局所記述子に基づく幾何学的変換にロバストな画像著作権保護

横田　哲†　黄瀬　浩一††　岩村　雅一††　汐崎　陽††

† 大阪府立大学大学院工学研究科
〒 599-8531 大阪府堺市学園町 1-1
E-mail: †yokota@m.cs.osakafu-u.ac.jp, ††{kise,masa,shiozaki}@cs.osakafu-u.ac.jp

あらまし　近年，インターネット上でコンテンツの不正コピーによる著作権の侵害が社会的な問題となっている．著作権侵害の防止策としては，電子透かしというデジタルコンテンツに著作権情報を埋め込む技術がある．しかし画像に関して言えば，画像を改竄し，埋め込まれた情報を取り出せなくしてしまう攻撃 (Stirmark 攻撃など) がある．特に，近年，幾何学的変換への耐性が問題となっている．本稿では，この問題を解決するため，画像の局所記述子を用いた新しい電子透かし法を提案する．画像の局所記述子は，幾何学的変換に影響を受けにくいという特性があるため，従来の問題点を解決できる可能性がある．本手法の特徴は，ノンブラインド型の電子透かし法であるため，局所記述子で定められる，画像の局所領域に順序をつけて，電子透かし情報を埋め込める点にある．これにより，透かし情報の容量を増加させることが可能となる．実験では，Stirmark 攻撃を受けた画像から，正しく局所領域を連結して透かし情報が読み出せるかどうかを検証する．

キーワード　著作権，電子透かし，Stirmark，ノンブラインド，SIFT

Document Image Retrieval Based on Cross-Ratio and Hashing

Satoshi YOKOTA†, Koichi KISE††, Masa IWAMURA††, and Akira SHIOZAKI††

† Graduate School of Engineering, Osaka Prefecture University
Gakuen-cho 1-1, Sakai, Osaka, 599-8531 Japan
E-mail: †yokota@m.cs.osakafu-u.ac.jp, ††{kise,masa,shiozaki}@cs.osakafu-u.ac.jp

Abstract　In recent years, illegal copies on the Internet have become a serious social problem. As a method of copyright protection, digital watermarking is a well-known mean which embeds copyright information to digital contents to be protected. However, for the case of digital still images, for example, there exist image falsification attacks (e.g., Stirmark) which change images to make it difficult to read the embedded copyright information. In particular, robustness against geometric transformation becomes an important issue. In this paper, we propose a method for solving this problem by using “local descriptors” of images. Local descriptors have a property insensitive to geometric transformation, they have a potential to solve the problem. The characteristic feature of the proposed method is that it can sequence local regions defined by local descriptors for embedding information. This indicates that the amount of information increases as compared to independent embedment on each local region. From the experimental results, we show that the sequence of local regions can be correctly read and embedded information can be successfully decoded from most of images that undergo the Stirmark attack.

Key words　Copyright, Digital watermark, Stirmark attack, Non-blind, SIFT

1. ま え が き

近年，パソコンの高機能化により誰でも個人規模で音声，画像，動画などのデジタルコンテンツを扱えるようになった．しかし，技術の発展は便利な反面，多くの問題を生んでいる．その一つがコンテンツの不正コピーによる著作権の侵害である．以下，本研究ではとりわけ画像の著作権保護に焦点をあてて述べる．

防止策の一つとして，電子透かし [1] という技術がある．この技術は画像に対して著作権情報を埋め込み，必要な時に検出し，著作権の主張を可能にするものである．

しかし，問題点として埋め込んだ著作権を無効化する技術の存在が挙げられる．その代表的なものとして Stirmark 攻撃 [2] と呼ばれるものがある．Stirmark 攻撃とは人の目に知覚できな

い範囲で画像に変化を加えるものである．Stirmark 攻撃を受けると画像が改竄され，埋め込んだ電子透かしが取り出せなくなり，著作権を主張する証拠を失ってしまう．原因としては，電子透かしが Stirmark 攻撃で加えられる画像変換，とりわけ幾何学的な変換やクロップ変換に弱いということが挙げられる．

