2진화상워터마킹체계에서 견고성개선의 한가지 방법

김윤복, 김진성

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《새로운 과학기술분야를 개척하기 위한 사업도 전망성있게 밀고나가야 합니다.》(《**김정일**선집》 증보판 제11권 138페지)

워터마크정보의 부호화 및 복호화는 워터마킹체계의 견고성을 높이기 위한 중요한 수단으로서 선행연구[1]에서는 DWT에 의한 워터마킹에서 BCH부호를 리용한 방법을, 선행연구[2]에서는 중첩부호를 리용한 방법을, 선행연구[3]에서는 터보부호를 리용하는 방법들을 제기하였다. 그러나 이 방법들에서는 삽입하는 정보부호렬을 독립인 우연량렬이라고 보았으며 정보부호들사이의 상관성이 있는 경우는 고려하지 못하였다.

론문에서는 삽입하는 워터마크정보가 2진화상인 경우 린접한 화소점들에서 화소값들의 상관이 크다는것을 리용하여 워터마킹체계의 견고성을 높이기 위한 한가지 복호화방법을 제기하고 그것의 효과성을 워터마크삽입알고리듬[4]을 리용하여 검증하였다.

1. 2진워터마크화상의 중첩부호화

2진워터마크화상의 중첩부호화는 다음과 같은 방법으로 진행한다.

$I(i,\ j)\in\{0,\ 1\}$ $(i=1,\cdots,\ m,\ \ j=1,\cdots,\ n)$을 $m\times n$ 크기의 2진워터마크화상이라고 하자.

2차원화상 $I(i,\ j)$를 1차원으로 변환하여 다음과 같은 W를 얻는다.

$$W:=(w(1),\ w(2),\ \cdots,\ w(m\times n)),\ \ w(k)=w((i-1)\cdot n+j)=I(i,\ j)\ \ (k=1,\cdots,\ m\times n) \quad (1)$$

$w(k)$에 대하여 1부터 8까지의 상태 state(k)와 4개 비트로 이루어진 부호단어 $c(k)$를 다음과 같이 대응시킨다.

$$\text{state}(1):=\text{key},\ \ \text{key}=1,\cdots,\ 8$$

$$\text{state}(k):=\ A(w(k)+1,\ \text{state}(k-1))\ \ (k=2,\cdots,\ m\times n)$$

$$c(k):=B(w(k)+1,\ \text{state}(k))$$

여기서 A는 상태이행행렬, B는 부호행렬로서 다음과 같다.

$$A:=\begin{pmatrix}1&3&5&7&1&3&5&7\\2&4&6&8&2&4&6&8\end{pmatrix}$$

$$B:=\begin{pmatrix}0000&1100&1010&0111&1101&1110&0100&0110\\1111&0011&0101&1000&0010&0001&1011&1001\end{pmatrix}$$

즉 2진워터마크화상의 매 화소값 $I(i,\ j)$는 이행행렬 A와 부호행렬 B에 의하여 4bit로 부호화되며 화상의 부호화결과는 $C=(c(1),\ c(2),\ \cdots,\ c(m\times n))$이다.

2. 화소값들의 상관을 고려한 Viterbi복호화

두 중첩부호사이의 거리는 일반적으로 아래와 같은 하밍거리를 리용한다.[2]

$$d(C,\ C') := \sum_{k=1}^{m\times n} d_H(c(k),\ c'(k)) \tag{2}$$

여기서 $c(k) = (b_1,\ b_2,\ b_3,\ b_4)$, $c'(k) = (b'_1,\ b'_2,\ b'_3,\ b'_4)$ 일 때

$$d_H := (c(k),\ c'(k)) = |\{l \mid b_l \neq b'_l \ \ (l = 1,\ 2,\ 3,\ 4)\}|$$

워터마크검출알고리듬에 의하여 검출된 중첩부호를

$$C' := (c'(1),\ c'(2),\ \cdots,\ c'(m\times n))$$

이라고 하자.

