

相関型電子透かしの誤検出確率保証法における見逃し確率の改善

藤田 高彬[†] 岡本 邦宏^{*†} 吉田 真紀[†] 藤原 融[†]

[†] 大阪大学大学院情報科学研究科
〒565-0871 大阪府吹田市山田丘1-5

E-mail: $\{\{t-fujita@ist,k-okamoto@iff.ics.es,maki-yos@ist,fujiwara@ist\}.osaka-u.ac.jp$

あらまし 電子透かしの検出結果を利用するには、検出誤り確率が十分低いことが望ましい。著者らはこれまでに相関型電子透かし法に共通して満たされ得る性質を導出し、その性質が満たされることを前提条件とした誤検出確率保証法を提案した。その保証法では、透かしの検出を導出した性質に関する仮説検定とみなしている。仮説検定の性質より、本来は標本を大きくすれば誤検出確率を保証したまま、見逃し確率を改善することができる。しかし透かしの検出における仮説検定では、標本を大きくすると誤検出確率が増えてしまい、誤検出確率が保証されない。本稿では、その問題点を解決し、見逃し確率をより低くする誤検出確率保証法を提案する。

キーワード 相関型電子透かし法, 仮説検定, 誤検出確率の保証, 見逃し確率の改善, 閾値選択

Improvement of the False Negative Error Probability for Correlation Based Watermark Detection Ensuring the False Positive Error Probability

Takaaki FUJITA[†], Kunihiro OKAMOTO^{*†}, Maki YOSHIDA[†], and Toru FUJIWARA[†]

[†] Graduate School of Information Science and Technology, Osaka University
Yamadaoka 1-5, Suita-shi, 565-0871 Japan

E-mail: $\{\{t-fujita@ist,k-okamoto@iff.ics.es,maki-yos@ist,fujiwara@ist\}.osaka-u.ac.jp$

Abstract To use results of watermark detection, a detection error probability is required to be low enough. We have derived a property satisfied commonly by correlation based watermarking schemes, and have proposed a method to ensure the false positive error probability for correlation based watermarking scheme. The watermark detection is regarded as a hypothesis testing of the hypothesis on the derived property in the method. In general hypothesis testing, the false negative error probability can be reduced by employing a large sample size while ensuring the false positive error probability. However, in the method, a large sample size causes increase of the false positive error probability, that is, the false positive error probability is not ensured. In this paper, we solve this problem and propose a method to ensure the false positive error probability for correlation based watermarking which reduces the false negative error probability.

Key words correlation based watermarking, hypothesis testing, ensuring false positive error probability, threshold selection

1. はじめに

電子透かし技術は、主としてデジタルコンテンツの著作権を保護するための技術である。例えば、コンテンツに透かしとして購入者情報を埋め込んでおくことで、そのコンテンツの不正コピーが押収されたとき、透かしの抽出あるいは検出するこ

とでコピーの流出元が特定でき、その結果不正コピーを抑止できる。透かしの抽出とは、与えられたコンテンツからそのコンテンツに埋め込まれている透かしを取り出すことである。一方、透かしの検出とは与えられたコンテンツに与えられた透かしが埋め込まれているか否かを判定することである。

コンテンツには、圧縮などの様々な信号処理が加えられる可能性がある。信号処理が加えられることによってコンテンツが変化し、抽出あるいは検出において誤りが起こり得る。誤りは

(注) : 現在、シャープ株式会社所属。

流出元の誤認や見逃しなど深刻な問題に繋がるため、電子透かし法の信頼性を保証するためにも、誤り確率を十分低くすることが重要である。

検出型の電子透かし法に対する信頼性保証は、抽出型の電子透かし法に対する保証にも繋がるため[1]、本稿では、検出型の電子透かし法を対象とする。

検出誤りには、二種類の誤りが存在する。コンテンツに、与えられた透かしが埋め込まれていないにもかかわらず、埋め込まれていると判定する誤り（誤検出）と、埋め込まれていないにもかかわらず、埋め込まれていると判定する誤り（見逃し）である。電子透かし法の信頼性を保証するためにも両方の検出誤りの確率を十分低くすることが重要であるが、一般に、これら二つの誤り確率はトレードオフの関係にある。そこで、流出元の誤認等、より深刻な問題を引き起こす誤検出の確率を指定した確率に十分近くすること（誤検出確率の保証）が求められる[2]。