この問題に対処するため，近年，画像認識の分野で開発された技術を応用した電子透かしの手法がいくつか提案されている [3]〜[5]．これらの手法は，局所記述子 (local descriptor) を画像から多数抽出し，各々に対応する局所領域に電子透かしを埋め込むものである．局所記述子は，一般に幾何学的変換にあまり影響を受けずに抽出できることに加え，局所領域への埋め込みであるため，クロップ変換で破壊される可能性が低いという利点も得ることができる．しかしながら，従来の電子透かしの手法に比べて，Stirmark などの攻撃に対する耐性が十分検証されていない，すべての局所領域に同じデータを埋め込むため，透かしとして埋め込める情報の容量に限界がある，などの問題点も存在する．

本研究では，このような問題点を解決する試みとして，局所記述子を用いた新しい電子透かし法を提案する．提案手法が従来法と最も大きく異なる点は，従来法がブラインド型の電子透かし，すなわち，電子透かしを読み出すのに原画像を必要としないのに対して，提案手法はノンブラインド型，すなわち原画像を用いる点にある．

一般に，ノンブラインド型の電子透かしはブラインド型のものに比べて，透かしの読み出し時に比較対象となる原画像を参照できるため，ロバスト性や容量の点で有利である．一方で，原画像データベースの中から，どの原画像を参照すべきかを決めるための検索のオーバーヘッドが存在するという問題点もある．この問題点に関して，我々は既に大量の画像の中から高速かつ高精度に原画像を検索する枠組みを提案している [6]．この手法では，Stirmark やクロップなどの画像変換を受けた画像をキーとして，1 万画像のデータベースから原画像を 200 ミリ秒程度で探し出すことができるものである．検索精度も 99.5%が得られていることから，ノンブラインド型の大きな問題点は解決されつつあるといえる．

本稿では，上記の結果を受けて，実際にノンブラインド型で電子透かしを埋め込む一手法を提案する．提案手法の特徴は，ノンブラインド型の特徴を活かして，複数の局所領域を順序付けて，透かし情報を埋め込むことにより，単独で用いる場合に比べて容量や精度を増加させる点にある．局所領域の順序，すなわち，どの順番でどの領域からデータを読み出せば正しく復号できるのかについては，原画像のデータベースに記録しておく．また，埋め込みに用いる領域とそれ以外の領域の区別も記録しておき，読み取り時の精度を向上させる．

個々の局所領域に電子透かしを埋め込む手法として，現在，本手法が用いているものはプリミティブであるため，実現されている容量はそれほど大きくないものの，従来法 (例えば, [4]) と同様の方式を用いることにより増加させることが可能であると考えられる．

2. 電子透かし

電子透かしとは，デジタル画像の不正な複製を防止するために，著作権情報などを埋め込み, 必要に応じて検出する技術である．

電子透かしの持つべき性質は大きく分けて２つ考えられる．１つは埋め込んだ画像の視覚的劣化が少ないことであり，もう１つは知覚出来ない程度の改竄によって埋め込み情報を除去をされないことである．

埋め込みは多くの場合，画像の画素値を書き換えることで行われる．そして検出は埋め込み方に応じて，画素値の書き換えを認識することで行われる．画素値の書き換えを顕著に行えば，それに伴いより画像の改竄にロバストな埋め込みが可能である．しかし一方，埋め込み自体が画像を劣化させてしまう結果となる．よって，埋め込みの強度と視覚的劣化のつり合いをとる必要がある．

電子透かしには大別してブラインド型，ノンブラインド型がある．ブラインド型は電子透かしを検出する際に原画像を必要としない方式である．利点は，著作者以外が原画像を所有せずに済むことである．一方ノンブラインド型は原画像を必要とするため，電子透かしを埋め込む際に原画像の情報を所有する必要がある．利点は，原画像の情報を利用することでより高度な埋め込み及び検出が可能となる点である．

このうち，近年の主流の手法はブラインド型である．これは，ノンブラインド型のように，参照する原画像を保存・検索せずに済むため，利便性が高いことが理由である．また，共通する大きな問題点として，著作権侵害目的の改竄に多く見られる幾何学的変換やクロップ変換に弱いということが挙げられる．その改竄の代表的な手法として，次章に述べる Stirmark 攻撃がある．

