

JPEG ビットストリーム領域でのファイルサイズ不変画像暗号化法

小林 弘幸[†] 貴家 仁志^{††}

[†] 東京都立産業技術高等専門学校 〒140-0011 東京都品川区東大井 1-10-40

^{††} 首都大学東京システムデザイン学部 〒191-0065 東京都日野市旭が丘 6-6

E-mail: [†]hkob@metro-cit.ac.jp, ^{††}kiya@tmu.ac.jp

あらまし 本報告では、JPEG 画像に対するビットストリームレベルでの暗号化法を提案する。提案法は、暗号化後も JPEG 形式を保持し、かつそのファイルサイズは、暗号化前のサイズと完全一致することを可能とする。JPEG 画像に対するビットストリームレベルでの暗号化手法はこれまでに数多く提案されているが、それらは暗号化過程において特殊命令コードであるマーカコードが発生・消失してしまうため、暗号化前後でファイルサイズが変更されてしまう。提案法では、JPEG ビットストリームを入力し、ハフマン符号の付加ビット成分を、今回提案される条件に従い選択的に暗号化する。暗号化前後で、ファイルサイズを変化させないという特徴は、画像データの送信処理で記録されたデータサイズが、フック処理による暗号化画像への置換処理後が変わってしまうことを回避し、フック処理後の継続処理を正しく動作させることを保証する。

キーワード JPEG, 暗号, ビットストリーム領域

A Generation Scheme of Encrypted JPEG Images with Unchanged File Sizes in the Bitstream Domain

Hiroyuki KOBAYASHI[†] and Hitoshi KIYA^{††}

[†] Electric and Electric Engineering Course,
Tokyo Metropolitan College of Industrial Technology, 140-0011, Tokyo, Japan

^{††} Department of Information and Communication Systems,
Tokyo Metropolitan University, 191-0065, Tokyo, Japan

E-mail: [†]hkob@metro-cit.ac.jp, ^{††}kiya@tmu.ac.jp

Abstract An encryption scheme of JPEG images in the bitstream domain is proposed. The proposed scheme preserves the JPEG format even after encrypting the images, and the file size of encrypted images is the exact same as that of the original JPEG images. Several methods for encrypting JPEG images in the bitstream domain have been proposed. However, since some marker codes are generated or lost in the encryption process, the file size of JPEG bitstreams is generally changed due to the encryption operations. The proposed method inputs JPEG bitstreams and selectively encrypts the additional bit components of the Huffman code in the bitstreams. This feature allows us to have encrypted images with the same data size as that recoded in the image transmission process, when JPEG images are replaced with the encrypted ones by the hooking, so that the image transmission are successfully carried out after the hooking.

Key words JPEG, Encryption, Bitstream domain

1. ま え が き

デジタルカメラやスマートフォンの普及により、デジタル画像を利用する機会が増大している。一般的に、撮影した画像は即座に JPEG 符号化され記録される。これらの画像はユーザの端末に保管されるだけでなく、ソーシャルネットワークや

クラウドフォトサービスなどにアップロードすることが多い。これらのクラウドサービスの多くは、任意のファイルを受け付けるわけではなく、指定された画像のファイル形式であることを要求している。また、このようなクラウド環境は、プロバイダの信頼性やユーザーの操作ミスなしを前提としており、決してユーザにとって信頼できる状況ではない。このような背景

から、画像形式を保ったまま画像を暗号化する方法が盛んに研究されている。

Encryption Then Compression システム (以下 EtC と呼ぶ) [1]~[11] は、符号化前の画像に対して暗号化を行う方式である。この方式は暗号化後に圧縮を可能としており、プロバイダーによる再圧縮などへの耐性も考慮されている。EtC の圧縮特性は、非暗号化時とほぼ同程度であるが、両者のファイルサイズは一致しない。また、ビットストリームで暗号化を実施する手法もいくつか提案されている [12]~[17]。JPEG 2000 画像に対しては、暗号化に伴う特殊命令コードの発生を考慮し、かつファイルサイズを変更しないビットストリームレベルでの暗号化方式が提案された [12]~[14]。JPEG 画像に対しても、ビットストリームレベルでの暗号化方式は提案されているが、バイトスタッフィングの有無が生じてしまいファイルサイズが変更してしまっている [15]~[17]。例えば、[15] では AC 係数のランレングスをビットストリームのまま並び替えを行うことで、ファイルサイズを保ったまま暗号化を実施することを試みたが、並び替えにより発生する疑似マークコードの回避については検討されていない。この場合、暗号化されたビットストリームをデコード時に正しく復号ができないか、またはファイルサイズが変化してしまう。さらに、[16],[17] の手法では、ビットストリームレベルでのブロックスクランブルや係数スクランブル等を実施している。これらの手法では JPEG 形式を正確に保持するために、バイトスタッフィングの影響を考慮して暗号化処理を実行しているが、暗号化前後で数バイトの変化が発生することが示されている。