誤検出確率を保証するために、これまでに多くの研究がなされてきた[3]~[6]。これらの研究では、透かし埋め込み方式を限定した上で、統計理論に基づいて誤検出確率を保証する透かし検出方式を設計している。透かしの検出では、検出対象の透かしとコンテンツから計算される値（検出値）を、閾値と比較することで透かしの有無が判定される。文献[3]~[6]では、透かしの検出を仮説検定とみなし、埋め込みによるコンテンツの変化量に関して妥当と考えられる前提条件をおき、最適な検出を実現する検出値および閾値を計算可能な形で定式化している。なお最適な検出とは、誤検出確率を保証し、その上で見逃し確率を最小とする検出である。このうち、[3]、[4]では透かしに対する攻撃の影響を考慮していないが、[5]、[6]では考慮している。

本研究では、特定の埋め込み方式に対する検出方式ではなく、多くの実用的な電子透かし法に対して共通して適用可能な誤検出確率保証法を提案することを目標とする。設計の際には、攻撃の影響も考慮する。実用的な電子透かし法としてパッチワーク法[11]やそれに基づく様々な方法が提案されている[12]。これらに共通する特徴は、コンテンツと透かしとの相関を強めることで透かしを埋め込み、相関を検出値として用いることである。文献[3]~[6]では、パッチワーク法やそれに基づく方法は扱われていない。相関を利用する電子透かし法を相関型電子透かし法と呼び、[7]~[10]および本稿における誤検出確率保証の対象としている。文献[7]、[8]では、相関型電子透かし法で共通して満たされ得る性質を導出し、その性質が満たされることを前提条件とした誤検出確率保証法を提案した。具体的には、透かしの検出を導出した性質に関する仮説検定とみなし、誤検出確率が保証されるように閾値を選択するアルゴリズムを提案した。さらに、[7]、[8]ではパッチワーク法に対して、[9]、[10]では動画像用の単純な相関型電子透かし法に対して提案した閾値選択アルゴリズムを適用し、誤検出確率が保証されることを実験により確かめた。

一般に仮説検定では、標本を大きくすることによって、第一種の誤りが起こる確率（有意水準）を固定したままで第二種の誤りが起こる確率を小さくすることができる[13]。透かしの検

出を仮説検定とみなした場合、誤検出確率と見逃し確率はそれぞれ第一種の誤りが起こる確率と第二種の誤りが起こる確率に対応する。よって、誤検出確率を指定した確率としたまま見逃し確率を減少させることができる。しかし、[7]、[8]で提案した手法では、検定における標本が小さければ誤検出確率を保証できる閾値を選択できるが、標本を大きくして選択した閾値では、誤検出確率が大きくなる。これは、[7]、[8]では妥当と考えていた前提条件が、標本を大きくした場合に妥当でなかったためと考えられる。

本稿では、前提条件を再検討し、検定における標本を大きくしても誤検出確率が保証されるように閾値選択法を改良する。これによって、誤検出確率を保証したままで見逃し確率を改善することができる。

本稿の章構成を以下に示す。2.では、相関型電子透かし法のモデルと何をもって誤検出確率が保証されたとみなすかを示す。3.では、[7]、[8]で提案した閾値選択法を示す。4.で[7]、[8]の閾値選択法における問題点を考察し、解決方針を述べる。5.で改良した閾値選択法を示す。6.では、改良した閾値選択法の実験評価について示し、最後に7.でまとめと今後の課題について述べる。

2. 相関型電子透かし法

本章では、2.1で相関型電子透かし法のモデルを示し、2.2で誤検出確率の保証について述べる。

2.1 モデル

本稿で対象とする相関型電子透かし法は、以下で示す埋め込みアルゴリズムと検出アルゴリズムからなる。

埋め込みアルゴリズム μ_{embed} : 埋め込みアルゴリズムは、入力として原コンテンツ s と、透かしと対応づけられた鍵 k をとり、透かし入りコンテンツ $x_{s,k}$ を出力する。このとき、