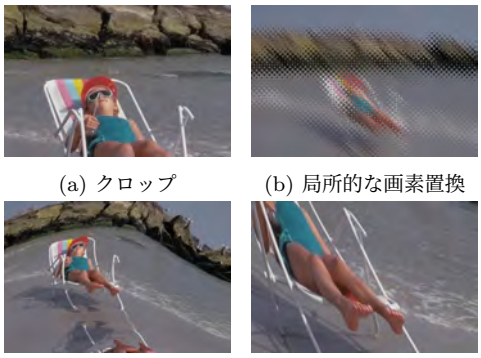
3. Stirmark 攻撃

Stirmark 攻撃は画像を改竄するフリーツールであり，電子透かしの耐性を評価するために用いられている．この改竄により，画像はある閾値の範囲でランダムに回転・拡大・縮小・線形変換などの混合変換が施され，画素値が変更される．その結果，埋め込んだ情報の検出が困難となる．

図 1 に原版を示し，Stirmark 攻撃で用いられる画像処理の例を図 2 に示す．なお，図 2 では分かりやすくするために大幅な変化を与えているが，クロップを除けば，実際には変化は知覚出来ない範囲に留まる．図 3 に Stirmark 攻撃と電子透かしの関係を示す．著作権情報はＡ社が著作権を有している画像をＢさんが購入したということを示すものである．図 3 は，Stirmark 攻撃前には正しく検出されていた著作権情報が攻撃後に検出されなくなったことを示している．

この様に電子透かしは Stirmark 攻撃により無効化されてしまう．混合変換のなかでも，回転・クロップ変換などの幾何学的変換にとりわけ弱いことが知られている．以上のことを考慮して次の章で提案手法について述べる．

図 1　原　　版



(a) クロップ　　(b) 局所的な画素置換

(c) コーナーシフト　　(d) センターシフト

図 2　Stirmark 攻撃の多様な処理

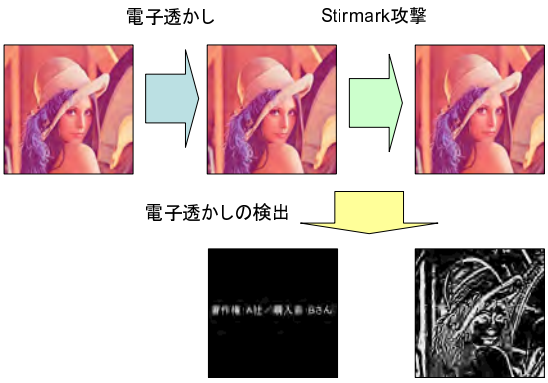


図 3　Stirmark 攻撃と電子透かし検出

4. 提 案 手 法

4.1 考　え　方

本稿では，幾何学的変換に耐性のある電子透かし法を提案する．

第一の着眼点は，画像認識の分野で提案されている局所記述子を電子透かしに導入する点にある．局所記述子とは，そもそも画像認識を安定的に行うために開発された画像の記述子である．一般に画像認識においては，認識対象となる物体が斜めから撮影されるなど幾何学的変換を被ることや，隠れなどのために一部分しか画像に含まれないという状況が通常である．この問題に対処するため，局所記述子は，幾何学的変換に対してほぼ不変な特徴量を抽出するものとなっており，画像の局所領域の特徴を記述することによって，部分的な撮影に対してもロバスト性を得ている．

この技術を電子透かしに導入し，局所領域に透かし情報を埋め込むと，著作権保護対象の画像が幾何学的変換を受けても安定して取り出せ，かつクロップにも高いロバスト性が得られると期待できる．数は少ないながら，これまでにもいくつか，そのような手法は提案され [3]〜[5]，有効性が検証されつつある．

第二の着眼点は，上記の局所領域に基づく電子透かし法の問題点を解決するためのものである．上記の手法は基本的にブラインド型の手法であるため，処理の基本は，画像から抽出した個々の局所領域を一つの「画像」として捉え，透かし情報を埋め込むものである．一般に画像からは多数の局所領域が得られるが，それらには基本的に同じ情報が埋め込まれる．読み出し時には同じ情報を何度も取得することによって，局所領域の抽出誤りや電子透かしの読み出し誤りに対処している．局所記述子を用いない手法では，画像全体に透かし情報を埋め込めるため，比較的多くの情報量を，人間には知覚されにくい形で埋め込むことが可能である．一方，局所領域を用いる手法では，元の画像サイズにもよるが 1 辺が数十画素程度の局所領域に情報を埋め込むため，埋め込める容量に限界が生じる．