このような背景から、本稿では、暗号化前後でファイルサイズを変化させない、ビットストリームレベルでの JPEG 画像に対する暗号化手法を提案する。提案法が想定する環境は、アプリケーションに暗号化システムを内蔵する形式ではなく、通信路内で画像情報をフックして暗号化を実施する形式である。このような通信路においては、アプリケーション・サーバ間でファイルサイズの情報をやりとりしていることが考えられるため、暗号化前後でファイルサイズ一定であることが望まれる。提案法は暗号化過程において、JPEG マークコードの発生・消失を回避する仕組みを設けることで、ファイルサイズ一定を保証するものである。

2. 既存手法とその問題

2.1 JPEG ビットストリーム [18]

ここでは、JPEG ビットストリームの構成について述べる。図 1(a) は JPEG ビットストリーム全体の構成を示したものである。図中の SOI(Start of Image) および EOI(End of Image) はそれぞれ、JPEG ビットストリームの開始と終了を示すマークコードである。マークコードは 16 進数で「FFxx」という形で示される特殊なコードであり、後段の“image data”以外の Segment の先頭にも設置される。これら Segment 内には量子化テーブルやハフマンテーブルなど、復号に必要な情報が記録されている。各 Segment の識別はマークコードの二バイト目(上記 xx の部分)で行われる。

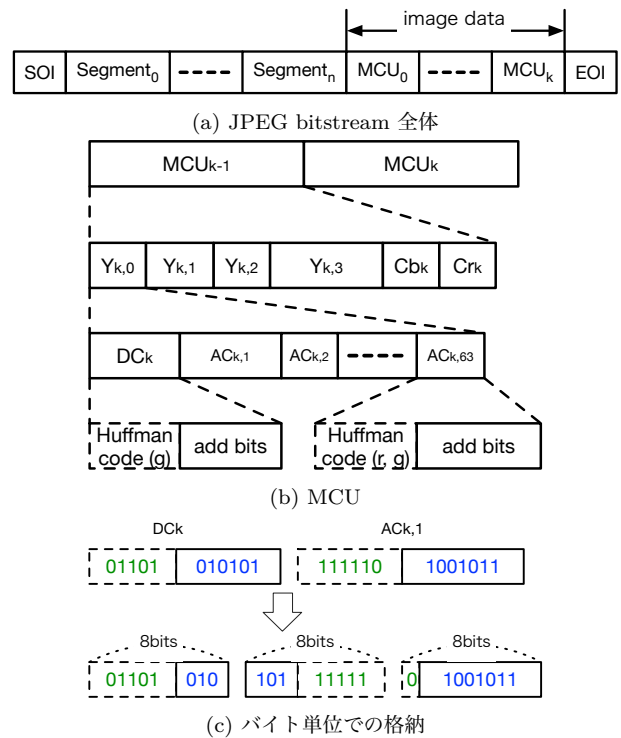


図 1 JPEG ビットストリームの構成

図 1(b) は“image data”内の構造である。“image data”は MCU (Minimum Coded Unit) と呼ばれる単位で順に格納される。図は色間引き 4:2:0 の場合の例であり、各の MCU に 8×8 の輝度ブロック (Y) が 4 つ、間引き後の色差ブロック (Cb, Cr) がそれぞれ 1 つ格納されている。一つのブロックには、前のブロックの DC 係数との差分値である DC_k と 63 個の AC 係数 $AC_{k,n}$ ($n = 1 \dots 63$) が格納されている。さらに各系数値は、値の範囲を決めるグループ番号 (g) を示すハフマンコードと範囲内の値を一意に特定するための付加ビット (add bits) で構成される。また、AC 係数の場合はハフマンコードの中に、有意な値が存在するまでのゼロ値のランレングス (r) も含まれている。

