様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２１　日現在

機関番号：　１２５０１
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６８２０１３８

研究課題名（和文）画像情報に対するハイブリッド型多重情報ハイディングの研究

研究課題名（英文）A Study on Reversible Information Hiding with Image Scrambling Encryption

研究代表者
今泉　祥子（Imaizumi, Shoko）

千葉大学・大学院融合科学研究科・准教授

研究者番号：８０５３５０１３

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究では、不正な二次利用による著作権侵害や画像に含まれるプライバシ侵害、また、画像の改ざんによる真正性の損失などの問題に対応することを目的とし、著作権や真正性を保証する電子透かし技術と、画像情報をある程度劣化させることでプライバシ情報を保護する情報半開示法を同時に実現する画像保護技術について研究した。また、情報を多重に埋め込むことにより、改ざん位置の特定精度の向上を図り、同時に、暗号鍵の効率的な生成手法についても検討を行った。

研究成果の概要（英文）：In an effort to achieve the protection of copyrights, privacy, and authenticity of digital images simultaneously, we studied a hybrid method with data hiding and block-permutation-based encryption in this research. Additionally, we also improved the accuracy for detection of the tampered area by a multiple information hiding technique and focused on effective key derivation schemes.

研究分野：　マルチメディアセキュリティ

キーワード：　情報ハイディング　電子透かし　ブロックスクランブル暗号化　情報半開示　画像符号化　鍵生成

１．研究開始当初の背景

近年、通信路や通信端末の急速な発達に伴い、ホームページや SNS などネットワークを介したディジタル画像の公開が一般的となった。しかし一方で、公開された画像が、第三者によって不正に改ざんされたり、二次利用されたりする問題が多く生じている。これに対して、著作権情報や撮影日時・場所などの固有データをコンテンツに埋め込む、電子透かし技術について多くの研究がなされている。これらの研究では、一般に、埋込による画質劣化を抑え、かつ、想定される様々な攻撃に対して安全性を保持することが考慮されている。また、電子透かし技術の利用により、改ざん検出やその位置推定を行うことが可能となっている。これは、原画像の特徴量をそれ自身に埋め込むことにより、改ざん検出過程において、埋め込まれた原画像の特徴量と、再度算出される検査対象画像の特徴量とを比較し、改ざんの有無を検定するものである。このように、電子透かしでは、不正な二次利用や改ざんを抑止することを目的としている。

一方、ネットワーク上で公開される画像には、顔部をはじめとする身体的特徴や、文字として表わされる個人情報など、個人を特定可能な内容が含まれていることが多い。それにも関わらず、これらの内容を含む画像が、本人の許可なく無断で公開されることが問題となっており、公開画像に対するプライバシ保護が求められている。このとき、画像のプライバシ保護の手段として、一般に二つの手法が挙げられる。一つは、画像情報全体の暗号化である。この手法は画像保護の手段としては堅牢であるが、内容の確認ができず、画像検索などの機能に制約を与える。また、この手法を用いて暗号化された暗号化画像は、のちに圧縮処理を施した際に圧縮効率が著しく損なわれるため、暗号化後に圧縮処理を施すことは考慮されていない。そこで、情報半開示法が研究されてきた。これは、画像に対して、その内容が確認できる程度に品質を劣化させる手法である。この情報半開示法は、インターネットサービスにおける重要なセキュリティ技術の一つとして、すでに広く提供されている。

上述の電子透かし法と情報半開示法は、代表的な情報ハイディング技術である一方、その目的の違いにより、秘匿する情報がそれぞれ異なっている。前者は、画像の著作権や真正性を保証した状態で画像全体を一般に公開することを目的とし、画像情報に対して別の情報を秘匿する手法である。一方、後者は、画像内容の一部のみを一般に公開して全体情報は特定のユーザにのみ公開するという目的から、画像情報自身を秘匿する手法である。これらの手法は画像保護技術として非常に有用であるが、両者の目的を同時に実現する安全かつ効率的な手法は実現されていない。