本手法では，この問題点を解決するため，複数の局所領域に順序を付けて，それらに一連の情報を埋め込むことを考える．このような手法を可能とするためには，局所領域の順序を正しく復元することが求められる．方法としては種々考えられるが，提案手法では，情報を埋め込む際に定めた順序をデータベースに記録しておき，それを読み出し時に用いることを考える．このような手法は，電子透かしを読み出す際に原画像（から得られた情報）を参照するため，ノンブラインド型の電子透かしといえる．具体的には原画像から局所記述子を抽出した際に，それを埋め込みに用いるか否か，用いる場合には何番目の情報を埋め込むのかを原画像のデータベースに合わせて記録しておき，読み出しに利用する．本手法では，このような方式により，容量の問題点の解決を図る．

4.2 処理の流れ

処理の流れを図 4 に示す．処理は，埋め込み・検索・検出の 3 つのステップからなる．

本手法では，まず保護したい画像（以下，原画像）群の局所記述子をデータベースに登録しておく．次に，著作者は原画像に電子透かしを埋め込み販売する．この画像が Stirmark などの画像変換を経た後に，インターネット上にアップロードされることを考える．インターネット上で著作権侵害の可能性のある画像（以下，被疑画像）は，原画像のデータベースとの照合によって発見される．データベースとの照合は，局所記述子を単位として行われるため，照合の結果として，被疑画像の局所記述子と原画像の局所記述子の対応が得られる．その結果，各々の局所記述子に対応付けられた局所領域同士を比較することが可能となり，電子透かしを読み出すことができる．また，原画像の局所記述子には，埋め込みの際の順序が記述されているため，読み出した透かし情報を正しい順序に並べ替えることができる．

