{w_{xy}} = v(x,y,a_{xy}) = \sum_{m=1}^{a}\sum_{n=1}^{b} B_{m,n}(a_{xy})\ \phi_{m,n}(x,y) \tag{53}$$

$$B_{m,n}(0) = A_{m,n} \tag{54}$$

$$A_{m,n} = \frac{4}{ab}\int_0^b\int_0^a f(x,y)\phi_{m,n}(x,y)\,dxdy \tag{55}$$

$$B_{m,n}(a_{mn}) = A_{m,n}e^{-\lambda_{m,n}ka_{xy}} + C_{m,n}(a_{mn}) \tag{56}$$

$$C_{m,n}(a_{mn}) = \int_0^{a_{mn}} e^{-\lambda_{m,n}k(a_{xy}-\tau)}\,Q_{m,n}(\tau)\,d\tau \tag{57}$$

$$Q_{m,n}(t) = \frac{4}{ab}\int_0^b\int_0^a q(x,y,t)\ \phi_{m,n}(x,y)\,dxdy \tag{58}$$

먼저, 식(53)에서 $B_{m,n}(a_{xy})$는 식(54)~(58)로 표현되므로 식(58)에서 비밀키 $q(x,y,t)$를 이용하여 $Q_{m,n}(t)$를 구한 후 식(57)을 이용해 $C_{m,n}(a_{xy})$를 구한다. 또한 식(55)에서 비밀키 $f(x,y)$을 이용해 $A_{m,n}$을 구한 후 이미 구해진 결과들을 식(56)에 적용하여 $B_{m,n}(a_{xy})$를 구한다. 한편, $\widehat{w_{xy}}$은 이미 복호화된 가중치 이므로 식(53)의 우변에 $B_{m,n}(a_{xy})$를 적용하여 최종적으로 a_{xy}를 복호화 한다. 전체적인 복호화 알고리즘의 수식적인 해석은 식(59)와 같다.

$$a_{xy} = V^{-1}(\ x,\ y,\ U^{-1}(\ x,\ y,\ \widehat{a_{xy}}\ )) \tag{59}$$

Ⅲ. 실험 및 고찰

본 논문에서 제안한 암호화 알고리즘의 성능 평가를 위하여 입력 영상으로 256×256 "Lena", "Girl", "Miss America" 영상을 이용하였다. 그림 7~9는 각각의 입력 영상에 대하여 제안한 물질전달함수, 즉 암호화 함수 및 가중치 생성 함수에 의하여 암호화 범위를 각각 60, 120, 180, 230으로 가변했을 경우 암호화된 결과 영상을 보이고 있다.

실험 결과에서 그림 7~9와 그림 10의 암호화 된 영상이 다른 패턴을 보이는 이유는 암호화 함수 및 가중치 함수의 생성에 쓰이는 비밀키들을 다르게 설정하였기 때문이다. 이는 설정된 비밀키에 따라 암호화 함수가 달라지기 때문에 결과 영상에서 다른 패턴이 나타난다.

본 논문에서는 암호화 함수의 생성시 비밀키로 쓰이는 경계조건 $g(x)$와 $h(x)$는 식(60), (61)과 같이 DST(Discrete Sine Transform) 기저함수(basis function)의 커널의 첫번째 row 성분을 $g(x)$, 마지막 row 성분을 $h(x)$로 이용하였다. 식(60)에서 a는 암호화가 수행되는 범위를 의미하고 k가 1일 때를 $g(x)$, k가 a일 때를 $h(x)$로 각각 설정하였다.

