

パッチワークによる署名画像に対する秘密鍵の探索攻撃

山 田 隆 行 松 井 甲 子 雄

防衛大学校 情報工学教室

電子透かしは、デジタルデータの不正利用を防止するために開発され、人が知覚できない冗長部分にノイズとして埋め込まれる。これまでにその耐性強度を測定するために各種の攻撃法が検討されているが、評価尺度はいまだ確立されていない。電子透かしがどのくらいの耐性を持っているか正しく評価することは重要なことである。この報告では、パッチワーク法によって署名を施した多値画像に対して、その透かし情報として用いられた疑似乱数系列とシフト量を求める全数探索アプローチを提案する。その判定尺度として、SN比と分散を利用し、一枚の署名済画像からパッチワークの秘密鍵を求めることができることを示す。

Key-search attack on image signed by patchworking

TAKAYUKI YAMADA and KINEO MATSUI

Department of Computer Science, National Defense Academy

A digital watermark is developed to prevent from the illegal use of the digital data and is embedded in the redundant part where it can not be perceived as interference noise. So far, various attack methods are examined to measure the robustness of digital watermark but the evaluation measure of watermark is not established yet. It is important to us how much robustness the digital watermark has. In this report, we propose the general hit search approach which looks for the pseudo-random number sequences and the shift quantity which is used as the watermark to the digital monotone picture signed by the patch-working. It is shown in the report for attacker to find the secret key of patch-working from the signed picture by using SN ratio and variance.

1. はじめに

電子透かしは、マルチメディアコンテンツに著作権情報を埋め込む技術である。すでに多くの透かし方式が提案されているが¹⁾、それらの方式の耐性強度を比較するための尺度がいまだ確立されていない²⁾。この報告では、パッチワーク法と呼ばれている電子透かしの方式について、その秘密鍵を求める方法を検討する。その前提として、与えられた一枚の多値画像に透かし情報が埋め込まれていること、その埋め込みアルゴリズムが既知、すなわち、この報告ではパッチワーク法であること、さらに使用された乱数は疑似乱数系列であること、などを仮定しておく。このとき、以下に述べる方法で一枚の署名済画像から透かし情報を探索できることを示す。

2. パッチワーク法の概要

統計量を利用する透かしのアプローチをパッチワークと呼んでいる³⁾。仮定として疑似乱数を使う。パッチワークはガウス分布のような統計量を目に見えないように原画像に埋め込む手法である。まず、画像から

無作為に2画素 a_i と b_i を選び、二つの画素の差分を

$$s_i = a_i - b_i \quad (1)$$

と置く。この操作を n 回繰り返す。ここで s_i の分布の和 S_n を次のように定義する。

$$S_n = \sum_{i=1}^n s_i = \sum_{i=1}^n (a_i - b_i) \quad (2)$$

統計過程に疑似乱数を使うと s_i の期待値 $\bar{s}_i$ は 0 となる。 S_n の期待値 $\bar{S}_n$ は

$$\bar{S}_n = n \times \bar{s}_n = n \times 0 = 0 \quad (3)$$

となる。そこで、与えられた原画像に対して S_n が期待値から大きく偏るように透かし情報 δ を埋め込む。ただし、 δ は 5 以下の正整数値とする。その手順は以下になる⁴⁾。

手順1：既知の疑似乱数発生器に特定の鍵を与えて二つの画素 a_i, b_i を選ぶ。

手順2：パッチ a_i の輝度値を δ だけ上げる。

$$a_i \leftarrow a_i + \delta \quad (4)$$

手順3： b_i の輝度値を δ だけ下げる。

$$b_i \leftarrow b_i - \delta \quad (5)$$

手順4：上記の手順1～3を n 回繰り返す。

こうして得られた透かし画像から情報を取り出す過程で埋め込み後の期待値 S'_n は以下のようになる。

$$S'_n = \sum_{i=1}^n \{(a_i + \delta) - (b_i - \delta)\}$$

$$= \sum_{i=1}^n \{(a_i - b_i) + 2\delta\} \quad (6)$$

n を増大するに従い、 δ の期待値の累積分だけ分布は右へ移動する。この移動量から 原画像と透かし画像の画素差の分布を類別でき、1 ビットの透かし情報を埋め込むことができる。 δ が大きくなるほど分布間の差が広がるが、同時に画質劣化も大きくなる。以下、この方法で原画像の画素値をランダムに増減した画像を特に透かし画像と呼ぶことにする。

