

DCT係数の交換によるスクランブル画像のファイルサイズの増加を抑制した半開示スクランブル技法 Image Partial Scrambling Technique for Controlling Increase in Size of File of Scrambled Image by Exchanging DCT Coefficient

チョウ キザワ[†] 姜 錫[‡] 坂本 雄児[‡]
Kizawa Chou Seok Kang Yuji Sakamoto

1. まえがき

近年、インターネット配信など、デジタル画像の有料配信サービスが盛んになってきている。それに伴ってDRM(Digital Rights Management)技術が注目されている。

DRMの一つとして、画像スクランブル法という技術がある。画像スクランブル法は、配信者が画像の閲覧権を購入した課金者によりのみ閲覧を許可する事を目的とした技術で、画像に可逆的な劣化処理を施す事により視聴者に元の情報を認識させない技術である。画像スクランブル法の中には半開示画像スクランブル法という技術がある[1][2]。従来の画像スクランブル法のように完全に画像を隠蔽するのではなく、画像の内容を確認できる程度に劣化させた半開示スクランブル画像を閲覧者全員に配信する。非課金者は半開示スクランブル画像をサンプルの代わりに閲覧し、その画像に興味を示して購入のため課金をすると、復号鍵を配信者から受け取り、オリジナルの画像を見ることが出来る。よって、別途にサンプルを作成する手間が省けるという利点がある。

従来の半開示画像スクランブル法[2]においては、作成されるスクランブル画像の劣化度合いを定量的に制御できたが、ファイルサイズが増加してしまうデメリットがある。そこで、スクランプリングによるファイルサイズの増加を最低限に抑え、かつ、客観的指標を用いた定量的に画質制御が可能な半開示画像スクランブル法を提案する。また、実際に提案手法を用いたスクランプリング結果を示し、考察を行う。

2. 半開示画像スクランブル技法と関連技術

2.1 半開示スクランブル

半開示スクランブル技術は、画像の情報を完全に隠蔽するのではなく、一部の情報のみを開示し、概要を視聴者に認識させる事ができるスクランブル方式である。

半開示画像スクランブル法の基本的な運用の流れは以下の通りである。

1. 暗号化により画像内容をある程度隠蔽した半開示スクランブル画像を閲覧者全員に配信
2. 課金した視聴者によりのみスクランブル解除のための復号鍵を配布
3. 課金した視聴者は復号鍵を使いスクランブルを解除

半開示画像スクランブル法の運用例を図1に示す。

2.2 JPEG

本手法に使用する半開示スクランブル画像の圧縮フォーマットにはJPEG[3]が使用されている。よって、JPEG圧縮の処理を簡単に説明する。

JPEGでは、画像をブロックに分割してからDCTを行う。DCTによって得られたDCT係数を量子化テーブルの値に応じた量子化値で除算する。JPEGにおいて符号化するには、ランレングス符号化とハフマン符号化を組み合わせて符号化を行う。ランレングス符号化は連続する同一の値を「値×回数」という列の長さの情報に書き換えてデータ圧縮を行う。ハフマン符号化は出現頻度の高いデータに短いビット数を、出現頻度の低いデータに長いビット数を割り当ててデータの圧縮を行う。

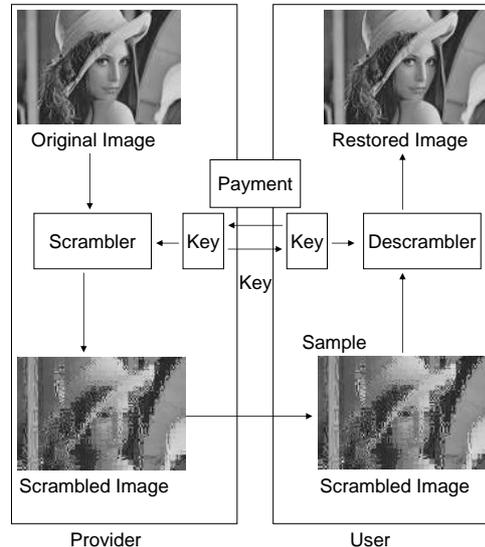


図1 半開示画像スクランブル法の運用例

2.3 半開示スクランブルの従来手法

画像にDCTと量子化を施す。目標とするPSNR値(T_{psnr})から、1ブロックのDCT係数に合計で生じさせるべき二乗誤差(必要二乗誤差)を算出する。求めた必要二乗誤差に達するまで、擬似乱数によって決定したDCT係数を増減させる。係数の増減のさせ方は、埋め込みと復元が逆操作になっていれどのような方法を用いてもよい。可変長符号化を行い、JPEG画像としてスクランブル画像を生成する。

2.4 従来手法の欠点

DCT係数をランダムに増減したことにより、可変長符号化の効率が低下してしまう。可変長符号化効率が低下すると画像のファイルサイズが大きく増加する。これは画像の保存や配信に不都合である。

3. 提案手法の概要

従来の半開示スクランブル法[2]でスクランブルを施したときにファイルサイズが増加してしまう欠点を解決するため、DCT係数の交換のみによるスクランプリングでファイルサイズの増加を抑えた半開示画像スクランブル手法を提案する。DCT係数の値が0の場所と0でない場所を交換するとランレングスが違ってファイルサイズが増加する恐れがあるため、DCT係数の値が0でない2つの係数を交換対象とする。擬似乱数によって選ばれた2つのDCT係数を交換させて、生まれる二乗誤差を計算する。この二乗誤差が必要二乗誤差を超えるまで交換を行う。二乗誤差が必要二乗誤差に達しないブロックが存在する場合がある。このとき、不足している分の二乗誤差を次のブロックに繰り越す。その場合、次のブロックに必要な二乗誤差は必要二乗誤差に不足分の二乗誤差を足した値になる。また、二乗誤差が必要二乗誤差を超えた場合も同様に繰り越す。

