HTJ2K に基づく Encryption-then-Compression 法の検討

A Study on Encryption-then-compressed method based on HTJ2K standard

坂本 佑介
指導教員 渡邊 修

拓殖大学大学院 工学研究科

キーワード: JPEG 2000, HTJ2K, Encryption-then-Compression, プライバシー保護

1. はじめに

JPEG 2000 は，静止画像符号化の国際標準である．2000 年に JPEG(Joint Photographic Experts Group) によって規格化されてから，デジタルシネマをはじめとして, 医療画像, 衛星画像, 公文書アーカイブ等の高画質を要求される分野で用いられてきた．JPEG 2000 は高い圧縮効率や，豊富なスケーラビリティ機能を持つ反面，エントロピー符号化に要する演算量が膨大であるという問題を抱えていた．JPEG 2000 Part 15 として出版された High-Throughput JPEG 2000（以下 HTJ2K）は, この問題を解決する新しいエントロピー符号化を定義する [1].

ディジタル画像のプライバシー保護を目的として，Encryption-then-Compression（以下 EtC）システムが知られている．EtC システムは，入力画像に対して，可逆かつ，後段の符号化処理になるべく影響を与えない方法によるスクランブル処理を施し，その後画像符号化を行うプライバシー保護方式である．SNS 等のサービスを提供する SNS プロバイダは，ユーザがアップロードした画像を，ユーザの許諾なしに再符号化したり，生成 AI 用の学習データとして用いることがある．EtC システムの利用によって，このようなユーザの許諾なしの処理に対して，画像の内容を保護することが可能となる．

本稿では，HTJ2K を用いて符号化された画像のための EtC システムを提案する．提案する EtC システムは，HTJ2K の符号化効率に与える影響は小さく，さらにスクランブルの程度も制御可能であることが実験によって確認された．

2. 要素技術

2.1. HTJ2K

HTJ2K では，新しいブロックコーダ (FBCOT: Fast Block Coding with Optimized Truncation) を定義する．FBCOT は JPEG 2000 Part1 で規定されている従来の

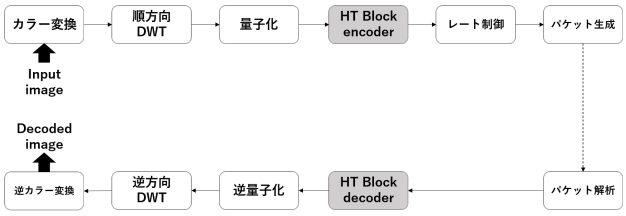

図 1: HTJ2K を用いた画像の符号化

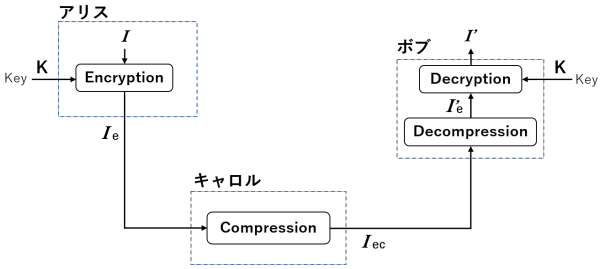

図 2: Encryption-then-Compression システム

ブロックコーダ, EBCOT(Embedded Block Coding with Optimized Truncation) の単純な置き換えとして機能し，処理に伴うスループットを十倍以上向上させることが可能である．図 1 は, HTJ2K を用いた画像の符号化と復号処理の流れを示すブロック図である. 図中の網掛け部分「HT block encoder/decoder」が HTJ2K で規定される新しいブロックコーダである．その他の処理は従来の JPEG 2000 Part 1 と同一であり，符号化結果であるコードストリームのシンタックスも同一である．

2.2. EtC (Encryption-then-Compression) システム [2]

EtC システムは, 入力画像に対して，可逆かつ，後段の符号化処理になるべく影響を与えない方法によるスクランブル処理を施し，その後画像符号化を行うプライバシー保護方式である．図 2 に, EtC システムを用いた画像通信の流れを示す．I は入力画像，I_e はスクランブル処理後の暗号化画像，I_{ec} は I_e を符号化した画像である．EtC システムの主な利点を以下に列挙する．