図 1(c) は具体的なハフマンコードと付加ビットを例示したものである。各データは可変長ビットで構成されているため、バイト単位に整列されて格納される。“image data”終了時にバイト区切りに達していなかった場合には、残りのビット部分に 1 がパディングされる。

2.2 ファイルサイズ変化の原因

“image data”を構成するハフマンコードおよび付加ビットは、任意の値を取りうるため、バイトスタッフィング処理によって特別な意味を持つマークコードと同じビット配列が発生してしまう可能性がある。このため、JPEG 符号化ではマークコード回避するための対策が実施されている。図 2 にその手順を例示している。同図は、図 1(c) の DC_k の最後の 3bit を「111」に変更したものである。この時、バイトスタッフィングされたデータの 2 バイト目は全て「1」となり、マークコードの 1 バイト目である「FF」と一致してしまう。マークコードとの誤認を防ぐために、エンコーダでは「FF」の直後に「00」を挿入する。一方、デコーダ側では、「FF00」というデータを読み込

生・消失する場合があるため、暗号化は行わない。

(3) FF の直後の 00 の場合: 付加ビット分ではないので、暗号化は行わない。

(4) 一部にハフマンコードが含まれ、そのコードのビットが全て 1 の場合: 暗号化により FF が発生・消失する場合があるため、暗号化は行わない。

(5) 一部にハフマンコードが含まれ、そのコードのどこかに 0 が含まれる場合: 暗号化により FF が発生・消失することがないため、付加ビット部分のみを暗号化する。

(6) DQT segment の Q-table は常に暗号化可能である。

また、提案法ではどの部分を暗号化するかについて、暗号化側と復号側での同意により調整することが可能である。AC 係数のみを暗号化した場合、暗号化されたビットストリームの直流成分は保持されるため、半開示のような効果を得ることも可能である。また、画像のブロック位置は保持されているため、両者の合意のもとで一部分だけを暗号化することも可能である。ただし、この場合復号するためのキーだけでなく、暗号化した場所の情報も共有する必要がある。

4. シミュレーション

提案法の有効性を示すためにシミュレーションで確認した。実験は JPEG が配布しているリファレンスソフトウェア [19] を利用し、4:2:0 の色間引きの下で実行された。

4.1 暗号化画像の画質評価

まず、暗号化した画像の画質を評価した。図 5(a) は標準画像 lena を Q-factor 80 で符号化したものである。この符号化列をオリジナルとし、提案法で処理部分を変化させながら暗号化を実施した。同図 (b)~(f) は暗号化後のビットストリームを標準の JPEG デコーダで復号した画像である。

図 5(b) は DC 成分のみを暗号化した画像である。DC 成分は画像のエネルギーを保持する部分であるため、排他的論理和で値が大きく変更されたブロックにおいて大きく色や振幅が変化している。また、DC 成分は差分値が記録されているため、水平方向に値を引きずっていることがわかる。AC 成分は保持しているため、画像の輪郭は一部残っている。

一方、図 5(c) は AC 成分のみを暗号化した画像である。DC 成分が変化しておらず、画像の外観はほぼ保持している。図 5(d) は、DC、AC の両成分を暗号化したため、(b)、(c) に比べ現画像の情報がさらに失われていることがわかる。

図 5(e) は、量子化テーブルのみを暗号化したものである。量子化テーブルはある程度推定できるので、これ単体では暗号化の効果は少ないが、(d) と組み合わせることで図 5(f) の結果を得ることができる。

4.2 暗号化対象バイト

表 2 は、“image data” 内の付加ビットに対して暗号化が施された比率を示したものである。除外されたデータは 3.3 の条件 (2)(4) に該当するデータ数である。Q-factor が大きくなるほど暗号化対象の割合が小さくなっていることがわかる。これは、Q-factor が大きくなるに従い量子化後の DCT 係数の値が大きくなり、add bits のデータ量が増え、必然的に条件 (2) に