$$x_{s,k} = \text{embed}(s, k)$$

と書く。透かしを embed の入力とする代わりに、透かしと対応付けられた鍵を入力とするため、以降では「透かしが埋め込まれている」という代わりに、「鍵が埋め込まれている」という。埋め込みは、鍵 k と k が埋め込まれたコンテンツ $x_{s,k}$ との相関がある条件を満たすようにコンテンツを変更することで行われる。相関は、コンテンツと鍵から計算される統計量によって評価される。どのような統計量かは、電子透かし法によって異なる。コンテンツ S と鍵 K から計算される統計量を $v(S, K)$ で表す。なお、相関を満たす条件とは $k' \neq k$ を満たす鍵 k' に対し、以下の式(1)および式(2)が十分高い確率で満たされることである。

$$v(s, k) < v(x_{s,k}, k) \quad (1)$$

$$v(x_{s,k}, k') < v(x_{s,k}, k) \quad (2)$$

埋め込みアルゴリズムの例: embed の具体例としてパッチワーク法[11]における埋め込みアルゴリズム embed_p を挙げる。パッチワーク法は、静止画像を対象とした相関型電子透かし法であ

る。パラメータとして透かしの強度 δ 、および変更する画素の組数 N を持つ。以下に $embed_p$ およびパッチワーク法で相関として利用される統計量 v_p を示す。

[埋め込みアルゴリズム $embed_p(s, k)$]

- (1) k を用いて擬似乱系列を生成する。
- (2) この擬似乱系列を用いて s から N 個の画素の組 (a_i, b_i) ($1 \leq i \leq N$) を選択する。
- (3) 全ての i において a_i の輝度値を δ だけ増加させ、 b_i の輝度値を δ だけ減少させる。

[統計量 $v_p(x, k)$]

コンテンツ x の N 個の画素の組 (a_i, b_i) ($1 \leq i \leq N$) を、 $embed_p$ と同じ方法により、 k を用いて選択されたものとする。統計量 $v_p(x, k)$ は次の式によって定義される。

$$v_p(x, k) = \frac{1}{N} \sum_{i=1}^N (a_i - b_i)$$

x に k が埋め込まれていないとき、 $v_p(x, k)$ は 0 を中心に分布し、 x に k が埋め込まれているとき、 $v_p(x, k)$ は 2δ を中心に分布する。

検出アルゴリズム: 検出アルゴリズムは、入力としてコンテンツ x と鍵 k をとり、 x に k が埋め込まれているか否かを判定し、その結果を出力する。パラメータとして閾値 T を持ち、判定は x と k から計算される統計量 $v(x, k)$ を T と比較することで行われる。

- $v(x, k) \leq T$ ならば、 x に k が埋め込まれていないと判定する。
- $v(x, k) > T$ ならば、 x に k が埋め込まれていると判定する。

ここで、「 x に k が埋め込まれていない」とは、 x に k 以外の鍵 k' が埋め込まれているか、あるいは x にかかるといかなる鍵も埋め込まれていないかのどちらかを指す。

文献[3]~[6]と同様に、本稿では透かしが埋め込まれたコンテンツには別の透かしは埋め込まれていないものとする。

2.2 誤検出確率の保証

検出において、検出対象コンテンツ x に鍵 k が埋め込まれていない場合 (事象 H_0 とする) に、「 x に k が埋め込まれている」と判定すると (すなわち閾値 T が $v(x, k)$ より大きければ) 誤検出が起きる。一方、 x に k が埋め込まれている場合 (事象 H_1 とする) に、「 x に k が埋め込まれていない」と判定すると (すなわち閾値 T が $v(x, k)$ 以下であれば) 見逃しが起こる。よって、誤検出確率 $P_{fp,(x,k)}$ および見逃し確率 $P_{fn,(x,k)}$ は、以下のように定義できる。

$$P_{fp,(x,k)} = P(v(x, k) > T | H_0) \quad (3)$$

$$P_{fn,(x,k)} = P(v(x, k) \leq T | H_1) \quad (4)$$

誤検出確率を保証することは、 $P_{fp,(x,k)}$ が指定された確率 (\overline{P}_{fp} と表す) となり、同時に $P_{fn,(x,k)}$ が $1 - \overline{P}_{fp}$ より十分小さな確率となるように閾値 T を選択することである。