Viterbi복호화방법은 동적계획법으로 가능한 모든 부호 C 들중에서 하밍거리 (2)의 의미에서 C' 와 가장 가까운 부호

$$C^* := \arg\min_{C} d(C,\ C')$$

를 찾기 위한 알고리듬이다.

워터마크정보가 2진화상인 경우 린접한 화소점들에서의 화소값들은 높은 상관성을 가진다. 즉 검출된 중첩부호 C' 에서 $c'(k)$ 가 나타내는 비트를 $w'(k)$ 라고 하면 $w'(k) = w(k-1)$ 이 성립될 가능성이 크다고 볼수 있다.

이로부터 론문에서는 하밍거리 (2)대신 린접한 부호비트들사이의 이행확률을 고려한 다음과 같은 거리를 도입한다.

$$\hat{d}(C,\ C') := \sum_{k=1}^{m\times n} -\log P(w(k)|w(k-1)) \cdot d_H(c(k),\ c'(k)) \tag{3}$$

여기서 $P(u \mid v)$ 는 $k-1$ 째 비트값이 v 일 때 k 째 비트값이 u 로 될 확률이다.

거리 (3)을 리용한 Viterbi복호화방법은 다음과 같다.

$W := (w(1), \cdots,\ w(m\times n))$ 은 정보부호렬이고 $S := (s(1),\ \cdots,\ s(m\times n))$ 은 W 의 상태렬이며 $C := (c(1),\ \cdots,\ c(m\times n))$ 은 W 의 중첩부호렬, $C_k := (c(1), \cdots,\ c(k))$, $W_k := (w(1),\ \cdots,\ w(k))$ 는 각각 C, W 의 부분렬이라고 하자.

또한 $A_k(i,\ j) := \{C_k \mid s(k) = i,\ w(k) = j\}$ 는 k 째 상태가 i, $w(k) = j$ 인 C_k 들의 모임이며 $C_k^*(i,\ j) := \arg\min_{C\in A_k(i,\ j)} \hat{d}(C,\ C'_k)$, $F_k(i,\ j) := \hat{d}(C_k^*(i,\ j),\ C'_k)$ 라고 하자.

그리고 $W_k^*(i,\ j)$ 는 $C_k^*(i,\ j)$ 에 대응한 정보부호렬이라고 하자.

이때 $F_k(i,\ j)$, $W_k^*(i,\ j)$ 들은 다음과 같은 알고리듬에 의하여 계산된다.

① 초기상태 key, 최대반복회수 $N_{\max}$, $F_k(i,\ j)$ 에 대한 변화량 ε 을 설정한다.

$$N \leftarrow 0,\ F_{\min} \leftarrow +\infty,\ \Delta F \leftarrow +\infty$$

$$P(u|v) \leftarrow 0.5\ \ (u,\ v \in \{0,\ 1\})$$

② $N < N_{\max}$, $\Delta F > \varepsilon$ 인 동안 아래의 처리를 반복한다.

③ $W_0^*(i,\ j) = \varnothing\ \ (i = 1, \cdots, 8;\ j = 0,\ 1)$

④ $F_0(i,\ j):=\begin{cases}0, & j=\text{key}\\ +\infty, & j\neq\text{key}\end{cases}$ $(i=1,\cdots,8;\ \ j=0,\ 1)$

⑤ For $k=1$ to $m\times n$

For state = 1 to 8

For bit = 0 to 1

$F_k(\text{state},\ \text{bit})=f(i^*,\ j^*)$

$f(i,\ j)=F_{k-1}(i,\ j)-\log(P(\text{bit}|j))\cdot d_H(B(i,\ j+1),\ c'(k))$

$(i^*,\ j^*)=\underset{\{(i,\ j)|A(i,\ j+1)=state\}}{\arg\min} f(i,\ j)$

$W_k^*(\text{state},\ \text{bit})=(W_{k-1}^*(i^*,\ j^*),\ \text{bit})$

End

End

End

⑥ $(i^*,\ j^*):=\underset{i=1,\cdots,8,\ j=0,\ 1}{\arg\min} F_{m\times n}(i,\ j)$, $F^*:=F_{m\times n}(i^*,\ j^*)$ 이라고 하면 복호화된 정보부호렬 W^*은 $W^*=W_{m\times n}^*(i^*,\ j^*)$로 계산된다.