以上が提案手法の概要である．次節以降では，この提案システムを実現させるための技術について述べていく．

4.3 特徴量抽出

処理の詳細について述べる前に，まず，提案手法で用いる局所記述子について述べる．

ステップ 1 の埋め込みは，画像認識分野で用いられる局所記

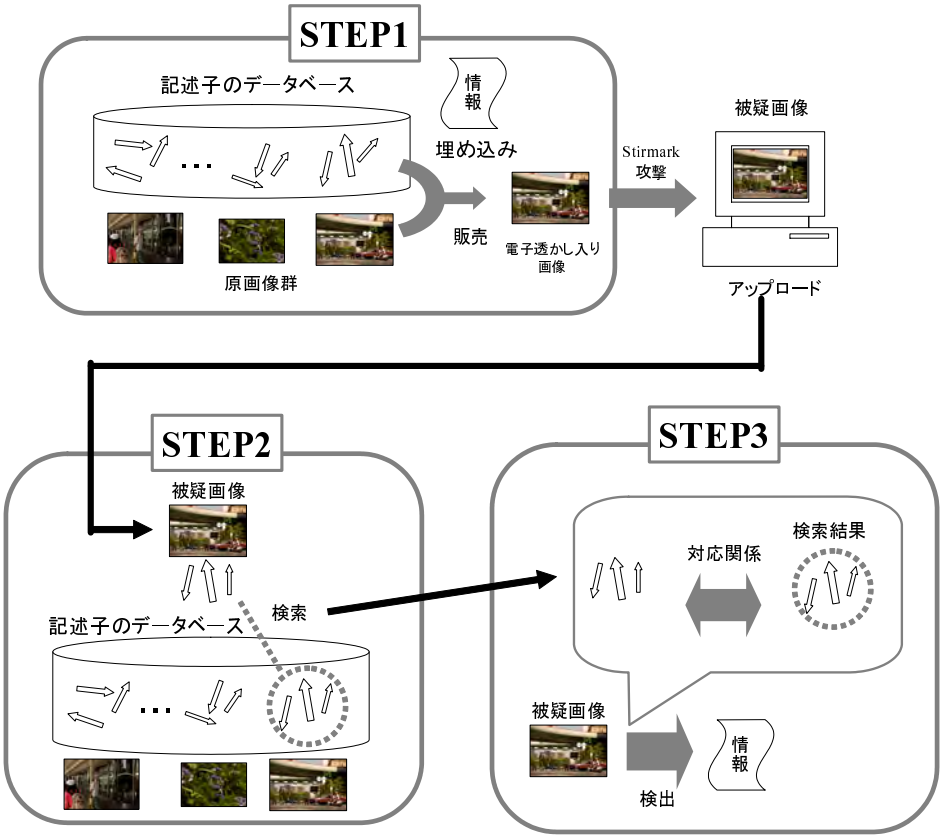


図 4　処理の流れ

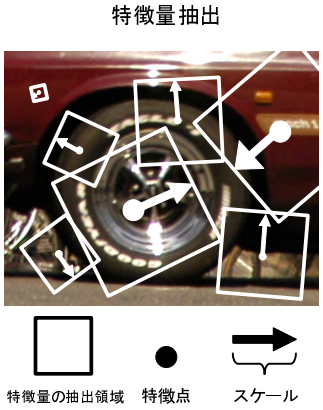


図 5　特徴量抽出

述子に基づき行う．画像認識の分野では，これまで多数の局所記述子が提案されているが，本手法では，その中でも，画像の回転や拡大縮小などの相似変換に不変な記述子である，PCA-SIFT [7] を用いる．PCA-SIFT は，図 5 に模式的に示すように，画像の輝度変化から特徴点を抽出し，スケールと方向を決定し，スケールに応じて周辺領域の輝度から抽出した特徴量を計算するものである．特徴点のスケールと方向は，画像の大きさや回転角度が変化しても，安定的に求められるため，それらによって定まる局所領域 (正方形) は相似変換に不変となる．

4.4　埋め込み

次に，電子透かしの埋め込み方法について述べる．図 5 に示すように，一般に PCA-SIFT の局所領域としては，様々な大きさの領域が多数抽出される．これらはすべて電子透かしの埋め込みに用いることができるわけではなく，以下の条件を満たす必要がある．

（1）　Stirmark 攻撃を受けた後でも，安定して取り出せること

（2）　透かし情報を埋め込むのに十分な大きさと数があること

（3）　領域が互いに重ならないこと

上記の (1) と (2) の条件を満たす領域を確認するため，Stirmark 攻撃を加えた画像を用いて予備実験を行った．その結果，比較的面積の大きい局所領域は Stirmark 攻撃を加えた後でも安定して取り出せるのに対して，面積の小さな領域は安定性に欠けることが分かった．また，面積の小さい領域は，画像が縮小された場合にも取り出せなくなる可能性が高いため，好ましくない．そこで本手法では，面積が大きな領域から上位 N 個を埋め込みに用いることにする．

次に上記の条件 (3) について述べる．互いの領域が重なるものに対して，透かし情報を埋め込もうとすると，一方に埋め込んだ後，他方によって上書きするような形になってしまい，先に埋め込んだ情報が破壊されてしまうという問題がある．特に大きな領域であればそれだけ，互いに重なり合う可能性が高い．この問題点を解決するため，本手法では，PCA-SIFT によって定められた局所領域のうち，一部分を用いて透かし情報を埋め込むことを考える．具体的には，図 6 に示すように，特徴点を

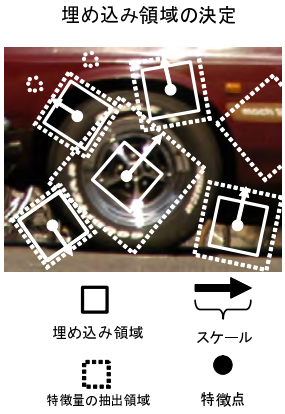


図 6　埋め込み領域

重心に持ち，局所領域と同じ辺の向きを持ちつつ，一辺の長さを M 画素に縮小した領域を考える．このように埋め込み領域を縮小することによって，互いに重なり合わないように領域を確保する．縮小した領域同士が重なる場合には，元の領域の面積が大きい方を優先して使用する．