$$\Phi(k,x)=\sqrt{\frac{2}{a+1}}\sin\left(\frac{\pi k x}{a+1}\right) \quad k,x=1,\ldots,a \tag{60}$$

$$g(x)=\Phi(1,x),\ h(x)=\Phi(a,x) \tag{61}$$

식(61)이 의미하는 것은 그림 5에서와 같이 경계조건 $g(x)$ 및 $h(x)$사이에서 암호화 함수 $U(\cdot)$의 해가 sinusoidal한 형태로 존재한다. 따라서, 암호화 함수 $U(\cdot)$의 해는 경계조건에 의존하는 것을 알 수 있다. 한편, 가중치 생성 함수의 생성에 쓰이는 비밀키 $q(x,y,t)$와 $f(x,y)$는 실험을 위하여 임의의 상수를 이용하였다. 그림 10은 중요도에 따라 암호화 위치 및 범위를 가변시켰을 경우의 결과 영상을 보이고 있다. 결과에서 보듯이 중요도에 따라 암호화 위치 및 범위를 가변할 수 있으므로 암호화 처리 시간을 단축할 수 있다.

실험에 사용된 구체적인 비밀키 함수와 수치적인 예는 다음과 같다. 여기에서, 암호화 범위는 간편성을 위하여 각각 2로 설정했고 비밀키들의 구체적인 함수와 원 영상의 화소값은 다음과 같이 설정했다.

- 암호화 함수의 생성시 쓰이는 비밀키

$g(x)=\sqrt{2/3}\sin(\pi x/3),\quad 1\le x\le 2$

$h(x)=\sqrt{2/3}\sin(2\pi x/3),\quad 1\le x\le 2$

- 가중치 함수의 생성에 쓰이는 비밀키

$q(x,y,t)=1,\quad f(x,y)=1$

- 원영상의 화소값

$a_{11}=137,\ a_{12}=136,\ a_{21}=135,\ a_{22}=137$

- 가중치 생성함수에 의한 가중치의 생성

① 본문의 식(35)를 이용하여 $Q_{m,n}(t)$를 구한다.

$$Q_{m,n}(t)=\left(1-\frac{2}{m\pi}\cos(m\pi)\right)\left(1-\frac{2}{n\pi}\cos(n\pi)\right)$$

② $\lambda_{m,n}$을 구한다.

$$\lambda_{m,n}=\left(\frac{m^2}{a^2}+\frac{n^2}{b^2}\right)\pi=\left(\frac{m^2}{4}+\frac{n^2}{4}\right)\pi$$

③ 본문의 식(42)를 이용하여 $C_{m,n}(t)$를 구한다.

$$C_{m,n}(t)=\int_0^t e^{-\lambda_{m,n}k(t-\tau)}Q_{m,n}(\tau)\,d\tau$$

④ 본문의 식(40)을 이용하여 $A_{m,n}$을 구한다.

$$A_{m,n}=\left(1-\frac{2}{m\pi}\cos(m\pi)\right)\left(1-\frac{2}{n\pi}\cos(n\pi)\right)$$

⑤ 본문의 식(44)을 이용하여 $\widehat{w_{xy}}$을 구한다.

$$\widehat{w_{11}}=\left(1+\frac{2}{\pi}\right)^2\left\{e^{-\frac{\pi}{2}ka_{11}}+\frac{2k}{\pi}\left(1-e^{-\frac{\pi}{2}ka_{11}}\right)\right\}$$

$\widehat{w_{12}}=0,\ \widehat{w_{21}}=0,\ \widehat{w_{22}}=0$

- 암호화 함수에 의한 화소의 암호화

① 본문의 식(19)를 이용하여 g_m , h_m을 구한다.

$g_m=\sqrt{2/3}\sin(\pi x/3),\quad 1\le x\le 2$

$\therefore\ g_1=\sqrt{2/3}\sin(\pi/3),\quad g_2=\sqrt{2/3}\sin(2\pi/3)$

$h_m=\sqrt{2/3}\sin(2\pi x/3),\quad 1\le x\le 2$

$\therefore\ h_1=\sqrt{2/3}\sin(2\pi/3),\quad h_2=\sqrt{2/3}\sin(4\pi/3)$

② 본문의 식(23)을 이용하여 $w_m(y)$를 구한다.

