画像認識を用いた著作権保護システムの実験的検討

横田 哲*　黄瀬 浩一　汐崎 陽
大阪府立大学大学院工学研究科

Expermental Investigation of a Copyright Protection System Based on Image Recognition

Satoshi Yokota*　Koichi Kise　Shiozaki Akira
Graduate School of Engineering, Osaka Prefecture University

Abstract　This report presents a system for copyright protection of digital still images based on an image recognition technology with local descriptors. For the purpose of copyright protection of images, image watermarking has been extensively studied for more than a decade. However, it is still difficult to achive an enough tolerance for alternations such as Stirmark attacks. In order to solve this problem, we propose a method of copyright protection based on a new image recognition technology that is tolerant to various image transformations including the geometric transformation. The image recognition enables us to find the corresponding image from thousands of reference images to be protected in response to a query image that undergoes Stirmark attacks and embedding of digital watermarks. From experimental results using 10,000 images in the database, we have confirmed that the method is capable of recognizing 99.49% of query images only within 216 ms / query (excluding feature extraction).

キーワード　著作権　画像　認識　保護

Key words　copyright　image　recognition　protect

1　まえがき

近年，インターネットの普及に伴い，通信回線の増強が行われ，音声，画像，動画などの大容量のデータが大量に流通するようになった．また，パソコンの高機能化により誰でも個人規模で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，新たな問題を生んでいる．その中でも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．

その防止策の一つとして，電子透かし [1] という技術がある．この技術はデジタルコンテンツに対して情報を埋め込み，著作権の主張を可能にするものである．埋め込まれる情報は，著作者情報，購入者情報，利用者情報などである．

以下，本研究では画像に焦点をあてて詳しく述べる．画像に関して言えば，画像を改竄し埋め込み情報を無効化する攻撃が存在する．この攻撃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 攻撃とは画像に人の目に知覚できない範囲で変化を加えるものである．Stirmark 攻撃など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る．よって，電子透かしの問題点としては Stirmark 攻撃などを受けると画像が改竄され，著作権を主張する証拠を失ってしまうことである．原因としては，電子透かしは Stirmark 攻撃で加えられる幾何学的な変換などに弱いということが挙げられる．

そこで，本稿では，Stirmark 攻撃などの画像の改竄にロバストな著作権保護システムを提案する．提案するシステムは，幾何学な変換などにロバストな最新の画像認識技術を応用したものである．利点は大量の画像から著作権を侵害されている可能性のある画像を瞬時に探し出せるという点である．つまり，画像認識技術の応用により保護したい画像群をデータベースとし，検索質問を Stirmark 攻撃を受けたインターネット上にアップロードされた画像とした時，検索質問が著作権保護の対象画像であるかどうか瞬時に判断でき，著作権侵害の可能性のある画像を探し出すことができる．

提案システムは３つのステップで構成されている．はじめは著作権侵害の可能性のある画像の検索をし、次に改竄されている検索結果の画像を元の画像に復元する．そして最後に復元した画像から著作権情報を検出する．

本稿では特に最も基本となるステップ 1 について詳述すると共に，一万画像のデータベースを用いた大規模な実験に

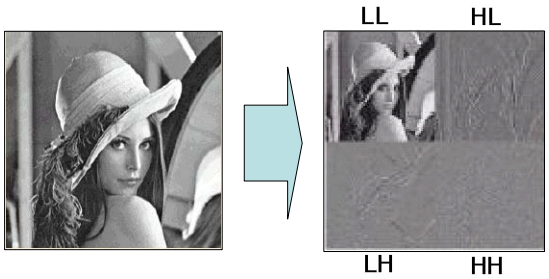


図 1　低周波成分と高周波成分に分解

よって有効性を検証する．

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む技術である．埋め込み方法は多くの場合，画像の画素値を書き換えることで行われる．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は埋め込み情報を破壊や除去をされないことである．

電子透かしは数多く種類があるが，ここでは実験に用いる Zhu らの手法 [3] について述べる．この手法はウェーブレット変換による多重解像度解析を利用したものである．多重解像度解析を用いれば，画像データを特定の周波数帯域を持ついくつかの小さいサイズの画像データに分割することができる．実際に原画像を高周波成分と低周波成分に分解すると図 1 のようになる．この様にして得られた低周波成分を原画像として、さらに高周波成分と低周波成分とに分解することで異なる成分の解像度の画像を生成する．この分解の結果得られた高周波成分に対して電子透かしを埋め込む．埋め込みたい画素値を x，元の画像の画素値を v，電子透かしの強度 α とした場合に，埋め込んだ後の画素値 $\acute{v}$ は，