3. 鍵探索方法

まず、図 1 に秘密鍵を探索する概要を示す。ただし、原画像は著作権者のみが所有するため、攻撃者はそれを使用できないものとする。

$$a_i \leftarrow a_i - \Delta \quad (7)$$

$$b_i \leftarrow b_i + \Delta \quad (8)$$

いま、ある透かし画像に対して、攻撃側は既知の透かし埋め込みアルゴリズムを解析し、パッチ a_i の画素値を Δ だけ下げ、パッチ b_i の画素値を Δ だけ上げる (このとき乱数発生のために必要となる種としての鍵を逆鍵と呼び、透かし画像に逆鍵を埋め込んだ画像を逆画像と呼ぶことにする)。もし、正しい逆鍵と $\delta = \Delta$ であれば、埋め込んだパッチは、理論上相殺される。ノイズとして埋め込まれた透かし情報は一般に透かし画像の分散を大きくするように働くため、正しい逆鍵を用いたとき分散は最小となり、誤った逆鍵を用いたとき分散はその値より大きくなる。

さらに、透かし画像に逆鍵を埋め込んだ画像に、パッチ a_i の画素値を Δ だけ上げ、パッチ b_i の画素値を Δ だけ下げる (このとき乱数発生のために必要となる種としての鍵を順鍵と呼び、逆画像に順鍵を埋め込んだ画像を順画像と呼ぶことにする)。

$$a_i \leftarrow a_i + \Delta \quad (9)$$

$$b_i \leftarrow b_i - \Delta \quad (10)$$

次に、著作権者が使った秘密鍵を全数探索で検索する。画素番号と乱数の埋め込み位置とその値を図 2 に、このときの画素値の変化の様子を図 3 に示す。図 3 に示すように画素値と乱数系列によっては桁あふれを生じる (多値を $2^8 = 256$ 階調で表現したとき、この範囲外のを本稿では桁あふれと記述する) ため、一般に透かし画像と順画像は同じ画像とはならず、その

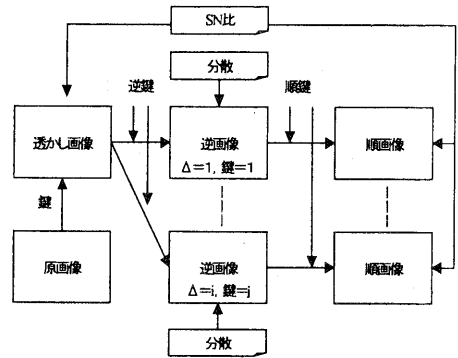


図 1 鍵探索の流れ

Fig. 1 Key-searching flow diagram.

位置	1	2	4	5
値	1	-1	1	-1

位置	2	1	5	4
値	1	-1	1	-1

1	2	3
4	5	6
7	8	9

位置	5	6	8	9
値	1	-1	1	-1

位置	6	5	9	8
値	1	-1	1	-1

図 2 埋め込み位置とその値

Fig. 2 Embedded position and value.

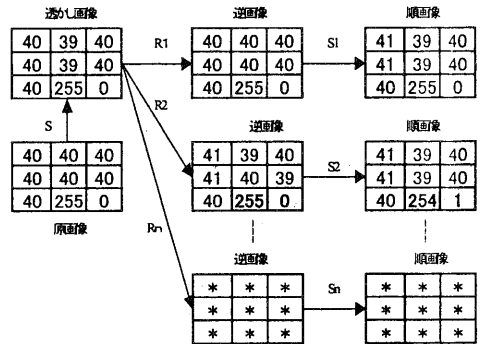


図 3 画素値の変化と桁あふれ

Fig. 3 Hysteresis of some pixel values and overflows.