(a) 原画像　(b) 暗号化した画像

図 3: 原画像と EtC による暗号化画像との比較

- アリス（ユーザ）はキャロル（SNS プロバイダ）に I を開示する必要がない
- 通信エラーがあったとしても，I_{ec} の復号が可能
- ネットワーク使用率を最大化するために，キャロルによる I_{ec} のコーディングレート（圧縮率）の制御が可能

3. 提案する HTJ2K に基づく EtC システム

3.1. 方法

HTJ2K では，量子化された DWT 係数を，その正負符号と絶対値に分けて符号化処理を行う．量子化された DWT 係数を χ，その正負符号，絶対値をそれぞれ s，μ とおく．HTJ2K では，MagSgn と呼ばれる値が存在し，MagSgn $= 2(\mu \ominus 1) + s$ で与えられる．ただし，$\ominus$ はゼロでの飽和付き減算を表し，$0 \ominus -1 = 0$ である．この MagSgn 値が符号化されたものが MagSgn bitstream であり，HTJ2K コードストリームの一部を構成する．提案する EtC システムでは，s を疑似乱数から生成した乱数系列を用いて反転させることで，スクランブル処理を行う．MagSgn bitstream の生成アルゴリズムでは，MagSgn 値の最上位ビットの位置が重要であるため，s が反転することによる符号化効率の影響は小さいと予想される．

3.2. 評価実験および結果

提案する EtC システムによって図 3a に示す原画像をスクランブル処理した結果を図 3b に示す．また，様々な量子化ステップサイズで符号化した際の，提案法によるスクランブル（暗号化）の有無が画質に与える影響，すなわちスクランブルの程度を図 4 に，符号化効率に与える影響を図 5 に示す．図 3 および 4 より，提案する EtC システムは，十分なスクランブル効果を持つことが分かる．また，図 5 より，提案する EtC システムは符号化効率にほとんど影響を与えないことが分かる．

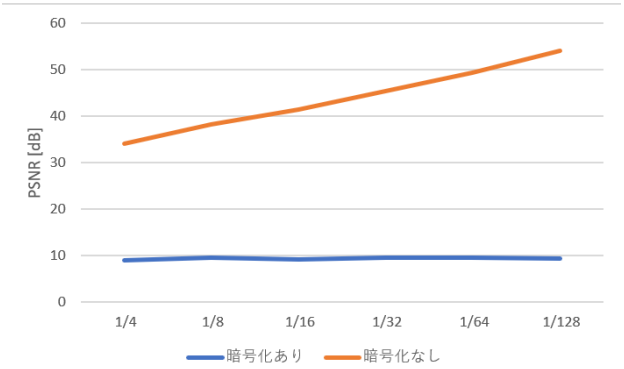

図 4: 暗号化の有無がスクランブルの程度に与える影響 (PSNR [dB] を用いた客観画質評価結果)

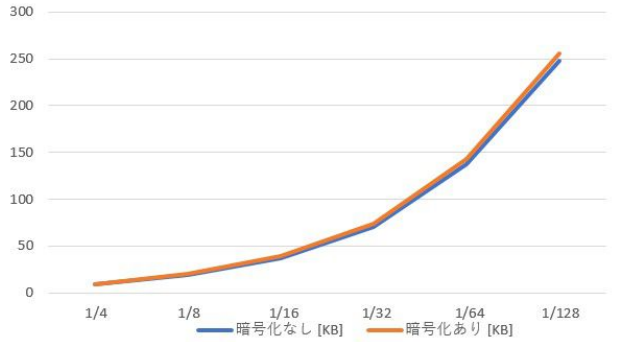

図 5: 暗号化の有無が符号化画像のサイズ (KB) に与える影響

4. まとめ

暗号化後の画像データと暗号化を行わなかった画像データにはファイルサイズに大きな差はなく，今回暗号化した画像の PSNR 値を平均すると 9.3158 [dB] と，圧縮率にかかわらずどれも小さい値になることが確認できた．以上の結果から，提案した EtC システムは HTJ2K によって符号化される画像のプライバシー保護に利用可能であると考えている．

参考文献

[1] ISO/IEC 15444-15:2019, “Information technology - JPEG 2000 image coding system - Part 15: High-Throuput JPEG 2000, ” 2019.

[2] O. Watanabe, A. Uchida, T. Fukuhara and H. Kiya, “An Encryption-then-Compression system for JPEG 2000 standard,” IEEE ICASSP, 2015, pp. 1226-1230, doi: 10.1109/ICASSP.2015.7178165.