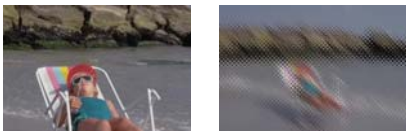
$$\acute{v} = v(1 + \alpha \cdot x)$$

で表される．この電子透かしの強度 α を上げれば，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，強度を上げすぎると，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，この電子透かしの強度 α が埋め込みの強度と視覚的劣化のつり合いをとる役割を担っている．

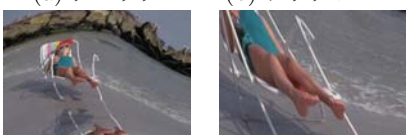
3　Stirmark 攻撃

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ことに用いられている．Stirmark 攻撃が画像に埋め込まれた情報を無効化する方法は，次の通りである．コンテンツ自体に人間に気付かれない程度に回転・拡大・縮小・線型変換などを加える．これらの操作により画素値がある閾値の範囲でランダム変更されるため，多くの電子透かしは無効にされてしまう．

図 2　原版



(a) クロップ　(b) フラクション



(c) 歪曲　(d) カーブ

図 3　Stirmark 攻撃の多様な処理

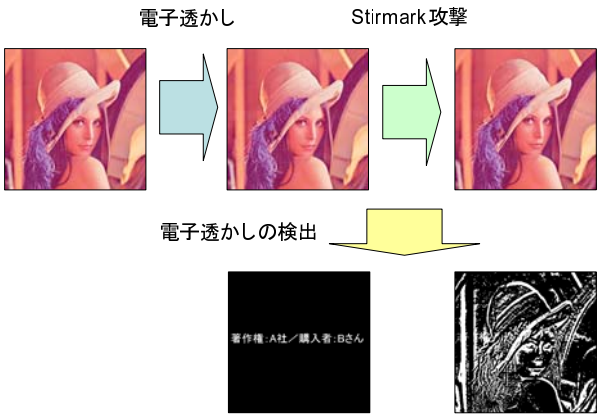


図 4　Stirmark 攻撃と電子透かし検出

図 2 に原版を示し，Stirmark 攻撃で用いられる画像処理の例を図 3 に示す．なお，図 3 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，Strimark 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．

4　提案手法

提案する画像の著作権保護システムの概要を述べる．まず，前提として，著作権を保護したい原版群があり，これらの画像から特徴量を抽出してデータベースに登録しておく．ここで特徴量とは画像を特定するものであり，異なる画像からは異なる値が得られるものである．詳しくは 5.1 で述べる．一方，ウェブ上にある画像を検索質問とする．ここで，ウェブ上の画像は電子透かしが埋め込まれた上に Stirmark

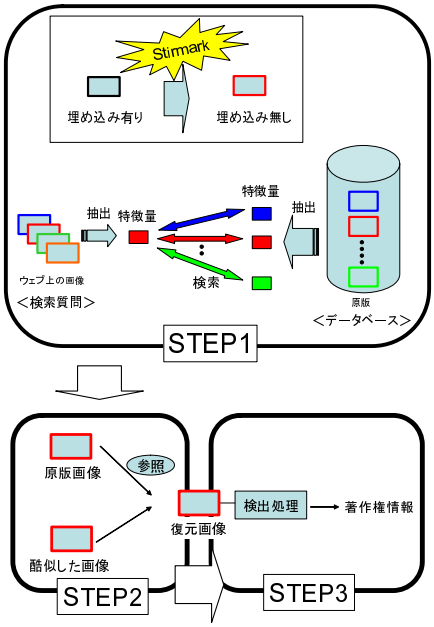


図 5　提案システムの概略

攻撃を受けていてもよい．

ここから，図 5 に示す STEP ごとに画像認識を用いた著作権保護システムの手順を述べていく．STEP1 では検索質問から特徴量を抽出し，特徴量とデータベースにある原版を比較して対応する画像を検索する．STEP2 では原版と検索結果の特徴量を用いて改竄されている画像の濃淡や位置を改竄前の画像に戻す．STEP3 で埋め込まれた情報を検出する．以下，本稿では STEP1 について焦点を当てて述べる．

5　画像認識

本稿で取り上げる画像認識は，以下のステップに分けられる．

1. 特徴量抽出：画像から特徴量を取り出す
2. 検索：特徴量に基づき対応する画像を検索する

提案システムではユーザが大量の保護したい画像群から著作権侵害の可能性のある画像を出来る限り早く検索したいという要求がある．また，その検索を誤ってはシステムの意味を成さない．従って，画像認識をいかに高速にかつ高い精度で行うことができるかが重要である．