最後に埋め込み方法について述べる．

上記の方法により埋め込み領域が得られたとする．個々の領域への埋め込みは，領域の RGB の平均画素を増減させることにより行う．情報量は RGB それぞれに増加させることでビット “1” を，減少させることでビット “0” を埋め込む．従って，局所領域あたりの埋め込みビット数は 3 ビットとなる．領域内の画素値を増加させるには $-B$ から A の一様乱数を加え，逆に減少させるには減ずる．

このような方法によって，合計で $3L$ ビットを埋め込むためには，L 個の局所領域を順序付けた上で 1 セットとして扱う必要がある．一般に，画像から得られる局所領域は L 個より多く設定できる．いま，その数を $LP(=N)$ 個とすると，局所領域には同じデータを P 回，繰り返して記録することになる．これによって，読み出しに失敗した場合やクロップへの対処が可能となる．

埋め込みに際しては，埋め込みに用いたか否か，また，局所領域の順序 $j(1 \leqq j \leqq L)$ を記録しておく．

具体的に例を挙げて説明する．今，著作権を保護したい画像に 9 ビット 111,101,000 の情報を埋め込むとする．そして，PCA-SIFT によって，図 7 左に示す 12 個の局所領域が得られたとする．埋め込みたい情報が 9 ビットなので，3 つの領域 1,2,3 を 1 セットとして合計 4 セットを設定する．そして，1,2,3 の領域に順に 111,101,000 と埋め込む．

4.5　検　　索

ステップ 2 の検索とは，インターネット上で著作権侵害の可能性のある画像を発見した場合に，著作権保護対象の画像データベースから，対応する画像を検索することである．検索方法は，まずインターネット上の画像から特徴量を抽出し，次に，予め登録済みの画像データベース内の特徴量と比較することで対応する画像を探しだすというものである．ここでいう，特徴量はステップ 1 の埋め込みで用いた PCA-SIFT である．このステップでは，Stirmark 攻撃により改竄された画像と対応する画像を大量の画像データベースからいかに速く正確に検索することが必要であるが，既に [6] で高精度高速度で処理可能であると検証済みである．

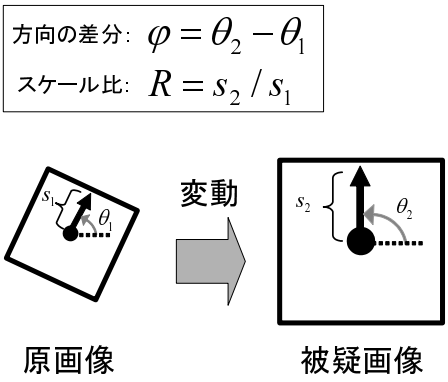


図 8　スケール比と方向の差分

4.6　検　　出

ステップ 3 の検出では，ステップ 2 の検索結果の画像から電子透かしを取り出す．ステップ 2 の結果，副産物として，局所記述子同士の対応が概ね得られているが，対応の中には，誤ったものも含まれている．

そこで，局所領域のスケール比と方向の差分を計算し，それらのヒストグラムを用いて誤対応を除外する．図 8 を用いて説明する．図中の四角形は対応付けられた局所領域の 1 組を表す．まず，スケール比 R$(=s_2/s_1)$ について，0.2 未満，0.2〜1.8 の範囲で 0.2 ずつ区切り，そして 1.8 以上という 10 個のビンを考える．s_1，s_2 は順に対応する原画像と被疑画像のスケールである．そして方向の差分 $\phi(=\theta_2-\theta_1)$ についても，0〜4π の範囲で $2\pi/5$ ずつ区切り 10 個のビンを想定する．θ_1，θ_2 は順に対応する原画像と被疑画像の方向である．次にスケールが大きいものほど対応が正確であるという記述子の特徴を踏まえて，原画像のスケール上位 K 位と対応する被疑画像のスケール上位 $T(\geq K)$ 位から選ばれた K 個の組について，前述の方法でスケール比と方向の差分を求め，ヒストグラムを作成する．そして，最頻値を得たビン及びその前後のビンに含まれたスケール比と方向の差分の範囲を求める．スケール比のヒストグラムの例を図 9 に，方向の差分のヒストグラムの例を図 10 に示す．スケール比の最頻値を得たビンは 6 であるので，前後のビン 5，7 も含めて，0.8〜1.2 を求める範囲とする．一方，方向の差分の最頻値を得たビンは 5 であるので，前後のビン 4，6 も含めて，$6\pi/5$〜$12\pi/5$ を求める範囲とする．