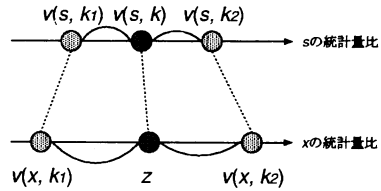


図1 式(5)で定義される値 z

3. 文献[7],[8]における閾値選択法

本章では、[7],[8]で提案した閾値選択アルゴリズムを示す。閾値選択アルゴリズムは、統計量に関して妥当と考えられる前提条件の下で、透かしの検出を仮説検定とみなし、 $P_{fp,(x,k)} = \overline{P}_{fp}$ となるように閾値 T を定める。3.1で、閾値選択における仮説検定について述べ、3.2で、統計量に関する前提条件を述べる。そして3.3では、選択法について述べる。

3.1 閾値選択における仮説検定

検出は、2.2における事象 H_0 を帰無仮説とし、事象 H_1 を対立仮説とする仮説検定とみなされる。すなわち、 H_0 が棄却されれば x に k が埋め込まれていると判定することになる。仮説検定において、誤って帰無仮説を棄却する誤り (第一種の誤り) は、 H_0 が正しい (すなわちコンテンツ x に鍵 k が埋め込まれていない) にもかかわらず、 H_0 を棄却してしまう (x に k が埋め込まれているとする) 誤りであり、検出における誤検出に相当する。第一種の誤りが起こる確率は有意水準に等しいので、有意水準を \overline{P}_{fp} とする有意点を検出の閾値として選択することで誤検出確率を保証できる。

本研究では、 x に k が埋め込まれていないときに満たされる性質 (P) を導出し、 H_0 および H_1 としてそれぞれ以下の仮説 H'_0 および H'_1 を用いる。

- H'_0 : (P) が満たされる
- H'_1 : (P) が満たされない

すなわち、検出を性質 (P) に関する仮説検定とみなす。本来、性質 (P) として、様々な種類の攻撃を受けたとしても x に k が埋め込まれていないとき、かつそのときに限り満たされる性質を導出し、仮説検定を行うことが理想である。しかし、そのような性質を導出し仮説検定を行うことは難しいと考えられる。よって、 x に k が埋め込まれていないときに満たされる性質を導出し、代わりに利用する。

3.2 前提条件

文献[7],[8]で導出され前提とされている条件を示す。ここでコンテンツ x および鍵 k に対して、確率変数 k_1 と k_2 は値として $k_1 \neq k_2$, $k_1 \neq k$, $k_2 \neq k$ となる鍵を取るものとし、確率変数 z を式(5)によって定義されるものとする。

$$\frac{z - v(x, k_1)}{v(x, k_2) - v(x, k_1)} = \frac{v(s, k) - v(s, k_1)}{v(s, k_2) - v(s, k_1)} \quad (5)$$

ただし、 s は x の原コンテンツとする。式(5)の意味を直観的に図で表すと、図1のようになる。

文献[8]では、コンテンツとして静止画像 *Lena*、埋め込み方式としてパッチワーク法の $embed_p$ 、攻撃として JPEG 圧縮・伸長を用いた場合、 z は正規分布に従い、 x に k が埋め込まれていないとき、 z の平均 μ は $v(x, k)$ に十分近い値となることが実験的に確認されている。

そこで、[7],[8]では、前提条件として、 x に k が埋め込まれていないとき、次の性質 (P) が満たされることを採用している。

(P) z の平均を μ としたとき、 $v(x, k) = \mu$

3.3 文献[7],[8]における閾値選択法

文献[7],[8]の閾値選択法では、3.2で示した性質 (P) に基づき、コンテンツ x に対して鍵 k で検出する際、 H_0' および H_1' としてそれぞれ以下の H_0'' および H_1'' を用いる。

- H_0'' : $v(x, k) = \mu$
- H_1'' : $v(x, k) > \mu$

H_1'' が両側対立仮説 ($v(x, k) \neq \mu$) でない理由は、 x に k が埋め込まれているとき $v(x, k)$ は大きいと考えられるためである。そのため、 x に対する k の検出は片側検定となる。ここで z の母分散が未知であることにより、検定は t -検定となる。閾値選択法は、パラメータとして検定における標本の大きさ A を持つ。標本の大きさは標本数ともいわれる。

閾値選択の具体的な手順は次の通りである。

(1) 原コンテンツ s と x, k 、ランダムに選択した鍵ペア (k_1, k_2) によって式 (5) から z の標本 \tilde{v} を A 個求める。ここで A は標本の大きさである。