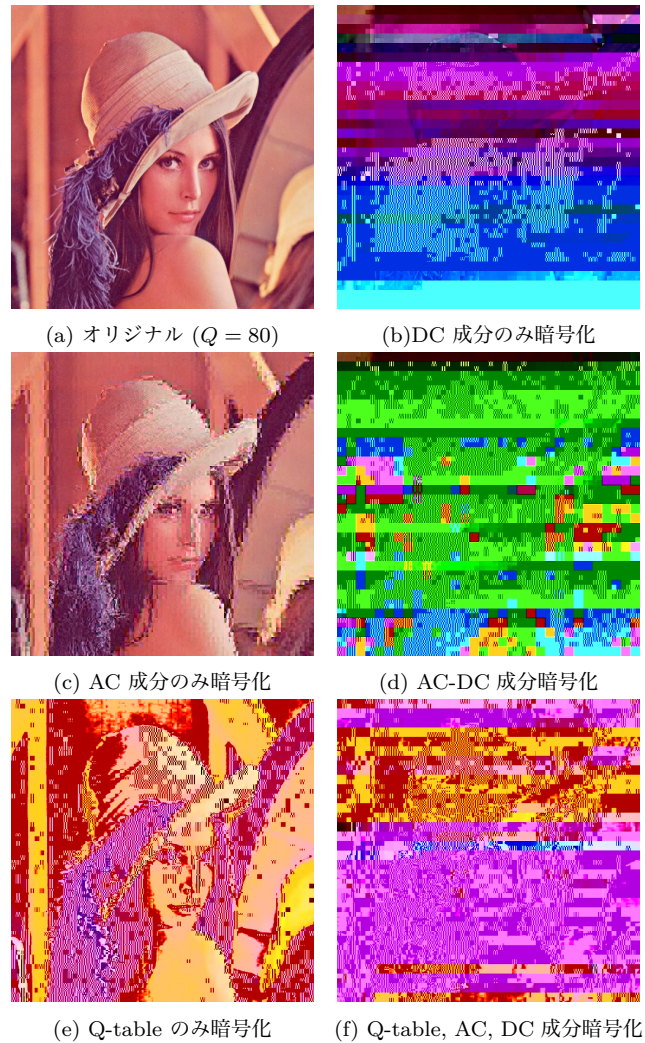


図 5 オリジナル画像と提案法による暗号化結果 (lena)

表 2 暗号化対象バイト / 暗号化除外対称バイトの総量 (画像 lena)

種別	(a) Q = 50		暗号化対象の割合 [%]
	暗号化除外対象 [byte]	暗号化対象 [byte]	
DC 成分のみ	70	4,729	98.5
AC 成分のみ	172	9,591	98.2
全成分	197	13,467	98.6
種別	(b) Q = 80		暗号化対象の割合 [%]
	暗号化除外対象 [byte]	暗号化対象 [byte]	
DC 成分のみ	420	6,306	93.8
AC 成分のみ	460	20,931	97.8
全成分	741	26,104	97.2
種別	(c) Q = 95		暗号化対象の割合 [%]
	暗号化除外対象 [byte]	暗号化対象 [byte]	
DC 成分のみ	1,758	7,152	80.2
AC 成分のみ	3,225	59,063	94.8
全成分	4,336	65,274	93.8

該当するバイト数が増えてしまうからである。

4.3 ファイルサイズの変化

表 3 は暗号化前後のファイルサイズの変化を示したものである。ただし、EtC については暗号化後にオリジナルと同じ

表3 ファイルサイズの変化 (() 内はオリジナルとの差)[byte]

Q-factor	50	80	95
オリジナル	24,279	43,879	106,548
Proposed	24,279(0)	43,879(0)	106,548(0)
Cheng [17]	24,281(+2)	43,865(-14)	106,553(+5)
EtC [1]	24,767(+488)	44,487(+608)	108,262(+1,714)

Q-factor で符号化している。EtC に関しては 16×16 単位でブロックスクランブルのみを実施したものである。MCU 内の組み合わせは変わらないため、同一 Q-factor で符号化している場合、AC 係数についてはオリジナルと同一係数になる。しかしブロックの並び替えにより、DC 係数の差分値が大きくなるため、ファイルサイズが変化する。また、Chang らのビットストリームレベルの暗号化は EtC に比べて、ファイルサイズの変化が少ない。しかしながら、2.2 で示したように、ブロック入れ替え等による「FF00」コードの発生・消失があるため、ファイルサイズが増加・減少してしまっているのがわかる。