そして，原画像のスケール上位 N 位と対応する被疑画像のスケール上位 T 位から選ばれた N 個の組の内，先ほど求めたスケール比と方向の差分の範囲内にあるもののみ，原画像の局所領域の濃度平均と，被疑画像の局所領域の濃度平均を比べることによって，透かし情報を読み出す．

その結果，j 番目のデータとして，P 個の局所領域からの読み出し結果が得られる．読み出しの最終結果は，多数決によって定める．

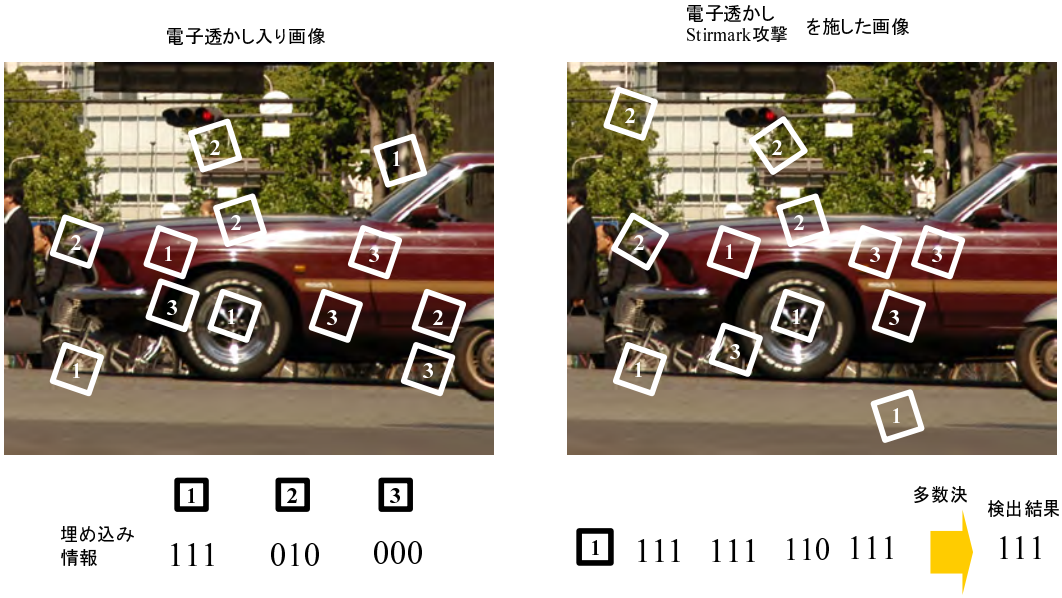


図 7　電子透かしの検出

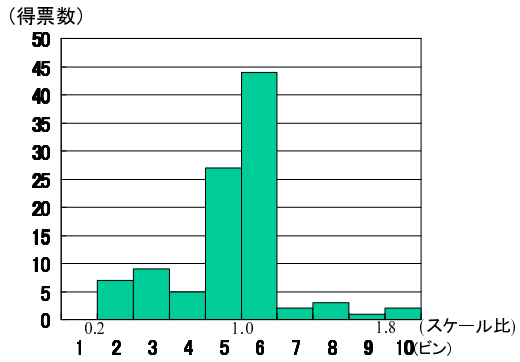


図 9　スケール比のヒストグラム

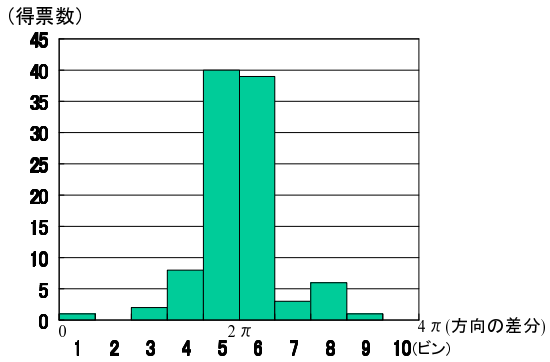


図 10　方向の差分のヒストグラム

具体例で見てみよう．先ほどの図 7 右のように領域が順序付きで得られたとする．例えば順序 1 の領域は，埋め込み時に 4 領域を設定したため，得られた領域も 4 領域となる．データを読み出した結果，同図右下に示すように 111, 111, 110, 111 であったとしよう．この場合，多数決によって読み出し結果は 111 となる．