(2) 標本 $\tilde{v}_i (1 \leq i \leq A)$ の平均 $\bar{\mu}$ を次の式によって求める。

$$\bar{\mu} = \frac{1}{A} \sum_{i=1}^A \tilde{v}_i$$

(3) 標本 $\tilde{v}_i (1 \leq i \leq A)$ の分散 $\hat{\sigma}^2$ を次の式によって求める。

$$\hat{\sigma}^2 = \frac{1}{A-1} \sum_{i=1}^A (\tilde{v}_i - \bar{\mu})^2$$

(4) Z を自由度 $A-1$ の t -分布に従う確率変数とし、 $g(Z)$ を Z の確率密度関数とする。このとき以下を満たす M を計算する。

$$\int_M^\infty g(Z) dZ = \overline{P_p}$$

(5) 閾値 T を以下の式で計算する。

$$T = \bar{\mu} + M \frac{\hat{\sigma}}{\sqrt{A}} \quad (6)$$

4. 文献[7],[8]における閾値選択法の問題点

一般に仮説検定では標本を大きくすることによって、第一種の誤りが起こる確率 (有意水準) を固定したままで第二種の誤りが起こる確率を小さくすることができる。すなわち、誤検出確率を保証したままで見逃し確率を下げるように閾値を選択することができる。しかし、[7],[8]における閾値選択法では、図2

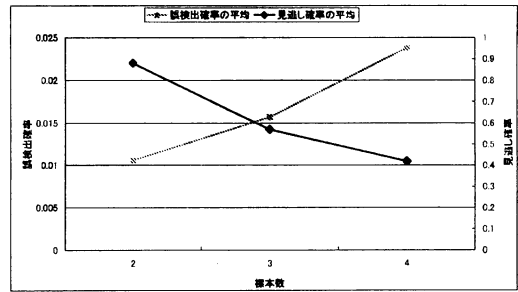


図2 文献[7],[8]の閾値選択法を適用したときの誤検出確率と見逃し確率

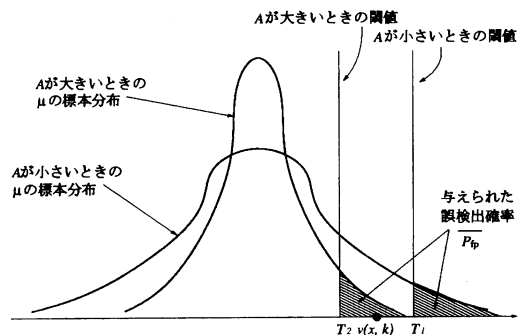


図3 標本の大きさ A を大きくした場合に誤検出確率が增大する理由

のグラフで示すように、パラメータである標本の大きさ A を大きくすると誤検出確率が增大してしまう。本章ではその問題点を考察し、解決方針を示す。

文献[7],[8]では3.3で述べた式 (6) に示すように、閾値 T を μ の標本分布をもとに選択している。 μ は、式 (5) で計算される z の平均である。標本の大きさ A を大きくすることで μ の標本分布の分散が小さくなり、閾値が小さくなる。文献[8]で、 x に k が埋め込まれていないとき $v(x, k)$ は μ に近い値であることが実験的に確かめられている。しかし、近い値であるため $v(x, k) > \mu$ となることがある。そのような x, k に対して、 A を小さくして選択した閾値で検出を行うと、 x に k が埋め込まれていないと判定され、 A を大きくして選択した閾値で検出を行うと、埋め込まれていると判定される。これは、図3で示すように、 A が小さいときは閾値が $v(x, k)$ より大きく選ばれていたが (図中の T_1)、 A を大きくすることで閾値が $v(x, k)$ より小さく (ただし μ より大きく) 選ばれてしまうためである (図中の T_2)。そのため、 A を大きくすると誤検出確率が増大したと考えられる。よって、 x に k が埋め込まれていないときに満たされる性質 (P) として「 $v(x, k) = \mu$ 」を用いる代わりに、「 $v(x, k)$ は μ に近い」を用いるべきである。 $v(x, k)$ が z の平均である μ に近いと判定する妥当な基準として z の標準偏差が考えられる。

