J-038

フレネル変換の距離パラメータの変化による透かし画像への攻撃
Attack on Watermarked Imeges by the Inflection of Distance Parameter of Fresnel Transform

姜　錫* Seok Kang　　青木由直* Yoshinao Aoki

1. まえがき

インターネット人口の拡大が急速に進む中，画像や音声などのマルチメディアに対する著作権の管理が問題となっている．デジタル化されたこれらのデータは，劣化することなく手軽に複製することができ，様々な加工に対しても柔軟に対応できるという利点がある一方，悪意ある消費者やソフト制作者らによる不正コピー，ネットを介した二次頒布等の被害を受ける可能性が高くなるという不利をも背負っている．

そのような環境への対策の一つとして，「電子透かし(Watermarking)」が提案されている．電子透かしとは，電子文書や画像，音楽，映像などの創作品の中に，IDなどの著作者固有の識別符号を密かに埋め込み，所有権の所在を主張しようと企図したものである．これ自身は複製を抑制することはできないものの，不正コピー者に無言の圧力を与え，あるいは著作権侵害に対する検証の道具として利用されることが期待されている [1].

電子透かしにおいて重要なことは，そのコンテンツの著作権が誰にあるかを明示するために埋めこまれた透かし情報が欠落しないまま永久に保存されることである．そのためには，各種のフィルタリングや再標本化，切り取り，データ圧縮などの処理によって，透かし情報が変質もしくは消失しないことが大切であり，近年研究が行われている電子透かし技法は攻撃に対しての耐性をもつようにしている．一方，ある電子透かし法の攻撃に対する丈夫さをテストできるようにしたStirmark[2]というベンチマークソフトが多く知られている．

本研究では，フレネル変換を施す際生じる量子化誤差とその変換の距離パラメータの値を少しずつ戻しながら行う逆フレネル変換による透かし画像への攻撃法を述べるとともに，その実験結果を示す．

2. フレネル変換による透かし画像への攻撃

2.1 フレネル変換

フレネル変換は波動のフレネル回折の記述に用いられ，ホログラムデータの数値処理などに利用される．2次元図形を波源面に置き，そのフレネル変換面を求める場合を考えると，波源面から遠ざかるほどそのフレネル回折パターンは広がり，波源分布パターンの形は崩れたものになっていく．図1の波源面 x_1-y_1 に2次元図形 $s(x_1,y_1)$ が置かれているとすると，観測面 x_2-y_2 でのフレネル回折パターンは次式のようになる [3].

$$F(x_2,y_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s(x_1,y_1)\exp\left[-\frac{j\pi}{D}\cdot\left\{(x_2-x_1)^2+(y_2-y_1)^2\right\}\right]dx_1\,dy_1 \quad (1)$$

*北海道大学情報科学研究科, Hokkaido Univ.

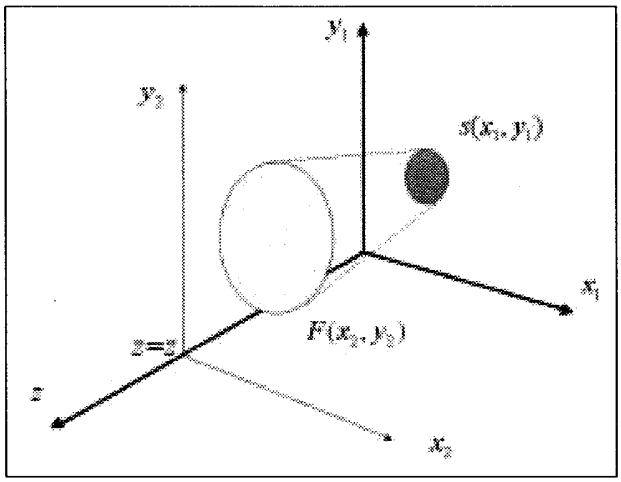


図 1: ２次元画像のフレネル変換

ここで，D はフレネル変換面を決めるパラメータであり，図1の物体面と観測面の距離 z と波長 λ で次のように表せる．

$$D = \frac{\pi\lambda z}{L^2} \quad (2)$$

式（1）は2次元図形関数 $s(x,y)$ と次の関数 $p(x,y)$ とのコンボリューション積分として表せる．

$$F = s * p \quad (3)$$

ただし

$$p(x,y) = \exp\left[-\frac{j\pi}{D}(x^2+y^2)\right] \quad (4)$$

コンボリューション定理より，$\mathcal{F}$ をフーリエ変換演算オペレータ，$\mathcal{F}^{-1}$ を逆フーリエ変換演算オペレータとすれば，式（1）は次式となる．