提案手法では、交換位置の決定と特定に擬似乱数を用いる。擬似乱数とは、計算機によって生成される、乱数と識別不能な数列のことである。乱数は本来規則性も再現性も持たない

[†] 北海道大学工学部情報エレクトロニクス学科

[‡] 北海道大学大学院情報科学研究科



図2 スクラミング結果



図3 スクラミング解除結果



図4 異なる Seed による解除結果



図5 通常の JPEG 画像

が、擬似乱数は計算によって生成されるので、生成器内部の初期値 (Seed) を同じ値にすれば全く同じ数列が生成される。スクランピングの時には、擬似乱数を用いて交換位置を決定する。解除時には、スクランピングの時と同じ擬似乱数の Seed を使うことによって、スクランピングの時と同じ擬似乱数を得て、交換位置を特定する。この時、Seed は秘密鍵の役割をしている。

4. 実験

用意した画像に対して提案手法を適用し、スクランブル処理と解除、及び劣化度合いの調節が可能かを確認する。さらに、ファイルサイズの増加率を調べる。劣化度合いの調節とファイルサイズについては、従来手法との比較を行う。原画像には標準画像データベース (SIDBA) のフルカラー画像を用いる。JPEG の Quality を 75 とする。

4.1 スクラミングと解除の実験

元画像に対してスクランピングを行った画像を図2, そのスクランブル画像を正しい Seed で解除した画像を図3, スクラミング時とは異なる Seed を用いて解除画像を図4に示す。また、解除画像と比較するために、通常の JPEG 圧縮画像を図5に示す。

4.2 劣化度合いの調節実験

Tpsnr を上げると PSNR 値は単調増加している。Tpsnr が 20, 30, 40 については Tpsnr と PSNR 値はほぼ同程度の数値となっている。しかし、Tpsnr が 10 の場合には大きく PSNR 値がずれている (図6)。これはスクランピングによって生まれる誤差は DCT 係数の値に依存しているため、最も必要二乗誤差と近い二乗誤差を生じさせても誤差が足りないためである。

4.3 ファイルサイズ増加率の実験

従来手法のファイルサイズの増加率が最も大きい 59.7% (図7) に対して、提案手法では、すべての画像ファイルサイズの増加率を 5.53% (図8) 以下に抑えている。

5. まとめ

本稿では DCT 係数の交換のみによってスクランピングを行う半開示スクランブル法を提案した。従来の半開示スクランブル法には、ファイルサイズの増大という問題点があり、それを改善するために DCT 係数の交換のみによってスクランブル処理を行い、ファイルサイズの増加量を抑制した。ま

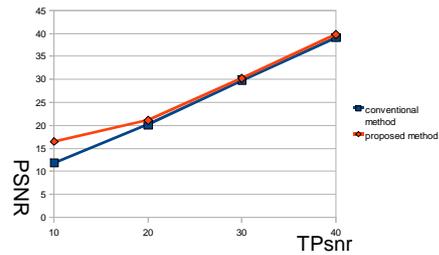


図6 提案手法と従来手法の PSNR 値の比較 (Lenna)

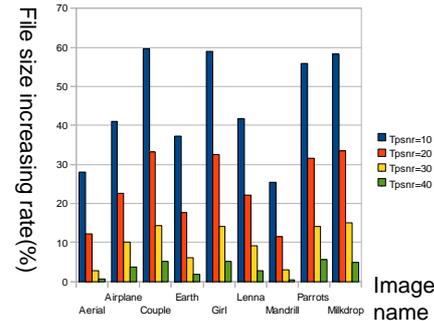


図7 従来手法におけるファイルサイズ増加率

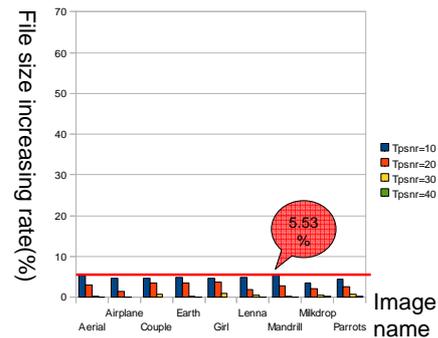


図8 提案手法におけるファイルサイズ増加率

た、提案手法に関する実験を行い、従来手法の利点を活かしつつ、提案手法の有効性を確認した。今後の課題としては、Tpsnr をある値より低くしても PSNR が下がらない問題点がある。新たなスクランピングアルゴリズムを考える必要がある。

謝辞

本研究の一部は日本学術振興会科学研究費 (挑戦的萌芽研究 23650036) を用いて行われたものである。

参考文献

- [1] 藤井寛, 山中康史, "デジタル画像情報流通支援のためのスクランブル方式", 情報処理学会論文誌, Vol.38, No.10, pp.1945-1955, 1997.
- [2] 澤田圭一, 姜錫, "擬似乱数を用いた劣化型電子透かし手法" 電子情報通信学会総合大会講演論文集 2007年 基礎・境界, 222, 2007-03-07.
- [3] 越智宏, 黒田英夫, "JPEG & MPEG 図解でわかる画像圧縮技術", 日本実業出版社 (1999).