SN 比は下がる。攻撃側が探索した鍵が正しいものであるか否かを判別するために、逆画像の分散と、透かし画像と順画像の SN 比を用いる。

ここに、SN 比と分散 σ^2 は以下の式を用いて算出する⁴⁾⁵⁾。

$$SN = 20 \times \log_{10} \left(255 / \sqrt{\sum_{i=1}^{m^2} (orig_i - emb_i)^2 / m^2} \right) \quad (11)$$

$$\sigma^2 = \frac{1}{m^2} \sum_{i=1}^{m^2} (x_i - \bar{x})^2 = \frac{1}{m^2} \sum_{i=1}^{m^2} x_i^2 - \bar{x}^2 \quad (12)$$

$$\bar{x} = \frac{1}{m^2} (x_1 + x_2 + \dots + x_{m^2}) = \frac{1}{m^2} \sum_{i=1}^{m^2} x_i \quad (13)$$

$orig_i$: 原画像の画素 i の画素値

emb_i : 透かし画像の画素 i の画素値

m : 画像のサイズ

$\bar{x}$: 平均

4. 鍵探索結果

4.1 透かし画像の作成

原画像として準画像 girl を使い, $k=1$, $\delta=1$, 埋め込み量 $n=10000$, 5000 として 2 枚の透かし画像を作成する。また, 鍵 $k=1$, $\delta=1$, 埋め込み量 $n=10000$ のときの透かし画像を図 5 に, 乱数の分布を図 6 に示す。原画像と透かし画像の SN 比は, $n=10000$ のとき 53.28dB であり, $n=5000$ のとき 56.29dB である。図 6 からほぼ均一に透かしが埋め込まれているのがわかる。

4.2 $n=10000$ における探索結果

全数探索の結果は紙面の都合上記すことができないため, 表 1 に鍵を 1 から 100, Δ を 1 から 3 の範囲の探索した結果を示す。SN 比の欄が のものは, 順画像が透かし画像と同一であることを示している。分散が小さく SN 比が良いものは $k=1, \Delta=1$ であり, これを鍵の候補と考えることができる。

4.3 $n=5000$ における探索結果

埋め込み量の推定が異なっているときの探索として, 表 2 に鍵を 1 から 100, Δ を 1 から 3 の範囲の探索した結果を示す。このときは, 埋め込み量の推定が正しいときに比べて, 分散と SN 比の分布が狭くなるため, 鍵の推定は難しくなるが $k=1, \Delta=1$ を候補として探すことが可能である。



図 4 原画像
Fig. 4 Original image



図 5 透かし画像
Fig. 5 Watermarked image



図 6 乱数分布
Fig. 6 Distribution of random number

表 1 鍵探索結果 (n= 10000)
Table 1 Result of Key-search(n= 10000)