２．研究の目的

(1)　著作権保護および改ざん検出の機能を有する電子透かしと、プライバシ保護の機能を有する情報半開示のハイブリッド化を行う。例えば、図１に示すように、透かし情報が埋め込まれた画像に対して情報半開示処理を施すことで、半開示が解除された元の画像に対して透かし情報が保持される手法を実現する。ここで、電子透かしと情報半開示を単純に組み合わせた場合、一方の効果が減少または損失する可能性がある。そのため、研究期間内に両者の機能を損なうことなく持続または向上させ、両者の特徴を同時に実現できる技術を研究する。ただし、後述の多重情報ハイディング処理を考慮して、透かし画像から原画像と埋込情報をともに復元可能な、可逆電子透かしによる手法を検討する。また、電子透かしにおいて、埋込み処理後の画像に対して一定の画質を保証する。

図１ ハイブリッド化の例

(2)　画像に改ざんが認められた場合、改ざん位置を精細に推定するために、可逆電子透かし法を用いて、埋込位置を変更しながら透かし情報を繰り返し埋め込む手段を研究する。ここで、埋込・抽出過程では検査鍵が用いられる。画像所有者はこの鍵を用いて、透かし情報の埋込と抽出をそれぞれ行い、改ざん検出や位置推定を行うことができる。検査鍵が漏洩した場合には第三者による不正な抽出や再埋込の防止、紛失した場合には所有者が再度検査鍵を取得可能な手段をそれぞれ検討することが求められる。この要求に対応するため、鍵漏洩・紛失の耐性を考慮する。

３．研究の方法

(1)　電子透かしと情報半開示の相互利用により著作権・プライバシの保護、および、改ざん検出を同時に有効とする二つの手法について検討する。まず原画像に透かし情報を埋め込み、生成された透かし画像に対して情報半開示処理を施す手法について検討する。これにより、プライバシ保護のためのスクランブルが解除された後も、著作権保護および改ざん検出の機能が電子透かしにより保持される。なお、両者の機能を損なわず、持続・向上させることを前提とする。

電子透かしは、その強度によってロバスト型とフラジール型に大別される。ロバスト型は攻撃耐性が強く、フラジール型は弱い。そのため、フラジール型は主に改ざん検出に利用されている。一方、電子透かしは、透かし画像から透かし情報と原画像をともに復元

できる可逆型と、透かし情報のみを復元できるが、原画像の復元はできない非可逆型にも分けられる。一般に、ロバストかつ可逆な電子透かしの開発は難解であるとされている。本研究では、改ざん検出機能を有効とするため、まずフラジール型を適用する。また、開発手法において、透かし画像の画質を埋込前の画像と比較して評価する。具体的には、PSNR や SSIM を用いた定量評価を行う。

(2)　可逆電子透かしを用いて、ハイディング処理を階層化し多重に施すことにより、改ざん検出とその位置推定を切り分け、さらに位置推定を効率的に実現可能な手法を研究する。多重情報ハイディング処理のため可逆電子透かしの利用が不可欠となる。また、鍵生成・管理に関して、一方向性ハッシュ関数を利用するなど、利便性と安全性を考慮した手法を研究する。

４．研究成果

(1)　図 2 に示す、可逆電子透かし（可逆情報埋込みともいう，以降 RDH と呼ぶ）と暗号化処理の二つの機能を有した暗号化システムについて研究した。

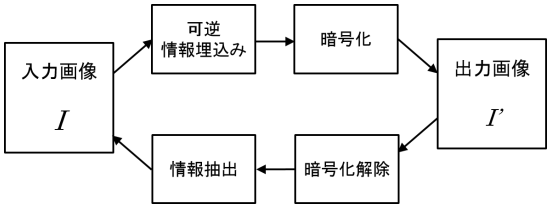


図 2　ハイブリッド型暗号化システム

まず、RDH に関して、Histogram Shifting（以降 HS と呼ぶ）による手法[1]をカラー画像に適用し、原画像の画質を大きく損なうことなく情報を埋め込む。

次に、埋め込まれた画像に対して、ブロックスクランブル暗号化[2]を施す。この暗号化手法では、図 3 に示すように、画像を一定サイズのブロックに分割した後、各ブロックに対して四つのスクランブル処理を施すことで、暗号化画像を生成する。