5. 実　　験

ステップ 1 の埋め込みとステップ 3 の検出について実験を行った．実験に用いた画像は，最近のディジタルカメラで得られるサイズ 3008 × 2000 の画像 11 枚である．各種パラメータは以下の値とした．透かしの埋め込み強度を表すパラメータ A と B については，$A = 12$, $B = 2$ とした．埋め込んだ透かしは 30 ビット ($L = 10$), 重複して埋め込む回数 $P = 20$ とした．従って，埋め込みに用いた局所領域の合計は $N = LP = 200$ 個である．また，検出対象に選んだ局所領域の合計は $T = 500$ 個である．これらの領域は，原画像から得られた局所領域のうち，スケールが大きいものの上位 200 個および 500 個である．なお，原画像，被疑画像ともに，平均して 2.8 万個の局所領域が得られた．埋め込みに用いる領域の大きさは，1 辺が $M = 60$ 画素の正方形とした．透かし情報として乱数を埋め込み，Stirmark 攻撃のデフォルト設定 (Stirmark ver.3.1) を施した後に，読み出しを試みた．また，誤対応を除外する範囲の算出にはスケールの大きさ上位 $K = 100$ 個を用いた．その結果，11 枚のうち，10 枚からは埋め込んだすべての情報を正しく読み出すことができた．

図 11 の (a) に成功例を (b) に失敗例を示す．失敗画像については，読み出し誤りが発生していた．実験に用いた枚数が少ないため確定的なことはいえないが，失敗した画像については，類似のテクスチャが多く，局所記述子間で誤対応が起こったことが原因として挙げられる．この問題に対処するためには，画像同士の照合も行って，対応結果を検証する必要があると考えられる．

6. む　す　び

本稿では，幾何学的変換への耐性を持つ電子透かし法として，画像の局所記述子に基づく手法を提案した．従来法の多くがブ

(a) 成功例

(b) 失敗例

図 11　埋め込み及び検出に関する実験の結果

ラインド型の手法であるのに対して，本手法はノンブラインド型である点が大きな違いである．これによって，埋め込みに用いた局所領域を順序付けることができ，結果としてより大量の透かし情報を埋め込む可能性が得られる．

局所領域への埋め込み法として本手法で用いたものは，濃度の平均に基づくものであり，従来法に比べて容量の点で大きく劣るものである．今後はこの点を改良し，実容量としても従来法を上回る手法へと改良する必要がある．大量の画像を用いた実験も，今後の重要な課題である．

文　　献

[1] 田中愛子, 岡本栄司：“電子透かしを用いたディジタル画像改竄検出方法に関する研究”, Master’s thesis (2004).

[2] URL:http://kinoshita.ee.kanagawa-u.ac.jp/ nayuta/2000/stirmark/stirmark.ht ml.

[3] P. Bas, J.-M. Chassery and B. Macq: “Geometrically Invariant Watermarking Using Feature Points”, Trans. IEEE Image Processing, Vol. 11, No. 9, pp. 1014–1028 (2002).

[4] 戸根, 浜田: ” スケール変換と回転等への耐性を持つ電子透かし法”, 信学論 (D-I), Vol. J88-D-I, No. 12, pp. 1750–1759 (2005).

[5] H.-Y. Lee, H. Kim, H.-K. Lee: “Robust Image Watermark-

ing Using Local Invariant Features", Optical Engineering, Vol. 45, No. 3, pp.037002-1–11 (2006).
[6] 横田, 黄瀬, 汐崎："画像認識を用いた著作権保護システムの実験的検討", 電気学会電子・情報・システム部門大会講演論文集 (2007).
[7] Y.Ke and R.Sukthankar: "A more distinctive representation for local image discriptors", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol.2, pp. 506–513 (2004).
[8] S. Arya, D. M. Mount, N. S. Netanyahu, R. Silverman and A. Y. Wu: "An optimal algorithm for approximate nearest neighbor searching fixed dimensions", Journal of ACM, Vol.45, No.6, pp. 891–923 (1998).