k \ Δ	3		2		1	
	分散	SN比	分散	SN比	分散	SN比
100	1818.83	73.03	1817.59	79.67	1816.89	90.28
99	1818.62	75.65	1817.43	82.87	1816.81	96.30
98	1819.02	75.36	1817.71	82.87	1816.96	
97	1820.30	75.50	1818.56	81.98	1817.37	93.29
96	1818.47	75.12	1817.33	80.98	1816.75	90.28
95	1819.08	75.69	1817.74	82.87	1816.95	93.29
94	1818.82	73.53	1817.57	80.17	1816.89	96.30
93	1819.47	76.17	1817.99	82.15	1817.09	93.29
92	1819.14	73.07	1817.80	79.67	1817.01	93.29
91	1819.06	75.65	1817.72	81.67	1816.95	91.52
90	1819.37	77.72	1817.93	84.53	1817.05	93.29
89	1820.21	74.07	1818.51	81.52	1817.36	96.30
88	1820.03	75.54	1818.36	81.67	1817.27	93.29
87	1819.83	72.48	1818.25	78.81	1817.22	89.31
86	1819.15	75.54	1817.79	82.32	1816.99	
85	1818.99	77.05	1817.67	84.25	1816.92	93.29
84	1818.79	76.25	1817.54	83.29	1816.86	96.30
83	1819.47	73.84	1818.00	79.96	1817.09	90.28
82	1819.39	75.47	1817.96	81.98	1817.07	93.29
81	1819.87	75.73	1818.28	82.68	1817.23	93.29
80	1819.42	74.80	1817.96	81.38	1817.07	93.29
79	1819.42	76.30	1817.96	82.49	1817.06	93.29
78	1820.06	74.93	1818.40	81.67	1817.29	96.30
77	1820.15	71.92	1818.47	77.43	1817.34	87.84
76	1819.08	73.74	1817.74	79.76	1816.97	91.52
75	1819.94	74.28	1818.32	80.85	1817.25	93.29
74	1818.88	75.12	1817.62	82.68	1816.90	96.30
73	1819.52	78.74	1818.02	85.88	1817.10	96.30
72	1819.57	74.20	1818.08	80.73	1817.14	96.30
71	1820.51	75.96	1818.68	83.29	1817.43	
70	1818.48	76.34	1817.34	83.99	1816.76	
69	1819.24	76.25	1817.84	82.68	1817.01	93.29
68	1818.88	73.69	1817.61	79.31	1816.90	88.51
67	1818.93	75.16	1817.62	80.50	1816.90	89.31
66	1820.07	74.15	1818.39	80.39	1817.29	91.52
65	1820.21	73.62	1818.50	79.76	1817.35	91.52
64	1820.36	74.56	1818.58	79.76	1817.38	89.31
63	1818.54	75.65	1817.38	82.32	1816.79	96.30
62	1818.46	74.02	1817.32	79.57	1816.76	90.28
61	1819.96	76.21	1818.32	82.68	1817.25	93.29
60	1819.48	73.31	1818.01	78.66	1817.10	87.26
59	1820.23	74.20	1818.53	81.38	1817.36	
58	1819.67	75.12	1818.12	81.67	1817.15	93.29
57	1818.62	75.47	1817.44	82.87	1816.81	96.30
56	1819.12	74.87	1817.76	80.98	1816.96	91.52
55	1818.93	75.92	1817.64	82.68	1816.91	93.29
54	1819.31	73.07	1817.90	78.30	1817.04	87.84
53	1819.50	76.66	1818.01	82.68	1817.10	96.30
52	1819.51	74.39	1818.04	81.82	1817.11	96.30
51	1819.65	73.84	1818.12	79.86	1817.16	91.52