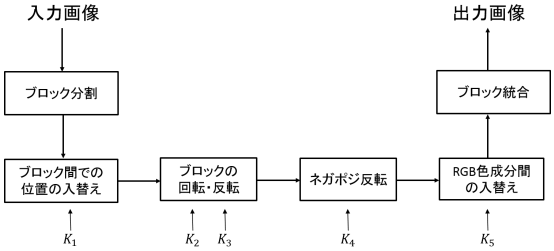
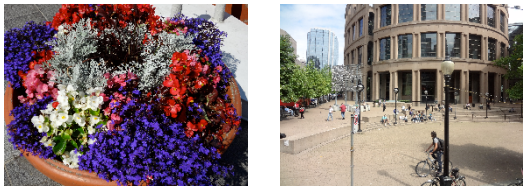
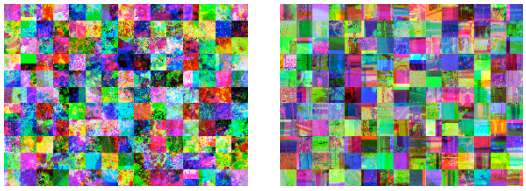


図 3　ブロックスクランブル暗号化法[2]

図 4 に、提案法を用いて生成された埋込・暗号化画像を示す。試験画像のサイズは 4608×3456 画素、ブロックサイズは 320×320 画素である。同図より、本手法で生成された画像は、原画像を推定困難な程度に暗号化されていることが確認できる。



(a) 原画像（Library）　(b) 原画像（Flower pot）



(c) 埋込・暗号化画像（Library）　(d) 埋込・暗号化画像（Flower pot）

図 4　埋込・暗号化画像の例

また、RDH 後の画像の PSNR はいずれも 40 dB 以上であることを確認している。

参考文献

[1] Z. Ni, et al., “Reversible Data Hiding,” IEEE Trans. Circuits Syst. Video Technol., vol.16, No. 3, pp.354-362, 2006.
[2] K. Kurihara, et al., “An Encryption-then-Compression System for JPEG/ Motion JPEG Standard,” IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238-2245, 2015.

(2)　本研究では、主に JPEG2000 符号化画像を対象に、その符号化列の構造を考慮した、RDH 手法を研究した。JPEG2000 符号化列内には、データを区切るためのマーカコードと呼ばれる特殊命令コードが存在する。マーカコードには、画像を復号するために必要な情報が含まれており、情報埋込みの際に消失したり、新たに発生させたりすると、画像の再生が正しく行われない。そのため、符号化列内にマーカコードを新たに発生させることなく可逆に情報を埋め込み、改ざん検出を実現する。この手法の特徴は、JPEG2000 の機能である階層的な再生に対応した情報埋込みを行うことで、様々な画質での復号画像に対して改ざん検出を行うことができる点である。

PWLC 情報埋込み[3]に基づくアルゴリズムにより、図 5，6 に示すように、各暗号化ハッシュ値を、レイヤ i、および、解像度レベル j における、最下位 JPEG2000 パケット（またはボディデータ）にそれぞれ多重に埋め込む。最下位 JPEG2000 パケットへの埋込みができない場合、埋込み可能な最下位 JPEG2000 パケットに埋め込む。

改ざん検出は、図 7，8 に示すように、レイヤあるいは解像度のいずれを指定して画像再生を行う場合でも、情報が埋め込まれた JPEG2000 パケットから埋込み情報を抽出可