5. 提案する閾値選択法

z の標本分布に対する $v(x, k)$ の値を見ると、 x に k が埋め込

表 1 x に k が埋め込まれていないとき, $v(x, k) < \bar{\mu} + \alpha\bar{\sigma}$ となる $v(x, k)$ の個数 (α は定数, z の標本の大きさ A は 4)

α の値	0	0.5	1	1.5	2
$v(x, k)$ の個数 (10,000 個中)	3808	6644	9018	9600	9819

まれていないとき, ほとんどの $v(x, k)$ において $v(x, k) \leq \bar{\mu} + \bar{\sigma}$ ($\bar{\mu}$ は z の標本平均, $\bar{\sigma}$ は z の標本標準偏差) であった (表 1 参照). そこで, 性質 (P) として $v(x, k) \leq \mu + \bar{\sigma}$ を用いる. $\bar{\sigma}$ を σ の代わりに用いるのは, z の標準偏差である σ が不明であるためである.

本稿で提案する閾値選択法では, コンテンツ x に鍵 k が埋め込まれていないときに満たされる性質として $v(x, k) \leq \mu + \bar{\sigma}$ を用いる. ここで, $\bar{\sigma}$ は z の標本標準偏差である. すなわち, 3.3 で示した仮説検定における H_0'' および H_1'' を, それぞれ仮説 H_0''' および H_1''' とする仮説検定によって閾値を選択する.

- H_0''' : $v(x, k) = \mu + \bar{\sigma}$
- H_1''' : $v(x, k) > \mu + \bar{\sigma}$

具体的には, 3.3 で示した手順において手順 5 を次の手順 5' に変更する.

(5') 閾値 T を以下の式で計算する.

$$T = \bar{\mu} + M \frac{\bar{\sigma}}{\sqrt{A}} + \bar{\sigma}$$

この改良によって, 実際に標本の大きさ A を大きくしたとしても誤検出確率が保証される閾値が選択できることを, 次章で述べる実験により確かめた. すなわち, 誤検出確率を保証したままで見逃し確率を改善することができたことを確かめた.

6. 実験評価

5. で示した閾値選択法によって誤検出確率が保証されたまま見逃し確率が [7], [8] の閾値選択法より小さくなることを実験により確かめる. 本章では, 6.1 で実験の閾値選択法を, 6.2 で実験方法を述べ, 6.3 でその結果を示す.

6.1 実験の閾値選択法

閾値選択における帰無仮説 H_0''' を $v(x, k) = \mu + \alpha\bar{\sigma}$ (α は正の定数) とし, 対立仮説 H_1''' を $v(x, k) > \mu + \alpha\bar{\sigma}$ とする. そして α として, 0, 0.5, 1, 1.5, 2 を選択する. $\alpha = 1$ のとき, 5. で提案した閾値選択法となる. また, $\alpha = 0$ のとき, [7], [8] の閾値選択法となる. $\alpha = 0.5, 1.5, 2$ に対しても実験を行うのは, $\alpha \neq 1$ ならば誤検出確率がどの程度保証されないかあるいは, 見逃し確率がどの程度大きくなるかを調べるためである.

6.2 実験概要

まず, 実験の条件を示す. 標本の大きさ以外の条件は, [9], [10] で [7], [8] の閾値選択法を評価する際に用いた条件と同じである. 標本の大きさ A : 標本の大きさ A として, 2, 3, 4, 8 を用いた. なお, 4. で述べたように [7], [8] の閾値選択法では, 誤検出確率が保証できる閾値を選ぶことができるのは $A = 2$ のときだけであったため, [9], [10] では $A = 2$ に対してのみ評価実験をしていた.

指定した誤検出確率 $\overline{P}_{fp} = 0.01$ とした.

相関型電子透かし法: 動画用の単純な相関型電子透かし法を

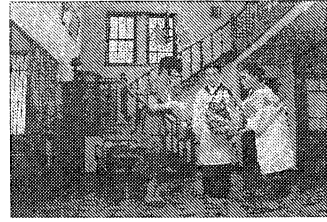


図 4 Entrance Hall における一フレーム

適用対象とした. この電子透かし法は, 動画像中の一枚のフレームに対して静止画像用の相関型電子透かし法をそのまま適用するものである. 静止画像用の相関型電子透かし法としてパッチワーク法 $embed_p$ を用いた. パッチワーク法のパラメータは $\delta = 3, N = 10,000$ とした. これらの値は, 透かしを埋め込むフレームの品質を保ち, かつその上で前提条件が高い確率で満たされるのに十分であると考えられる [11]. 本稿で提案した閾値選択法は [7], [8] と同様に出検対象コンテンツの原コンテンツを必要とするが, [9] で示した動画像への適用法に従うことで, 原コンテンツなしで閾値を選択できる. 詳細は, 実験手順の (3) で述べる.

