I-092

結託攻撃に対する画像電子透かし耐性向上についての一検討

A Study of Image Watermark Resistance to Collusion Attacks

藤村　誠† 今村 幸祐‡ 黒田　英夫††
Makoto Fujimura Kousuke Imamura Hideo Kuroda

1.まえがき

近年，ネットワークの高速化，大容量化に伴い，動画像配信，画像公開などが活発になるとともに画像コンテンツの不正コピーなども増加してきており，電子透かしの重要性も増してきている．特に，電透かしに対する攻撃はこれまでの単独攻撃に加えて結託攻撃に対する耐性も求められるようになってきた[1][2].

電子透かしに対する結託攻撃の一つである平均化攻撃では，同一画像に対して異なる電子透かし情報が埋め込まれた複数のコンテンツを用いることで，埋め込まれた透かし情報を除去した画像を生成する．これは透かし情報が埋め込まれた原画像は同一であり，平均化処理などを行っても原画像は復元可能であることが前提になっている．文献[3]では，結託攻撃に対して耐性を持つ結託耐性符号を透かし情報として画像コンテンツに埋め込んでいる．

また，結託攻撃では電子透かしの埋め込み位置の特定を目的とする場合もある．同一原画像のほぼ同じ箇所へ異なる透かし情報を埋め込むために，透かし情報を埋め込まれた画像間で差分とられることなどで埋め込み位置の特定が可能になるためである．このことに対しては，同一画像に対して埋め込み位置を変化させることで，電子透かしの検出対策を行ったり，ダミーの電子透かし情報を埋め込むことで，攻撃結果の混乱を招くことを狙いにした対策も可能である．

結託攻撃の狙いは，同一原画像に異なる電子透かしを埋め込んだ複数の画像コンテンツを利用することである．複数の画像を用いて平均化することにより、透かしを除去した画像を得ることが可能であるからである。

しかし，画像コンテンツの配信において，必ずしも同一の画像を使用する必要はないものと考えられる．例えば，画像符号化では一般に人間の視覚特性を利用して本質的には画像品質を劣化させて情報量圧縮を行っており，人間が検知できない程度の劣化であれば異なる圧縮率の配信を行うこともできる．このことから，配信するユーザに対して，視覚特性上違和感のない映像でありさえすれば，それぞれのユーザに微小な変位のある画像を配信することも可能である．

本稿では，原画像そのものを加工して，ユーザごとに異なる画像を配信することを検討する．画像符号化との兼ね合いを考慮すると，周波数成分を変更することは望ましくないと考え，まずは間引きや並行移動などの画素位置のずれが生じるような加工を検討する．

†長崎大学，‡金沢大学，††FPT 大学（ベトナム）

原画像に平行移動などの処理を加えることによって，平均化攻撃の際に原画像そのものの劣化を引き起こすことを目的とする．

以下，2 ではアフィン変換による画像への変位付加について述べる．3 では実験結果を報告し，4 でまとめる．

2.アフィン変換による画像への変位付加

画像のアフィン変換による原画像からの微小変位を加えることで，視覚的には検知できない程度の異なる画像を検討する．

アフィン変換は平行移動などであるが，回転では補間するためのフィルタ処理が必要であり，平行移動であっても半画素単位の移動の場合も補間フィルタが必要になる．このため，単なる画素値の移動になるというわけではない．

また，画像全体に対する単純なアフィン変換のみでは攻撃者に解析されやすくなるという恐れがある．そこで，単純なアフィン変換に間引き処理のような画像領域ごとに異なるアフィン変換を施すことで，解析に対する耐性を高めることも考えられる．

画像を領域ごとに異なるアフィン変換を施すということは，領域境界に新たなエッジが生じることになるこのため，平坦な領域に境界を設定することは視覚的に問題がある．しかし，画像への変位により符号化効率が著しく低下することは問題である．加えて，人間の主観的な画像品質の低下も抑える必要がある．そこで，もともと存在しているエッジの領域に沿って境界を設定するなど画像ごとの特性に合った処理が有効であると考えられる．