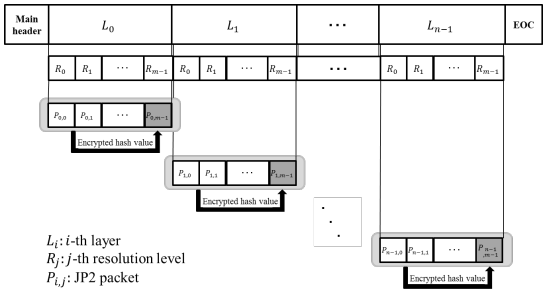


図 5　レイヤに対するハッシュ値の埋込み

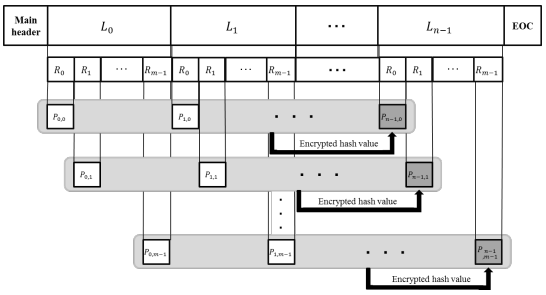


図 6 解像度レベルに対するハッシュ値の埋込み

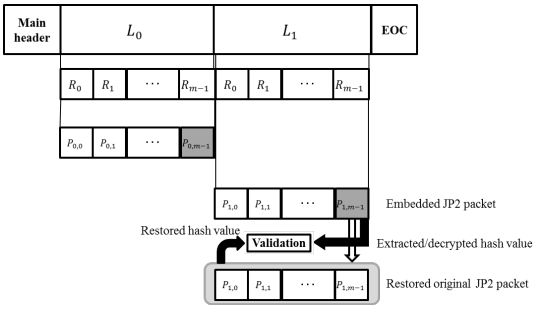


図 7　改ざん検出の例（レイヤ 0, 1 指定による画像再生の場合）

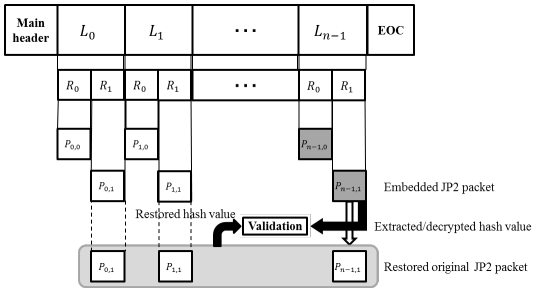


図 8　改ざん検出の例（解像度レベル 0, 1 指定による画像再生の場合）

能である。

また、埋込み画像の画質について、試験画像 Lena を用いて SSIM により評価した。その結果、ハッシュ長が 4 ビットで 0.9824、16 ビットで 0.9655、 64 ビットで 0.9294 となった。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　4　件）

1. Kenta KURIHARA, Shoko IMAIZUMI, Sayaka SHIOTA and Hitoshi KIYA, “ An Encryption-then-Compression System for Lossless Image Compression Standards,” IEICE Trans. Inf. & Syst., vol.E100-D, no.1, pp.52-56, January 2017. （査読有）

2. Anu ARYAL, Shoko IMAIZUMI, and Takahiko HORIUCHI, “Hierarchical Scrambling Method for Palette-Based Image Using Bitwise Operation,” Bull. Soc. Photogr. Imag. Japan, vol.26, no.1, pp.1-9, June 2016. （査読有）

3. 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. （査読有）

4. Shoko IMAIZUMI and Kei OZAWA, “Palette-Based Image Steganography for High-Capacity Embedding,” Bull. Soc. Photogr. Imag. Japan, vol.25, no.1, pp.7-11, June 2015. （査読有）

〔学会発表〕（計　16　件）

1. Shoko IMAIZUMI, Takeshi OGASAWARA, and Hitoshi KIYA, “ Block-Permutation-Based Encryption Scheme with Enhanced Color Scrambling,” in Proc. of Scandinavian Conference on Image Analysis, LNCS 10269, pp.562-573, 13th June 2017, Scandic Ishavshotel (Tromso, Norway)

2. 氏家啓貴, 茂木一磨, 小笠原剛史, 今泉祥子, 城野誠治, 皿井舞, “文化財画像のための暗号化システムの開発,” 日本写真学会年次大会, no.B1p, p.155, 2017 年 6 月 20 日, 一橋講堂（東京都千代田区）.

3. 小笠原剛史, 今泉祥子, 貴家仁志, “攻撃耐性向上のためのブロックスクランブル暗号化法とその鍵管理,” 電子情報通信学会 EMM 研究会, vol.116, no.501 (EMM2016-91), pp.31-36, 2016 年 3 月 6 日, 宮古島マリンターミナルビル（宮古島市）.

4. Kazuma MOTEGI and Shoko IMAIZUMI, “Image Authentication Scheme with Localization Using YIQ Color Space,” in Proc. of International Workshop on Advanced Image Technology, 9th Jan. 2017, Hotel Equatorial Penang (Penang, Malaysia).

5. 小笠原剛史, 今泉祥子, 貴家仁志,“ロスレス画像圧縮のためのカラーブロックスクランブル暗号化法の拡張,”電子情報通信学会 EMM 研究会, vol.116, no.303 (EMM2016-61), pp.43-48, 2016年11月17日, コンパルホール（大分市）.

6. 石塚賢人, 今泉祥子, 青木直和,“JPEG圧縮を考慮したカラー画像に対する知覚暗号化法,”日本写真学会年次大会, no.A5p, p.194, 2016年6月8日, 東京工業大学すずかけ台キャンパス（横浜市）.