$$\therefore\ w_m(1)=g_m\frac{\sinh\left(\frac{m\pi}{2}\right)}{\sinh(m\pi)}+h_m\frac{\sinh\left(\frac{m\pi}{2}\right)}{\sinh(m\pi)}$$

$w_m(2)=h_m$

③ 본문의 식(26)을 이용하여 $C_{m,n}$을 구한다.

$$C_{m,n}=\frac{2n\pi}{(m^2+n^2)\pi}\left(g_m-(-1)^n h_m\right)$$

$\therefore\ C_{1,1}=g_1+h_1,\qquad C_{1,2}=\frac{4}{5}(g_1-h_1)$

$C_{2,1}=\frac{2}{5}(g_2+h_2),\quad C_{2,2}=\frac{1}{2}(g_2-h_2)$

④ 본 문의 식(24)를 이용하여 $v_m(y,t)$를 구한다.

$$v_m(y,t)=\sum_{n=1}^{2}C_{m,n}e^{-\left(\frac{m^2+n^2}{4}\right)\pi kt}\sin\left(\frac{n\pi y}{2}\right)$$

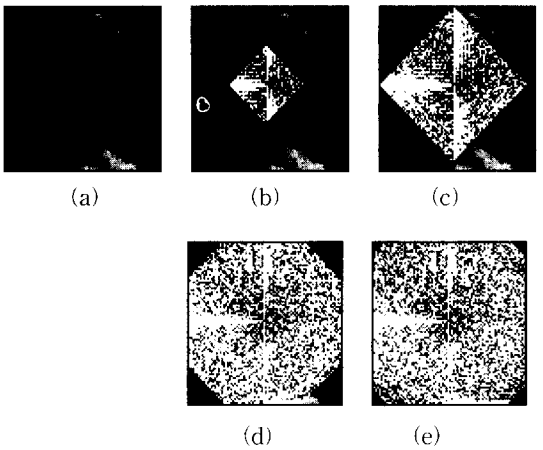
$$\therefore\ v_1(1,t)=C_{1,1}e^{-\left(\frac{1}{2}\right)\pi kt},\quad v_1(2,t)=0$$

$$v_2(1,t)=C_{1,1}e^{-\left(\frac{1}{2}\right)\pi kt},\quad v_2(2,t)=0$$

⑤ 최종적으로 본문의 식(27)을 이용하여 암호화된 값 $\widehat{a_{xy}}$를 구한다.

$\therefore\ \widehat{a_{11}} = w_1(1) + v_1(1, \widehat{w_{11}})$

$\widehat{a_{12}} = 0,\quad \widehat{a_{21}} = 0,\quad \widehat{a_{22}} = 0$

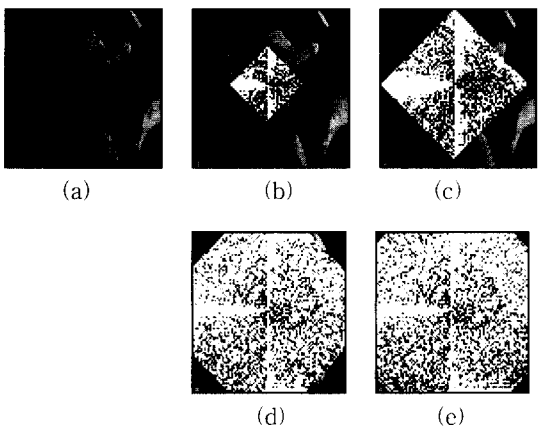


(a) (b) (c)

(d) (e)

그림 7. 암호화된 결과 영상
(a) "Girl" 원영상 (b) 암호화 범위 : 60 (c) 암호화 범위 : 120 (d) 암호화 범위 : 180 (e) 암호화 범위 : 230

Fig. 7. The result of encrypted image.
(a) Original image (b) Encryption range : 60 (c) Encryption range : 120 (d) Encryption range : 180 (e) Encryption range : 230