5.1　特徴量抽出

提案手法では，画像からの特徴量抽出に SIFT(Scale-Invariant Feature Transform) [4] を用いる．SIFT は Lowe によって考えられた特徴量抽出法である．SIFT では，画像の局所領域における輝度変化から特徴点を抽出し，特徴点ごとに 128 次元の特徴量を計算する．

SIFT の改良手法として，PCA-SIFT [5] がある．ここでは主成分分析を用いて特徴量を 128 次元から 36 次元に削減したものを用いる．この操作により検索の精度がさらに高くなり，計算量も減少する．

提案システムでは，PCA-SIFT の結果を特徴量として用いる．提案するシステムにおいて，この特徴量抽出法を用いる利点は，得られる特徴量が回転や拡大縮小などの幾何変換に不変となることである．

5.2　検索

提案手法における検索とは，検索質問に対応する画像をデータベースから選び出すことである．手順は以下の通りである．はじめに検索質問から抽出される一つの特徴ベクトルとデータベースの全特徴量ベクトルを比較して，対応する特徴ベクトルを保有する画像番号に投票する．そして，この操作を検索質問の特徴ベクトル全てに行い，得票数が最多であったデータベースの画像を検索結果とする．

提案手法では，データベースから対応するベクトルを求める手法に ANN(Approximate Nearest Neighbor) [6] を用いる．ANN とは多次元空間における近似的な最近傍検索法である．

6　実験

本実験の目的は提案システムの STEP1 における画像認識の有効性を検証することである．画像認識は画像に変動がない場合 100% 成功することは自明である．著作権保護の場合，画像の変動の原因は Stirmark 攻撃と電子透かしの埋め込みの 2 つであると考えられるので，これらに対する耐性が重要な検討項目である．Stirmark 攻撃に対しては，実際に用いられるような「知覚出来ないレベルの変動」に加えて，様々な画像変換による変動の耐性に関しても考察する．

データベースとしては原版を一万枚用意し，3 つの実験で共通に用いた．この画像は [5] で用いられている写真画像の一部である．次に，検索質問用に一万枚の中から 100 枚を選び出した．この準備の下，次の 3 つ観点から行った実験について以下に述べる．3 つの実験のすべてにおいて評価方法としては，全検索質問のうちどれだけ対応する画像を検索できたかを表す精度を用いた．また，必要に応じて一万画像の中から 1 枚の検索質問に対応する画像を選び出す処理時間を計測した．ただし，特徴量の抽出時間は含まない．

6.1　実験 1:知覚できないレベルの Stirmark 攻撃に対する耐性を検証する実験

最初に，実際に用いられる場面を想定し，知覚できないレベルの Stirmark 攻撃を与え，どの程度画像認識が有効であるかを検証した．まず，選択した 100 枚の画像にフリーツールである SteganoEngine Ver.2.3 [7] を用いて電子透かしを埋め込み，Stirmark 攻撃のデフォルト設定 (Stirmark ver.3.1) を用いてランダムに 100 パターンの画像の改竄を施した．そのようにして得られた検索質問一万枚用いて実験を行った．評価方法として，精度と処理時間を用いた．

結果を表 1 に示す．電子透かしを埋め込んでいない画像 (Stirmark 攻撃は受けている) の場合，画像認識の精度は 100% であった．一方，電子透かしを埋め込んだ場合は，その影響で画像特徴量に変動が生じたため，精度が 0.51% 低下したものの，依然として 99% 以上の高い値を維持するこ

表 1　実験 1 の処理結果

電子透かし	なし	あり
精度	100 %	99.49 %
処理時間	217ms	216ms

とができた．処理時間については両者とも 200ms あまりと高速であった．

6.2 実験 2:Stirmark 攻撃における 4 種類の画像変換に対する耐性を検証する実験

Stirmark 攻撃を知覚できるレベルにまで変化させた場合に，どの程度まで画像認識が可能かを検証した．まず，選択した画像 100 枚に対して電子透かしを埋め込み，Stirmark 攻撃の 4 種類の画像変換 (クロップ，フラクション，歪曲，カーブ) のパラメータ値を変化させ，計 43 パターンの改竄を施した．そして得られた検索質問を 4300 枚用意して実験を行った．評価方法には精度を用いた．