本稿では，基本的な検討として，まずは画像全体に対する平行移動による変位を加え，これらの画像に対する平均化処理を行い，その様子を調べることとする．

3.基礎実験

原画像に対して，何種類かの平行移動を行った画像を平均化することによる画質劣化を測定した．使用したテスト画像は，Mandrill および Lenna のカラー画像であり，画像サイズは 512x512 および 256x256 である．

今回行った平行移動のベクトルは，(0.5,0)，(-1,0)，(0,2)，(0,-3)，(1, 1)，(-2,2)，(1,-2)，(-0.5,-1)，(1,0)，(0,1) の 8 種類である．これは，規則的な移動を施した画像を対象にした場合は単なる平均値フィルタになってしまうため，できるだけ不規則な移動を対象とすることで劣化の様子を観察するためである．また，原画像を移動した後の領域については，輝度値を 0 とした．これらの平行移動を行った 8 枚の画像に対して，それぞれの画素値の位置での平均化処理の結果を求めた．

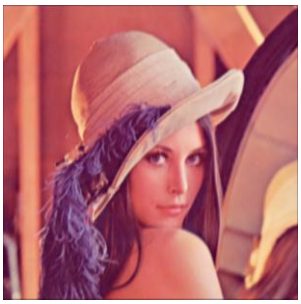
図 1 に実験結果を示す．図 1(a)は原画像 Mandrill であり，(b)，(c)はそれぞれ 512×512 のサイズおよび 256×256 の場合の平均化処理結果である。同様に(d)は原画像 Lenna であり，(e)および(f)はそれぞれのサイズでの平均化処理の結果である．これらの図より，同一の移動処理であっても画像サイズの小さい場合の方の劣化が大きいことが分かる．

(a)原画像(Mandrill) (256x256，512x512)

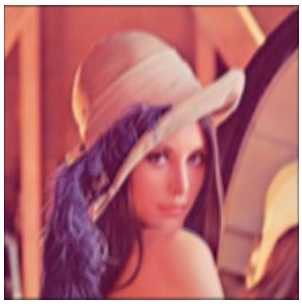
(b)処理画像(512x512)

(c)処理画像(256x256)

(d)原画像(Lenna) (256x256，512x512)



(e)処理画像(512x512)



(f)処理画像(256x256)

図 1　平行移動付加画像の平均化処理

以上の図より，原画像に平行移動を施した画像群に対する平均化処理により，画質劣化が生じているが，画像サイズが小さい方がより効果的であることが分かる．これは，同じ平行移動であれば，画像サイズに対する変位がより大きい方が，平均化処理を行った際の位置のずれが大きいためより劣化が大きくなるためである．

画像サイズに対する平行移動する大きさを求める必要がある．また，画像全体を単に平行移動するだけでは，平均化攻撃を受けた場合の劣化の度合いも限度があり，平行移動量を攻撃者に検知された場合は，対応されてしまう恐れがある．このため，画像ごとに対応した変位の付加を検討する必要がある．

4.まとめ

原画像に平行移動を加えた画像を配信画像とすることで，結託攻撃である平均化攻撃を受けた際に画質劣化を生じさせる方式を提案した．実験結果より，ある程度の劣化を確認できたが，原画像へのより効果的な変位を検討する必要がある．

参考文献

[1] H.Zhao, M.Wu, Z.Wang, and K.J.R.Liu, “Forensic Analysys of Nonlinear Collusion Attacks for Multimedia Fingerprinting”, IEEE Trans. Image. Process., Vol.14, No.5,pp.646-661,2005.

[2]S.He, M.Wu,”Joint Coding and Embedding Techniques for Multimedea Fingerprinting”, IEEE Trans. On Information and Security, Vol.1, No.2,pp.231-247,2006

[3] W.Trappe, M.Matsushima, and S.Hirasawa, “Anti-collusion Fingerprinting for Multimedia”, IEEE Trans. Signal Process., Vol.5, No.4,pp.1069-1087,2003.