$$F = \mathcal{F}^{-1}[\mathcal{F}[s]\mathcal{F}[p]] \quad (5)$$

ここで，$\mathcal{F}[p]$ は次のように解析的に求まる．

$$\begin{aligned}\mathcal{F}[p] &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\left[-\frac{j\pi}{D}(x^2+y^2)\right]\\ &\quad\cdot\exp\left[-j2\pi(\mu x+\nu y)\right]dx\,dy\\ &= -jD\exp\left[j\pi D(\mu^2+\nu^2)\right] \quad (6)\end{aligned}$$

ここで，μ と ν は空間周波数である．

2.2 フレネル変換による攻撃

フレネル変換による攻撃方法として，画像をフレネル変換した値は実数部と虚数部を持つが，その両方を含んだ値を用いて逆フレネル変換を施す際，距離パラメータの値を少しずつ戻しながら逆フレネル変換を行う方法と，実数部だけを用いて逆フレネル変換をする方法を試した．前者はほぼ画像の劣化がないが，攻撃力も弱い．後者は画像の劣化はあるが攻撃力が強い．攻撃によって画像が劣化してしまうのは他の攻撃（雑音付加，JPEG 圧縮など）と同じである．

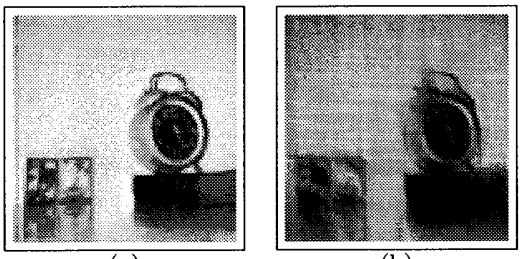
3. 実験結果

提案した方法の有効性を確かめるため，図 2 の (a) を透かし画像 (256× 256 pixel，8 bit 濃淡分解能) として実験を行った．攻撃を行ったのは電子透かし用のソフトウェアで JPEG 圧縮を始め各種画像編集にも耐えうるとされているものを使用した．この電子透かし法は埋め込みの強度を変えることができ，強く埋め込めば耐性は強くなるが，画像の劣化も大きくなる．

方法 1 は実数部，虚数部両方を用い，逆フレネル変換を行う際，距離パラメータの値を何回かに分解して施すことにより生じる量子化誤差による攻撃法であり，方法 2 は虚数部は切り捨てて，実数部だけを逆フレネル変換のデータとして行う逆フレネル変換による画像の劣化に基づく攻撃法である．表 1 の結果から，方法 1 では強度が高ければ攻撃は効かないが，強度 8 では画像の劣化もなく透かしデータを無効化した．方法 2 ではかなりの攻撃力があり，JPEG20%のときも失敗した強度 12 の場合にも攻撃ができた．しかし，図 2 の (b) に表しているように画像の劣化が激しい短所があり，そのときの PSNR の値は 20 程度であった．

表 1: 実験結果

強度	方法 1	方法 2	JPEG20%	JPEG60%
8	○	○	○	×
12	×	○	×	×



(a) (b)

図 2: 透かし画像と攻撃された画像

4. まとめ

本稿では，フレネル変換を施す際生じる量子化誤差とその変換の距離パラメータの値を少しずつ戻しながら行う逆フレネル変換による透かし画像への攻撃法に着目し，市販の電子透かしソフトに対する攻撃を試した．今回フレネル変換を用いた電子透かし画像への攻撃では耐性を持つとされる透かしデータを無効化することができ，本稿で提案している方法が透かしデータに対する攻撃手段となり得ることを確かめた．今後の課題としては様々な電子透かし法に対しても本手法による攻撃の可能性についての検討や攻撃後の画質を上げる法の検討が挙げられる．

参考文献

[1] 松井甲子雄, "電子透かしの基礎," 森北出版, 1998.

[2] Fabien A. P. Petitcolas, and M. Kutter, "A fair benchmark for image watermarking systems," In Electronic Imaging'99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans jose, CA, USA, 25-27 Jan. 1999.

[3] 青木由直, "オペレータ法ディジタル信号処理," コロナ社, 1996.