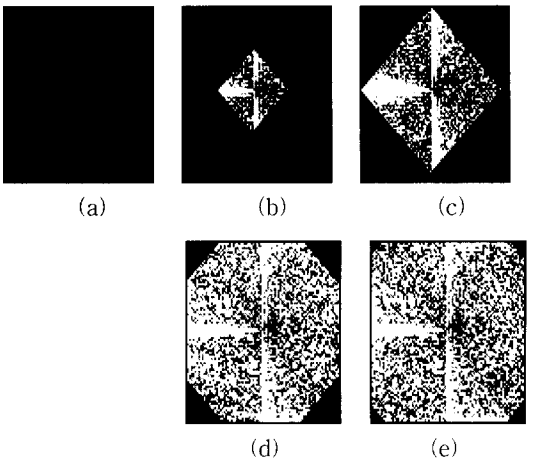


(a) (b) (c)

(d) (e)

그림 8. 암호화된 결과 영상
(a) "Lena" 원영상 (b) 암호화 범위 : 60 (c) 암호화 범위 : 120 (d) 암호화 범위 : 180 (e) 암호화 범위 : 230

Fig. 8. The result of encrypted image.
(a) Original image (b) Encryption range : 60 (c) Encryption range : 120 (d) Encryption range : 180 (e) Encryption range : 230



(a) (b) (c)

(d) (e)

그림 9. 암호화된 결과 영상
(a) "Miss America" 원영상 (b) 암호화 범위 : 60 (c) 암호화 범위 : 120 (d) 암호화 범위 : 180 (e) 암호화 범위 : 230

Fig. 9. The result of encrypted image.
(a) Original image (b) Encryption range : 60 (c) Encryption range : 120 (d) Encryption range : 180 (e) Encryption range : 230

Ⅳ. 결 론

본 논문에서는 물질전달함수를 이용한 영상 암호화 알고리즘을 제안했다. 제안한 알고리즘은 고인물에 떨어진 검은 잉크의 확산 현상을 기반으로 영상 정보의 특성을 고려하여 물질전달현상을 수학적으로 해석하고 해석된 결과를 영상정보 보호에 응용하였다. 즉, 영상 정보의 암호화 과정을 일종의 물질전달현상이 발생했다고 보는 시각이다.

기존의 영상 암호화 방식은 원영상의 주사선 및 블럭단위로 치환하거나 가산하는 형태의 암호화를 수행하는 반면, 본 논문에서 제안한 암호화 방식은 화소 단위로 암호화를 수행하기 때문에 암호화 강도를 향상시킨 결과를 얻을 수 있었고 중요도에 따라 암호화 범위를 가변시키므로서 처리 시간을 단축할 수 있었다.

제안한 알고리즘의 응용 분야는 영상 신호의 전송 시스템에서 영상 데이터의 보호에 응용될 수 있다. 예를 들면, 원격 화상회의 및 화상전화 시스템, HDTV 영상 전송 시스템, 초저속 동영상 전송 시스템 등에 응용될 수 있다. 특히, 초저속 동영상 전송 시스템은 동영상의 파형에 관한 정보를 전송하기 보다는 동영상의 파형에서 추출된 특징 파라미터들을 부호화하여 전송

그림 10. 중요도에 따라 암호화 위치를 가변시켰을 경우의 결과 영상
Fig. 10. The result of encrypted images changed with respect to position by importance.

하기 때문에 각 신호의 특성에 따라 암호화 방식을 달리해야 할 필요성이 있기 때문에 본 논문에서 제안한 암호화 알고리즘 이외에 기존에 제안된 스크램블링을 이용한 암호화 방식도 함께 이용하는 것이 효율적일 것이다.

향후 연구과제로는 채널을 통한 정보의 전송시 에러에 대처할 수 있는 오류정정이 가능한 암호화에 관한 연구와 부동소숫점 연산(floating point computation)을 정수(integer) 연산화 시키는 연구가 요구된다. 또한 암호화 강도의 분석을 위한 알고리즘 개발과 제안한 암호화 알고리즘의 3차원 확장을 위한 수학적 접근 방식이 요구된다.