k \ Δ	3		2		1	
	分散	SN比	分散	SN比	分散	SN比
50	1819.38	78.66	1817.93	86.75	1817.05	
49	1819.42	74.93	1817.98	81.38	1817.09	93.29
48	1818.88	74.80	1817.62	81.52	1816.90	93.29
47	1819.16	76.71	1817.78	82.87	1816.98	93.29
46	1818.82	72.57	1817.56	78.10	1816.89	87.84
45	1819.78	73.82	1818.20	79.39	1817.20	90.28
44	1818.93	73.03	1817.65	79.31	1816.92	90.28
43	1818.75	75.84	1817.51	82.49	1816.85	96.30
42	1819.21	76.85	1817.82	83.51	1817.00	96.30
41	1818.83	75.09	1817.58	82.15	1816.88	96.30
40	1819.55	73.69	1818.05	80.06	1817.12	91.52
39	1819.01	73.58	1817.70	79.39	1816.95	90.28
38	1818.76	74.68	1817.52	80.73	1816.85	91.52
37	1819.29	75.16	1817.89	82.15	1817.04	96.30
36	1820.48	73.53	1818.68	79.14	1817.43	88.51
35	1819.37	73.29	1817.95	79.57	1817.08	91.52
34	1819.84	74.12	1818.25	80.17	1817.22	91.52
33	1819.85	74.42	1818.27	81.38	1817.23	93.29
32	1819.88	73.51	1818.28	80.17	1817.24	93.29
31	1819.23	73.22	1817.86	79.31	1817.02	89.31
30	1818.92	75.88	1817.62	82.87	1816.91	
29	1820.14	77.21	1818.44	83.99	1817.31	96.30
28	1818.90	74.65	1817.62	81.82	1816.91	96.30
27	1819.62	73.99	1818.08	79.48	1817.13	90.28
26	1819.62	74.59	1818.09	81.38	1817.14	
25	1819.14	73.07	1817.79	78.81	1817.00	89.31
24	1819.75	76.08	1818.18	83.99	1817.18	96.30
23	1819.01	74.68	1817.70	80.98	1816.95	93.29
22	1819.60	72.93	1818.11	80.39	1817.15	96.30
21	1818.96	73.58	1817.66	78.81	1816.92	86.30
20	1819.00	73.74	1817.70	79.67	1816.95	88.51
19	1818.80	76.34	1817.54	82.68	1816.86	93.29
18	1819.71	75.02	1818.16	82.32	1817.18	96.30
17	1820.28	74.99	1818.55	82.87	1817.37	96.30
16	1819.49	74.17	1818.02	80.39	1817.11	91.52
15	1819.07	74.59	1817.73	80.85	1816.96	93.29
14	1820.06	76.21	1818.39	83.29	1817.29	96.30
13	1819.41	75.88	1817.95	82.32	1817.07	96.30
12	1819.45	74.42	1818.00	81.11	1817.09	90.28
11	1819.23	73.92	1817.83	79.67	1817.01	90.28
10	1819.20	77.16	1817.82	85.16	1817.00	96.30
9	1819.57	73.72	1818.08	80.06	1817.14	91.52
8	1819.53	74.68	1818.04	80.61	1817.11	91.52
7	1818.71	74.71	1817.49	80.98	1816.84	93.29
6	1818.84	75.19	1817.58	81.67	1816.88	93.29
5	1819.43	74.34	1817.98	80.50	1817.08	90.28
4	1820.33	74.34	1818.57	80.61	1817.38	93.29
3	1819.60	74.65	1818.10	82.15	1817.15	
2	1818.63	76.61	1817.43	83.99	1816.80	96.30
1	1817.86	83.07	1816.90	96.30	1816.53	

表 2 鍵探索結果 (n = 5000)
Table 2 Result of Key-search (n = 5000)

k \ Δ	3		2		1	
	分散	SN比	分散	SN比	分散	SN比
100	1817.59	79.48	1817.03	85.50	1816.75	93.29
99	1817.56	78.81	1817.02	85.50	1816.75	96.30
98	1818.08	79.14	1817.36	85.88	1816.92	
97	1818.66	81.67	1817.74	90.28	1817.10	
96	1817.36	79.22	1816.88	85.16	1816.67	96.30
95	1817.92	82.32	1817.24	88.51	1816.85	96.30
94	1817.52	78.66	1816.98	84.25	1816.73	96.30
93	1817.75	78.81	1817.13	84.25	1816.80	93.29
92	1817.86	78.59	1817.22	85.88	1816.85	
91	1817.68	79.76	1817.07	85.16	1816.77	96.30
90	1817.76	80.06	1817.14	86.75	1816.81	96.30
89	1818.89	79.96	1817.90	87.26	1817.19	
88	1818.34	79.76	1817.52	85.88	1817.00	96.30
87	1818.19	77.60	1817.43	84.83	1816.96	
86	1817.77	83.07	1817.14	90.28	1816.80	
85	1817.81	79.86	1817.17	85.50	1816.82	93.29
84	1817.87	83.99	1817.21	93.29	1816.83	
83	1818.34	77.91	1817.53	83.99	1817.01	96.30
82	1817.99	78.44	1817.29	84.53	1816.88	96.30
81	1818.61	79.86	1817.72	87.26	1817.09	96.30
80	1817.75	79.48	1817.13	87.26	1816.80	
79	1818.16	78.44	1817.40	83.74	1816.93	93.29
78	1818.21	80.28	1817.44	87.26	1816.95	
77	1818.44	75.26	1817.60	80.50	1817.04	90.28
76	1818.13	77.32	1817.39	83.07	1816.93	93.29
75	1818.15	77.43	1817.41	83.74	1816.94	93.29
74	1817.79	77.43	1817.16	83.51	1816.82	96.30
73	1818.25	83.29	1817.47	91.52	1816.97	
72	1818.12	79.76	1817.38	86.75	1816.93	
71	1818.69	80.39	1817.75	86.75	1817.11	
70	1817.44	81.52	1816.93	90.28	1816.69	
69	1818.00	81.67	1817.30	88.51	1816.88	96.30
68	1818.09	78.03	1817.36	83.29	1816.92	93.29
67	1817.61	80.28	1817.04	86.30	1816.75	96.30
66	1818.07	77.91	1817.35	83.51	1816.91	93.29
65	1818.41	78.23	1817.57	84.53	1817.02	96.30
64	1818.62	78.74	1817.71	84.83	1817.09	96.30
63	1818.18	78.51	1817.43	85.50	1816.95	
62	1817.25	80.06	1816.79	86.75	1816.63	
61	1818.00	80.61	1817.30	88.51	1816.89	
60	1817.95	74.87	1817.27	79.86	1816.88	87.84
59	1818.54	78.10	1817.67	85.16	1817.07	
58	1817.41	78.51	1816.91	85.50	1816.69	96.30
57	1817.58	80.28	1817.01	87.84	1816.74	
56	1817.63	85.50	1817.05	96.30	1816.75	
55	1817.50	81.24	1816.97	88.51	1816.72	
54	1818.14	77.84	1817.39	83.07	1816.93	93.29
53	1818.12	78.23	1817.38	83.99	1816.93	96.30
52	1818.50	79.86	1817.64	87.84	1817.05	
51	1818.54	77.05	1817.66	82.49	1817.07	93.29