結果を図 6 に示す．どの変換も大幅にパラメータ値を変化させるに連れて精度が低下している．具体例として，図 7 の原版に対して，電子透かしを埋め込んだ画像例を 4 種類の変換ごとに図 8〜10 示す．ここで，成功例の中で画像の変動が最大のものを (a) に，失敗例の中で画像の変動が最小のものを (b) に示している．なお，図中の精度は他の検索質問画像も加味した平均値である．

クロップ変換に関して言えば，図 8 の (a) ようにクロップのパラメータ値を 10 と大きく変化させた場合にも検索に成功した．フラクション変換については (a) のような知覚できる範囲の画像変換にも成功した．また (b) までパラメータ値を変化させたときに初めて失敗した．次に，歪曲変換の処理画像を図 10 に示す．(a) のように大幅な画像の改竄に対しても正しく認識できた．最後に，カーブ変換の処理画像を図 11 に示す．(b) のように大きく太らせる形になると失敗した．総じて，精度が低下している画像に関しては，原版と比較して改竄が激しく，外観を保っていないので著作権の保護対象とはならない画像であると見なすことができる．また，電子透かしの有無で精度に顕著な差は見られなかった．

6.3 実験 3:電子透かしの埋め込み強度と検索精度に関する実験

電子透かしの強度を変化させ，どの程度まで画像認識が出来るのかを検証した．まず，選択した 100 枚に，強度 α を 0.1 〜 1.0 まで 0.1 ずつ合計 10 段階変化させ電子透かしを埋め込んだ．そして Stirmark 攻撃のデフォルト設定 (Stirmark ver.3.1) を用いて，ランダムに画像の改竄を施し検索質問を 1000 枚用意し，実験を行った．その結果，図 12 に示すように強度 $\alpha = 0.3$ までは精度を 100% に維持できることがわかった．また，図 13(b) ように画像に変更を加えられた場合にも検索することができた．精度が 90% に低下した (c) の場合は原版 (a) と比較すると画像の乱れが激しいため，前述と同様に著作権保護の対象外と考えられる．

7 むすび

本稿では画像の著作権保護の分野において，従来手法の電子透かしの問題点を画像認識を用いて解決できるのではないかと考え，画像認識に基づいた著作権保護システムを提案した．また本稿では，提案システムの中でもとりわけ画像認識について詳述した．データベースの画像一万枚を用いた実験の結果，人に知覚出来ない範囲での電子透かしの埋め込みおよび Stirmark 攻撃を施した画像を検索質問にした場合，99.49% という高い精度を得ることができた．また，その時処理時間は 200ms 程度と高速であった．以上により，画像認識を用いた著作権保護システムが極めて有望であることが明らかとなった．

今後は，抽出した特徴量を用いて埋め込まれた電子透かしの復元に取り組み，著作権を主張できるシステムの構築を行いたい．

謝辞

本研究の一部は，大阪府立大学先端科学共同研究プロジェクトの補助による．

参考文献

[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.html.

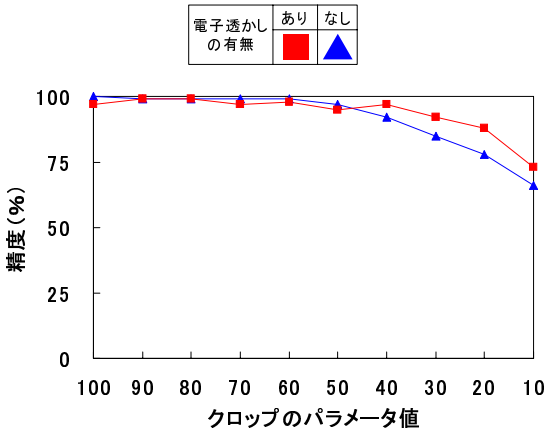
[3] W. Zhu, Z. Xiong and Y. Q. Zhang: “Multiresolution watermarking for images and video”, IEEE Transactions on Circuits and Systems for Video Technology, Vol.9, No.4, pp. 545–550 (1999).

[4] D. Lowe: “Distinctive image features from scale-invariant keypoints”, International Journal of Computer Vision, Vol.60, No.2, pp. 91–110 (2004).

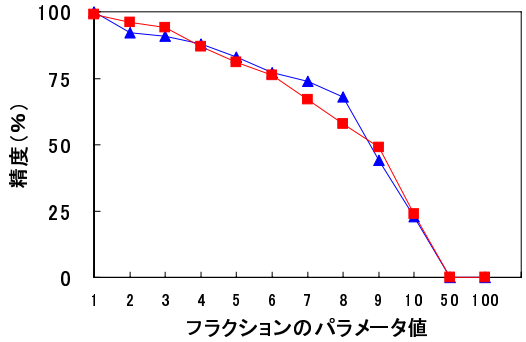
[5] Y.Ke and R.Sukthankar: “A more distinctive representation for local image discriptors”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol.2, pp. 506–513 (2004).