7. 中尾友哉, 今泉祥子, 青木直和,“視認困難性を考慮した可逆画像符号化のための知覚暗号化方式,”電子情報通信学会 EMM 研究会, vol.115, no.479 (EMM2015-85), pp.51-56, 2016年3月2日, 屋久島環境文化村センター（屋久島町）.

8. 茂木一磨, 今泉祥子, 青木直和,“YIQ色空間を用いたカラー画像のための改ざん検出法,” 電子情報通信学会 EMM 研究会, vol.115, no.479 (EMM2015-79), pp.19-24, 2016年3月2日, 屋久島環境文化村センター（屋久島町）.

9. Takeshi OGASAWARA, Shoko IMAIZUMI, and Naokazu AOKI,“Scalable Tamper Detection and Localization Scheme for JPEG2000 Codestreams,”in Proc. of Pacific-Rim Conference on Multimedia, LNCS 9315, pp.340-349, 17th Sep. 2015, Gwangju Institute of Science and Technology (Gwangju, Korea).

10. Anu ARYAL, Kazuma MOTEGI, Shoko IMAIZUMI, and Naokazu AOKI,“Improvement of Multibit Information Embedding Algorithm for Palette-Based Images,”in Proc. of Information Security Conference, LNCS 9290, pp.511-523, 11th Sep. 2015, (Trondheim, Norway).

11. Anu ARYAL, Shoko IMAIZUMI, and Naokazu AOKI,“Hierarchical Scrambling for Palette-Based Images Using Transposition Cipher,”in Proc. of International Conference on Advanced Imaging, no.T109-01, pp.701-704, 19th June 2015, 一橋講堂（東京都千代田区）.

12. 小笠原剛史, 今泉祥子, 青木直和, 小林裕幸,“可逆情報埋込みを用いた JPEG2000符号化画像の改ざん検出法,”電子情報通信学会 EMM 研究会, vol.114, no.511 (EMM2014-82), pp.31-36, 2015年3月12日, 大濱信泉記念館（石垣市）.

13. 茂木一磨, 今泉祥子, 青木直和, 小林裕幸,“限定色画像に対する多ビット情報埋込み方式の改善,”電子情報通信学会 EMM 研究会, vol.114, no.511 (EMM2014-79), pp.13-17, 2015年3月12日, 大濱信泉記念館（石垣市）.

14. 中尾友哉, 今泉祥子, 青木直和, 小林裕幸,“ROI領域に対するJPEG2000符号化画像の選択的暗号化方式,”電子情報通信学会 MM 研究会, vol.114, no.511 (EMM2014-78), pp.7-12, 2015年3月12日, 大濱信泉記念館（石垣市）.

15. 武田耀, 今泉祥子, 青木直和, 小林裕幸,“HAMを用いた暗号化型可逆情報埋込法,”電子情報通信学会 EMM 研究会, vol.114, no.424 (EMM2014-68), pp.9-14, 2015年1月28日, 東北大学（仙台市）.

16. Anu ARYAL, Shoko IMAIZUMI, and Naokazu AOKI,“Hierarchical Scrambling Scheme for Palette-Based Images,”in Proc. of IEEE International Symposium on Intelligent Signal Processing and Communication Systems, no.74, pp.65-70, 2th Dec. 2014, Hilton Kuching (Kuching, Malaysia).

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
2017年6月20日: 2017年度日本写真学会年次大会最優秀研究発表ポスター賞受賞（受賞者: 氏家啓貴）

参考ホームページ:
http://foto.tp.chiba-u.jp/publication-j.html
http://www.tj.chiba-u.jp/imgsci/

６．研究組織
(1)研究代表者
今泉　祥子　（IMAIZUMI, Shoko）
千葉大学・大学院融合科学研究科・准教授
研究者番号：８０５３５０１３

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
貴家　仁志（KIYA, Hitoshi）
首都大学東京・システムデザイン学部・教授
研究者番号：４０１５７１１０

城野　誠治（SHIRONO, Seiji）
皿井　舞（SARAI, Mai）
アリャル　アヌ（ARYAL, Anu）
石塚　賢人（ISHIZUKA, Kento）
中尾　友哉（NAKAO, Yuya）
茂木　一麿（MOTEGI, Kazuma）
小笠原　剛史（OGASAWARA, Takeshi）
武田　耀（TAKEDA, Hikaru）
氏家　啓貴（UJIIE, Hiroki）