鍵: 32 ビットの整数とした.

原動画像: 原動画像として, 映像情報メディア学会^(注1)の標準動画像の一つである Entrance Hall (図 4 参照) を用いた. この動画像は, 720×486 ピクセルのフレーム 450 枚で構成される.

画像への攻撃: ビットレートが 5Mbps の MPEG 圧縮・伸長を用いた. MPEG 圧縮・伸長には, mpeg2encode と mpeg2decode (MPEG Software Simulation Group^(注2)) を用いた.

次に, 実験手順を示す. 以下では, 動画像 x における t 番目のフレームを $x^{(t)}$ と表す.

各 α および A に対して以下を行う.

(1) 埋め込み鍵 k' と検出鍵 k としてそれぞれ 10 個と 30 個の整数をランダムに選択する.

(2) 各 k' に対して以下の (a) および (b) を行う.

(a) $embed_p$ を用いて原動画像 s 中の一枚のフレーム $s^{(r_{k'})}$ に k' を埋め込み, 透かし入り動画像 $x_{s, k'}$ を生成する. ここで $r_{k'}$ は, 擬似乱数生成器より k' を用いて生成した乱数である.

(b) $x_{s, k'}$ に攻撃である MPEG 圧縮・伸長 (p で表す) を加え, 動画像 $p(x_{s, k'})$ を生成する

(3) 各 k, k' に対して, 誤検出確率が \overline{P}_{fp} となるように閾値を選択し, 検出を行う. このとき, [9], [10] と同様, 検出対象フレーム $p(x_{s, k'})^{(r_k)}$ に隣接するフレームを原フレーム $s^{(r'_k)}$ の代わりに用いる.

6.3 実験結果

実験結果を図 5, 図 6 に示す. これらの図より, $\alpha = 1$ のとき, すなわち 5. で提案した閾値選択法を用いて検出を行うと, 標本の大きさ A を大きくすることで, 誤検出確率を保証しつ

(注1): <http://www.ite.or.jp/>

(注2): <http://www.mpeg.org/MPEG/MSSG/>

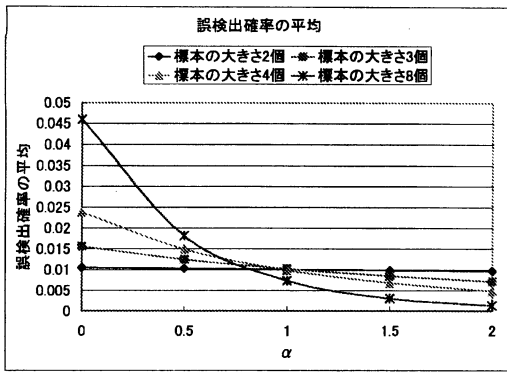


図5 実験結果: 誤検出確率の平均

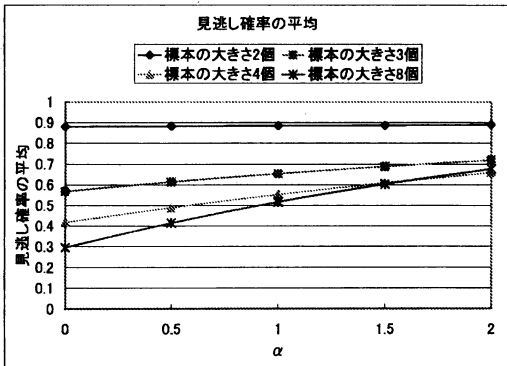


図6 実験結果: 見逃し確率の平均

つ見逃し確率を従来の閾値選択法 ($\alpha = 0, A = 2$) より小さくできることが確かめられた。具体的には、見逃し確率の平均が0.8から0.5に改善されている。一方、 $0 < \alpha < 1$ のときは誤検出確率が保証されず、 $1 < \alpha$ のときは $\alpha = 1$ のときより見逃し確率が大きくなる。例えば $A = 4$ のとき、 $\alpha = 1$ のときの誤検出確率は0.01であるのに対して、 $\alpha = 0.5$ のときは0.015となる。また $\alpha = 1$ のときの見逃し確率は0.55であるのに対して、 $\alpha = 2$ のときは0.65となる