[6] 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).

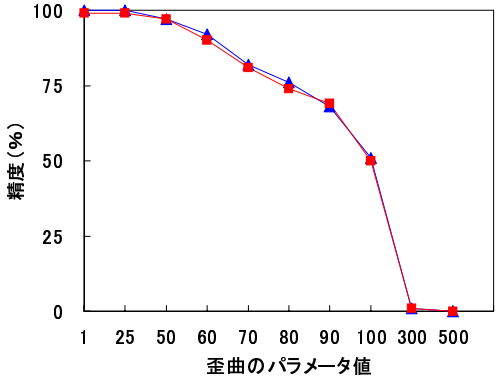
[7] URL:http://www.lnsoft.net/sw_convert.htm#steganoengine.



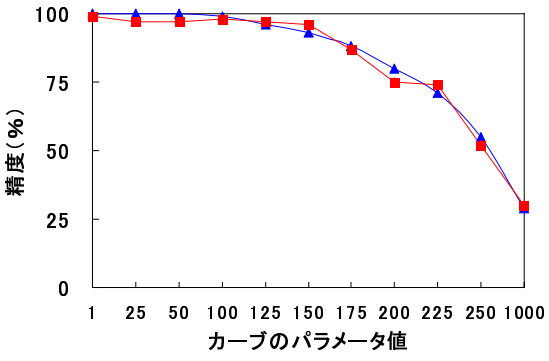
(a) クロップ変換



(b) フラクション変換



(c) 歪曲変換



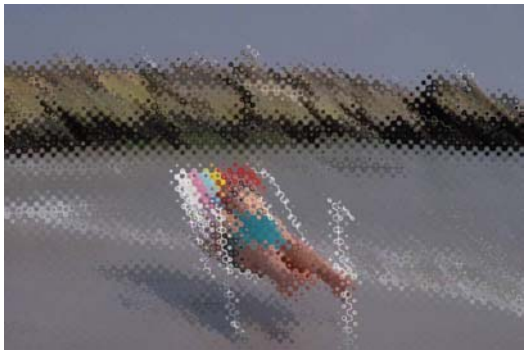
(c) カーブ変換

図 6　実験 2 の結果

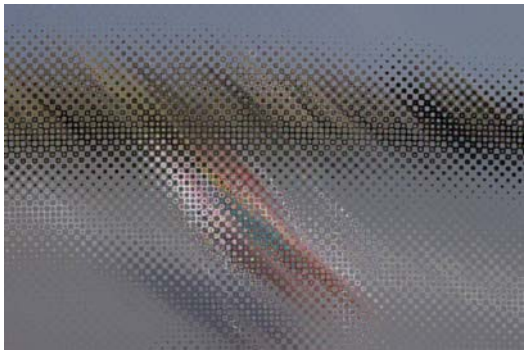
図 7　原版

(a) 成功例：クロップのパラメータ値 10

図 8　クロップ変換の処理画像



(a) 成功例：フラクションのパラメータ値 10



(b) 失敗例：フラクションのパラメータ値 50

図 9　フラクション変換の処理画像

(a) 成功例：歪曲のパラメータ値 100

(b) 失敗例：歪曲のパラメータ値 300

図 10　歪曲変換の処理画像

(a) 成功例：カーブのパラメータ値 225

(b) 失敗例：カーブのパラメータ値 250

図 11　カーブ変換の処理画像

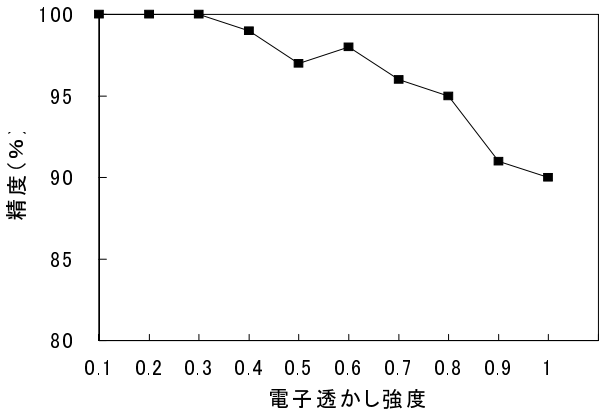


図 12　実験 3 の結果

(a) 原版

(b) $\alpha = 0.3$

(C) $\alpha = 1.0$

図 13　実験 3 の処理画像