k \ Δ	3		2		1	
	分散	SN比	分散	SN比	分散	SN比
50	1818.25	82.49	1817.46	91.52	1816.96	
49	1818.23	77.72	1817.46	84.25	1816.97	
48	1817.61	79.31	1817.04	86.30	1816.76	
47	1817.91	78.74	1817.23	83.99	1816.85	93.29
46	1817.49	78.17	1816.96	83.74	1816.72	93.29
45	1818.02	76.66	1817.31	82.32	1816.90	93.29
44	1817.76	77.66	1817.15	83.99	1816.81	96.30
43	1817.82	81.67	1817.17	88.51	1816.82	
42	1817.93	82.87	1817.25	91.52	1816.86	
41	1818.07	78.89	1817.35	86.30	1816.92	
40	1818.34	78.10	1817.53	85.50	1817.00	
39	1817.84	77.78	1817.20	84.53	1816.85	
38	1817.75	79.96	1817.13	85.88	1816.80	96.30
37	1818.04	81.24	1817.33	88.51	1816.90	
36	1818.50	78.51	1817.63	83.74	1817.05	93.29
35	1817.86	77.37	1817.21	83.07	1816.84	93.29
34	1818.05	77.05	1817.34	83.07	1816.91	96.30
33	1818.31	78.23	1817.51	84.25	1816.99	93.29
32	1818.02	77.10	1817.32	83.74	1816.90	96.30
31	1818.23	77.97	1817.46	84.83	1816.96	96.30
30	1818.06	81.67	1817.34	89.31	1816.90	
29	1818.48	79.96	1817.62	85.88	1817.05	96.30
28	1817.32	79.57	1816.85	85.88	1816.66	96.30
27	1818.57	76.25	1817.68	81.52	1817.08	91.52
26	1818.61	79.57	1817.71	87.26	1817.09	
25	1818.78	77.72	1817.84	84.83	1817.16	
24	1818.20	79.39	1817.43	85.50	1816.95	96.30
23	1817.40	78.51	1816.90	84.53	1816.69	96.30
22	1818.14	78.59	1817.41	85.88	1816.94	96.30
21	1817.70	77.10	1817.10	82.68	1816.79	90.28
20	1817.58	79.31	1817.02	85.50	1816.75	96.30
19	1817.95	78.17	1817.27	83.74	1816.87	93.29
18	1818.55	81.38	1817.67	89.31	1817.07	
17	1818.30	80.61	1817.51	88.51	1816.99	
16	1818.13	78.30	1817.39	85.50	1816.93	
15	1817.92	77.16	1817.25	83.29	1816.86	96.30
14	1818.73	78.59	1817.79	84.83	1817.14	96.30
13	1818.12	79.96	1817.38	86.75	1816.93	
12	1817.76	77.49	1817.15	83.07	1816.81	90.28
11	1817.71	78.03	1817.11	83.74	1816.79	93.29
10	1818.23	80.85	1817.45	87.26	1816.96	96.30
9	1818.33	77.10	1817.52	82.87	1817.00	96.30
8	1818.45	79.57	1817.60	85.50	1817.04	96.30
7	1818.22	81.38	1817.44	88.51	1816.96	
6	1817.68	78.03	1817.09	83.74	1816.78	96.30
5	1818.14	81.82	1817.40	89.31	1816.93	
4	1818.85	77.78	1817.87	83.74	1817.17	96.30
3	1818.00	81.67	1817.30	89.31	1816.88	
2	1817.68	81.98	1817.08	89.31	1816.77	
1	1817.63	85.16	1817.04	96.30	1816.75	