※ 본 논문의 연구는 과학재단 '94 특정연구과제 지원비에 의해 수행되었음.

참 고 문 헌

[1] 南憲明, 若杉耕一郎, 笠原正雄, "畵像情報のセキュリティ確保に關する考察", 信學技報, Vol.90, No 31, ISEC91-8, 1991.

[2] 汁井重男, 笠原正雄, "暗號と情報セキュリテイ", 昭光堂, 1990.

[3] 前田章, 古材文伸, 白石高義, "ティシタル畵像情報のセキュリティ確保に關する考察", 信學技報, Vol. 90, No. 31, ISEC 91-8, 1991.

[4] 前田章, 古材文伸, 白石高義, "デイジタル畵像に滴したデータ暗號化の一方法", 電子通信學會論文誌, Vol. J69-B, No. 11, 1986.

[5] Kazuhito TANAKA, Kazunari FUNAME, Masao KASAHARA, "A Method of Combining Coding and Encryption for Image Source", CIS'89.

[6] Yossi Matias, Adi Shamir, "A Video Scrambling Technique Based on Space Filling Curve", CRYPTO'87, 1987.

[7] Norio Shioiri, Hirotsugu Kinoshita, Yoshinori Sakai, "A Study on the Satellite teleconferencing Protocol for Security", 信學技報, Vol. 90, No. 31, ISEC 90-34, 1990.

[8] J. R. Welty, C. E. Wicks and R. E. Wilson, "Fundamentals of Momentum, Heat and Mass Transfer", pp 173-247, 363-452.

[9] Edward Haug and Kyung K. CHOI, "Methods of Engineering Mathematics", Prentice Hall, pp 280-382.

[10] L. E. Payne, "Improperly Posed Problems in Partial Differential Equations", Springer Lecture Notes, 1974.

[11] J. Hadamard, "Lectures on the Cauchy Problems in Linear Partial Differential Equations", Yale Univ. Press. New Haven, 1923.

[12] R. E. Showalter, "Well-posed problems for a partial differential equation of order 2m+1", SIAM J. Math. Anal. 1, pp 214-231, 1974.

[13] R. E. Showalter and T.W. Ting, "Pseudoparabolic partial differential equations", SIAM J. Math. Anal. 1, pp 1-25, 1970.

[14] Paul W. Berg and James L. McGregor, "Elementary Partial Differential Equations", Stanford University, 1966.

[15] Gerald B. Folland, "Introduction to Partial Differential Equations", Princeton University, 1976.

[16] Ladis D. Kovach, "Boundary-Value Problems", Addison-Wesely Publishing, 1983.

[17] S. J. Farlow, "Partial Differential Equations for Scientists & Engineers", John Wiley & Sons, 1982.

[18] 김승종, 김태우, 민병석, 김재훈, 김한우, 최병욱, "영상정보 보호를 위한 확산 암호화 기법", 제6회 신호처리학회논문지 제6권 1호, 1993

[19] 김승종, 김태우, 민병석, 김재훈, 김한우, 최병욱, "물질전달모델을 기반으로 한 영상 암호화", 제7회 신호처리학회논문지 제7권 1호, 1994

[20] Paul W. Berg and James L. McGregor, "Elementary Partial Differential Equations", Stanford University, pp 149-165, 1966.

저 자 소 개

金 承 琮(正會員)

1992년 2월 한양대학교 자연과학대학 수학과 졸업(이학사). 1994년 2월 한양대학교 대학원 전자통신공학과 졸업(공학석사). 1996년 11월 ~ 현재 한양대학교 대학원 전자통신공학과 박사과정. 관심분야는 디지틀 신호처리, 영상 통신 및 압축, 영상 암호 등

崔 炳 旭(正會員) 第 33卷 B編 第3號 參照.