一方、提案法は「FF00」コードの発生・消失するパターンを回避しているため、オリジナルと同一のファイルサイズとなっていることがわかる。

5. おわりに

今回の報告では、暗号化前後でファイルサイズを変化させない暗号化手法を提案した。提案法は暗号化過程において、JPEG マーカーコードの発生・消失を回避する仕組みを設けることで、ファイルサイズ一定を保証するものである。ファイルサイズが変更されないことで、通信途中における画像ファイルのフック処理などへの応用が期待できる。シミュレーションにより、提案法の効果が確認できた。

謝 辞

本研究の一部は、JSPS 科研費 JP17H03267 (基盤研究 (B) 一般)「プライバシー保護のための画像圧縮を可能とする知覚暗号化とその攻撃耐性」の助成を受けたものである。

文 献

- [1] Kenta Kurihara, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya: "An Encryption-then-Compression System for JPEG / Motion JPEG Standard," IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238-2245, November 2015.
- [2] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," IEEE Trans. on information forensics and security, vol. 9, no. 1, pp. 39-50, 2014.
- [3] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, "An encryption-then-compression system for JPEG 2000 standard," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2015, pp. 1226-1230.
- [4] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg standard," Picture Coding Symposium (PCS), 2015, pp. 119-123.
- [5] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An Encryption-then-Compression System for JPEG / Motion JPEG Standard," IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238-2245, November 2015.
- [6] K. Kurihara, O. Watanabe, and H. Kiya, "An encryption-then-compression system for jpeg XR standard," in IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2016, pp. 1-5.
- [7] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for lossless image compression standards," IEICE Trans. Inf. & Syst., vol. E100-D, no. 1, pp. 52-56, 2017.
- [8] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based etc systems against jigsaw puzzle solver attacks," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp. 2157-2161.
- [9] T. Chuman, K. Kurihara, and H. Kiya, "Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle solver attacks," IEEE International Conference on Multimedia and Expo (ICME), 2017, pp. 229-234.
- [10] Tatsuya Chuman, Kenta Iida, and Hitoshi Kiya, "Image Manipulation on Social Media for Encryption-then-Compression Systems," Proc. APSIPA Annual Summit and Conference, Kuala Lumpur, Malaysia, 14th December, 2017.
- [11] Tatsuya Chuman, Kenta Kurihara, and Hitoshi Kiya "On the Security of Block Scrambling-based EtC Systems against Extended Jigsaw Puzzle Solver Attacks," IEICE Trans. Inf. & Sys., vol.E101-D, no.1, pp.37-44, January 2018.
- [12] 岩村 恵市, 林 淳一: "JPEG2000 符号化画像のマーカーコード発生を回避できる暗号化方式," 信学論 (A) vol. J90-A no. 11, pp. 839-850, Nov. 2007.
- [13] H. Kiya, S. Imaizumi, and O. Watanabe, "Partial-Scrambling of Image Encoded Using JPEG2000 without Generating Marker Codes," Proc. IEEE International Conference on Image Processing (ICIP), no.WA-P1.3, 17th September, 2003.
- [14] 貴家 仁志, 今泉 祥子, 渡邊 修, "マーカーコードの発生を考慮した JPEG2000 符号化画像の情報開示法," 信学論 (D-II), vol.J86-D-II, no.11, pp.1628-1636, Nov. 2003.
- [15] Unterweger, Andreas and Uhl, Andreas: "Length-preserving Bit-stream-based JPEG Encryption," Proceedings of the on Multimedia and Security, MM&Sec '12, pp. 85-90, 2012.
- [16] X. Niu, C. Zhou, J. Ding and B. Yang, "JPEG Encryption with File Size Preservation," 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, 2008, pp. 308-311.
- [17] Cheng, Hang and Zhang, Xinpeng and Yu, Jiang and Zhang, Yuan: "Encrypted JPEG Image Retrieval Using Block-wise Feature Comparison," J. Vis. Comun. Image Represent., Vol.40, pp. 111-117, 2016.
- [18] "Information technology-Digital compression and coding of continuous-tone still images: Requirements and guidelines," International Standard ISO/IEC IS-10918-1, Feb. 1994.
- [19] "Text of CD ISO/IEC 18477-5 (Reference Software)," ISO/IEC JTC 1/SC 29/WG 1 N69019, Jun. 2015.