$\Delta F=F_{\min}-F^*$

$F_{\min}=F^*$

$N=N+1$

⑦ 복호화된 W^*로부터 $P(u|v)$를 계산한 다음 ③으로 간다.

2진워터마크화상 I'는 우의 알고리듬에 의하여 복호화된 비트렬

$$W^*=(w^*(1),\cdots,\ w^*(m\times n))$$

에 식 (1)의 반대과정을 적용하여 얻을수 있다.

3. 성 능 평 가

우리는 워터마크삽입알고리듬[4]과 선행연구[1－3]의 부호화, 복호화방법들, 선행연구[2]의 부호화와 론문의 복호화방법을 결합하였을 때 검출되는 워터마크의 견고성을 평가하는 방법으로 론문에서 제기한 복호화방법의 효과성을 검증한다.

워터마킹체계의 견고성은 $\text{BER}=\dfrac{\sum_{i=1}^{m}\sum_{j=1}^{n}|I(i,\ j)-I'(i,\ j)|}{m\cdot n}\cdot 100$에 의하여 평가한다. 여기서 I는 원래의 워터마크화상이고 I'는 검출된 워터마크화상이다.

Lena화상과 Babbon화상에 대하여 이전의 중첩부호화와 Viterbi복호화방법[2], BCH부호를 리용한 부호화와 복호화방법[1], 터보부호를 리용한 부호화와 복호화방법[3]과 론문에서 제기한 중첩부호화와 복호화방법들을 각각 적용한 경우 잡음추가공격, 려파공격, 압축공격, 척도변환공격을 비롯한 여러가지 공격에 대한 BER를 평가한 결과는 표와 같다.

표. 각이한 공격에 대한 비트오유률(BER)

	Lena 화상				Babbon 화상			
	방법[2]	방법[1]	방법[3]	론문의 방법	방법[2]	방법[1]	방법[3]	론문의 방법
가우스잡음추가(0.003)	10.4	27.3	2.8	1.4	7.9	23.2	3.6	1.3
Salt&pepper잡음추가(0.05)	3.5	20.1	3.0	0.3	7.0	18.5	3.2	0.9
Speckle잡음추가(0.005)	7.7	23.1	2.5	1.0	3.2	11.9	8.8	0.4
중간대역려파기(3×3)	7.0	16.9	4.5	2.0	13.3	11.6	3.3	3.3
위너려파기(3×3)	6.0	11.4	7.5	2.0	14.6	30.0	2.6	4.6
JPEG압축(50)	0.1	2.3	12.7	0.0	0.4	30.6	15.7	0.0
JPEG압축(75)	0.0	0.0	2.9	0.0	0.0	0.6	6.6	0.0
축소－확대(512－256－512)	10.2	17.4	6.9	3.4	16.4	36.0	3.1	8.4

우의 결과로부터 론문에서 제기한 복호화방법을 리용하는 경우 이전의 복호화방법들보다 BER가 훨씬 작아진다는것을 알수 있다.

참 고 문 헌

[1] N. Nigam et al.; Int. J. Comput. Appl., 110, 37, 2015.

[2] J. R. Hernandez et al.; In Proc. SPIE Conf. on Security and Watermarking of Multimedia Content II, 3971, 24, 2000.

[3] S. Pereira et al.; In IEEE Int. Conf. on Image Processing, 3, 671, 2000.

[4] F. Ernawan et al.; Electronic and Computer Engineering, 9, 2, 111, 2015.

주체107(2018)년 12월 5일 원고접수

A Method for Improving the Robustness in Binary Image Watermarking

Kim Yun Bok, Kim Jin Song

We propose a decoding method using characteristic of the binary watermark image to improve the robustness of the binary image watermarking system and verify its effectiveness.

Key words: decoding, binary watermark image