5. 鍵の探索時間

鍵の全数探索に必要な時間について検討を行う。UNIX 環境で表 1 に必要なデータ $100 \times 3 = 300$ 個をファイルとして書き出すのに 157 秒かかる。透かしアルゴリズムが同じ環境上で開発されたものとし、符号なしの整数型 (unsigned int) 変数を乱数発生の種類、すなわち鍵として用いているとすれば、鍵は 0 から 65535, Δ は 1 から 5 まで考えなければならない。このとき、 $65536 \times 5 = 327680$ 個の探索が必要となる。

探索時間は単純に、

$$(327680 / 300) \times 157 \approx 171486 \text{ (秒)}$$

つまり、

$$171486 / (60 \times 60) \approx 47.6 \text{ (時間)}$$

と計算される。この時間に鍵推定のための時間を加えたものが鍵の探索に必要な時間となる。

鍵の推定以外は並列化処理が行えるため、複数台のマシンを使いプログラムの高速化を行うことで実用的な時間内で探索が可能となる。

6. おわりに

本稿では、統計量を利用した透かし方式に対して、透かし埋め込みアルゴリズムが既知、または何らかの手段で入手できた場合に透かし画像から鍵を探索することが可能であることを示した。本手法の最大の利点は鍵の探索に原画像を用いていないことにある。つまり、透かし埋め込みアルゴリズムを知ることができれば、通常入手可能な透かし画像から著作権者しか知り得ない鍵情報を得ることができる。このことは、悪意のある者であれば、この知り得た鍵情報をもとに別の画像に対して透かしを埋め込むことや透かしを除去できることを意味している。

暗号システムでは、アルゴリズムを公開した上で鍵のみによって秘密情報の安全性を確保することが議論されている。しかし、電子透かしの多くは、そのアルゴリズムを秘密としている。電子透かしの安全性やユーザーの信頼を得るためにも今後透かしのアルゴリズムを公開することは必須になるものと考えられ、アルゴリズムを公開しても透かし情報の安全性が保てるような電子透かしの開発が望まれている。

今後、さまざまな画像に対して本手法が有効かどうか検証していくつもりである。

参 考 文 献

- 1) 高橋史忠, "電子透かしがマルチメディアを守る", 日経エレクトロニクス, no.683(2月24日号), pp.99-124, Feb 1997.
- 2) 大網亮磨, 宮本義弘, 太田睦, "電子透かしのアタックに対する耐性評価尺度の構築", 情報処理学会第 57 回全国大会講演論文集, 5G-06, 1998.
- 3) W.Bender, D.Gruhl, N.Morimoto: "Techniques for data hiding", Proc.of SPIE, vol.202, pp.2420-2440, 1995.
- 4) 松井甲子雄, "電子透かしの基礎-マルチメディアのニュープロテクト技術", 森北出版, 1998.
- 5) 越昭三, "数理統計学概論", 学術図書出版, 1991.