なお、いずれの場合も見逃し確率が0.3以上と大きい。これは、本実験で用いた電子透かし法が輝度値を変化させる単純な方法であり、攻撃への耐性が低かったためと考えられる。周波数成分へ透かしを埋め込む電子透かし法など、より耐性のある電子透かし法に閾値選択法を適用すれば、見逃し確率が小さくとなると考えられる。

7. まとめと今後の課題

本稿では、[7],[8]で提案した閾値選択法における問題点を考察し、閾値選択の際の標本を大きくしても誤検出確率が保証されるように閾値選択法を改良した。これにより、誤検出確率が保証されたまま見逃し確率を改善することが可能となった。また、実際に見逃し確率が改善されることを実験により確かめた。

今後の課題として、 $\alpha = 0.9$ や $\alpha = 1.1$ など $\alpha = 1$ に近い値とした閾値選択法についても検討することが考えられる。また、

より低い誤検出確率を指定した場合の誤検出確率および見逃し確率の評価、パッチワーク法以外の相関型電子透かし法に対して、提案した誤検出確率保証法を適用した場合の誤検出確率および見逃し確率の評価が考えられる。

文 献

- [1] Z. Li, S. Kwong, M. Choy, W.W. Xiao, J. Zhen, J.H. Zhang, "An Intelligent Watermark Detection Decoder Based on Independent Component Analysis," IWDW2003, pp.223-234, 2003.
- [2] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "Threshold Selection for Correlation-Based Watermark Detection," Proc. COST254 Workshop, pp.67-72, 1998.
- [3] Y. Hu, S. Kwong, and Y.K. Chen, "The Design and Application of DWT-Domain Optimum Decoders," Digital Watermarking, LNCS2613, pp.22-30, 2003.
- [4] Q. Chen and T.S. Huang, "An Additive Approach to Transform-Domain Information Hiding and Optimum Detection Structure," IEEE Trans. Multimedia, vol.3, no.3, pp.273-284, 2001.
- [5] Y. Shao, G. Wu, and X. Lin, "Optimal Detection of Transform Domain Additive Watermark by Using Low Density Diversity," Digital Watermarking, LNCS2613, pp.105-112, 2003.
- [6] Q. Chen and T.S. Huang, "Robust Optimum Detection of Transform Domain Multiplicative Watermarks," IEEE Trans. Signal Processing, vol.51, no.4, pp.906-924, 2003.
- [7] 岡本 邦宏, 上野 貴之, 吉田 真紀, 藤原 融, "統計量利用型電子透かしに対する検出結果の信頼性保証," SCIS2004 予稿集, pp.879-884, 2004.
- [8] K. Okamoto, T. Ueno, M. Yoshida, and T. Fujiwara, "A Method to Ensure Reliability of a Detection Result for Correlation Based Watermark Detection Scheme," Proc. ISITA2004, pp.299-304, 2004.
- [9] K. Okamoto, T. Fujita, M. Yoshida, and T. Fujiwara, "Correlation Based Watermark Detection Ensuring Given False Positive Error Probability for Video Using Inter-Frame Similarity," CSS2004 論文集, pp.163-168, 2004.
- [10] 藤田 高彬, 岡本 邦宏, 吉田 真紀, 藤原 融, "動画像用相関型電子透かしの誤検出確率を保証可能とするフレーム間類似度の評価," SCIS2005 予稿集, pp.1033-1038, 2005.
- [11] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM System Journal vol.35, No.3&4, pp.313-316, 1996.
- [12] N. Cvejic and I. Tujkovic, "Increasing Robustness of Patchwork Audio Watermarking Algorithm Using Attack Characterization," Proc. 2004 IEEE International Symposium on Consumer Electronics, pp.3-6, 2004.
- [13] 東京大学教養学部統計学教室, 統計学入門 基礎統計学 I, 東京大学出版会, 東京, 1991.