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

令和　２ 年　 ９ 月 １５ 日現在

機関番号：２２６０４
研究種目：基盤研究(B)（一般）
研究期間：2017～2019
課題番号：１７Ｈ０３２６７

研究課題名（和文）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

研究課題名（英文）Compressible Percheptual Image Encryption for Privacy-Preseving and Its Robusness against Attacks

研究代表者
貴家　仁志（KIYA, HITOSHI）

首都大学東京・システムデザイン研究科・教授

研究者番号：４０１５７１１０

交付決定額（研究期間全体）：（直接経費）　　10,300,000円

研究成果の概要（和文）：クラウド環境の普及に伴い、種々のデータ処理をクラウド環境において実行することが可能となった。しかしプロバイダーの信頼性の不十分さや事故によって、不正データ使用、データ流出やプライバシーの侵害など、データユーザにとって深刻な種々の問題が未解決な状態にある。そこで encryption-then-compression (EtC),と呼ばれる圧縮可能な画像暗号化法について研究を行った。この暗号化法は、暗号化画像を直接圧縮できるために、クラウドプロバイダーに、画像の視覚情報を非公開にすることを可能にする。さらに提案法がジグソーパズル解法を含む種々の攻撃法に対して十分なロバスト性を有することを確認した。

研究成果の学術的意義や社会的意義
本研究により得られた結果及びその独創性は次の通りである．(a)国際標準の画像圧縮方式に適用可能な暗号化法を世界で初めて提案した．(b)ジグソーパズル解法を世界で初めて攻撃として捉え，暗号化の安全性を評価した．
また本研究の意義は次の通りである．(a)圧縮の前に暗号化処理が実行でき，プロバイダーの信頼性が低い場合にも，画像の持つプライバシーの保護や不正利用の防止が可能となる．(b)国際標準の圧縮方式が適用可能であり，広く技術が社会に普及することを期待できる．(c)暗号化処理，情報圧縮分野の融合に相当し，これらの分野の研究に新しい視点を与え，さらに学術的に新しい分野を拓くことが期待できる

研究成果の概要（英文）：With the wide/rapid spread of distributed systems for information processing, such as cloud computing and social networking, not only transmission but also processing is done on the internet. However, cloud environments have some serious issues for end users, such as unauthorized access, data leaks, and privacy compromise, due to unreliability of providers and some accidents. Accordingly, we studied compressible image encryption schemes, referred to as encryption-then-compression (EtC), although the traditional way for secure image transmission is to use a compression-then encryption (CtE) system. EtC systems allow us to close unencrypted images to network providers, because encrypted images can be directly compressed even when the images are multiply recompressed by providers. In addition, Images encrypted by using the proposed scheme were shown to have strong robustness against various attacks including jigsaw puzzles solvers.

研究分野：信号処理

キーワード：画像暗号化　圧縮可能暗号化　JPEG　情報セキュリティ　SNS　クラウド

1.　研究開発当初の学術的背景

SNS の普及に伴い，ネットワークを通じて画像及びビデオ映像を共有・流通することが一般的になっている．画像情報の多くは，個人情報などを含むため，そのプライバシー保護が必須となっている．多 くの SNS では，プライバシー保護のために，画像の公開範囲をユーザー自身が設定する機能を提供している．この機能の有効性は，SNS プロバイダおよび不特定多数の閲覧者が「信頼できる第三者(Trusted Third Party:TPP)」であるという前提に基づいている．一方で，SNS プロバイダが，ユーザーがアップロードした画像に対して再圧縮および付加情報の編集を行っていることが知られている．SNS プロバイダは，再圧縮時にオリジナルの画像情報を知ることができるため，画像のプライバシーは，ユーザーコントローラブル(制御下)でない．SNS プロバイダが TPP であるという保証はなく，さらに意図 しない情報流出等の事故も起こっている．したがって，従来のプロバイダ制御下にある公開範囲設定のような機能は，画像のプライバシーを保護することを保証していない．

以上の背景から、画像通信において，暗号化処理を画像に施した後に暗号化されたデータを圧縮するという手順への適用が注目されている。しかし，これまでの研究では，圧縮を可能とする幾つかの知覚暗号法の発見はあるものの，適用可能な圧縮方式は極めて限定されており，SNS で一般的な国際標準規格に準じた方式の適用は困難な状況にあった．JPEG 方式に代表されるような国際標準規格が適用可能な新しい画像の知覚暗号化法の開発が急務の課題であった。

2.　研究の目的

ソーシャル・ネットワーク・サービス(SNS)の普及により，膨大な数の画像がネットワークを通じて 共有･流通されている．これに伴い，画像のプライバシー保護技術が注目を集めている．本研究の目的は，ユーザー自身が画像のプライバシー情報を制御し，保護することを実現するために，知覚暗号化という新しい暗号化法に基づいたプライバシー保護技術を考察することにある（図１参照）．本研究では，以下の２点を主な目的として行われた。

（１） 画像圧縮方式として，ほぼ全ての SNS で用いられる JPEG などの国際標準規格の使用を想定して、画像暗号化法を開発する．

（２） 暗号化に対する様々な攻撃に加え，ジグソーパズル解法という別分野における手法を攻撃として捉え，安全性の検証を行う．

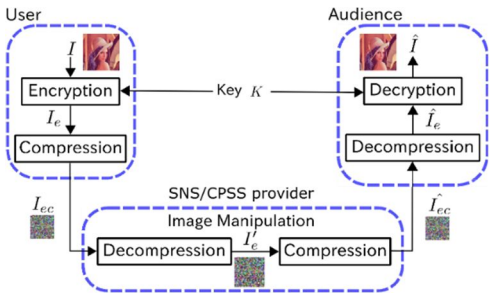

図１　Encryption-then-compression system

3.　研究方法

研究方法は，最新の研究動向調査，それに基づく理論的考察とシミュレーション実験が中心であった．　また，研究成果を国内外の学会で発表し，専門家の評価を受けた．次に多くの専門家の意見を反映させ，ジャーナル論文として成果をまとめた．具体的には、上述の２つの目的を達成するために、以下のように研究を遂行した。

（１）最先端ジグソーパズル解法の調査と安全の評価

知覚暗号化法について，各種攻撃に対する安全性の評価及び十分な画像データを用いた有効性の検証は，まだ不十分な状況にあった．さらに，暗号化とは異なる分野における手法であるジグソーパズル解法を用いた攻撃が可能であることが申請者らによって指摘されていた．ジグソーパズル解法は，世界中で盛んに研究され続けており，この攻撃は暗号化後のデータに相関を残す知覚暗号化に特有な攻撃と考えることができる．しかし，このような攻撃に対する安全性の評価に関する報告は，世界でも例がない．以上の各種攻撃について，理論的解析による安全性の評価を行うとともに，十分な数の画像データを用いたコンピュータ･シミュレーション実験によって，知覚暗号化の安全性に関する基礎的なデータを収集した．

（２）　JPEG 圧縮のための十分な耐性を有する知覚暗号化法の開発

上述のジグソーパズル解法も含めた各種攻撃に対して十分な耐性を有し、かつ JPEG 圧縮が適用可能な画像知覚暗号化法を開発した。圧縮性能の目標は、暗号化なしの画像と同等な圧縮特性を持つかつ繰り返し圧縮可能な暗号化法として設定された。

４．研究成果

具体的な研究成果は、以下の３つに要約される。

（１）　暗号化攻撃のためのジグソーパズル解法の提案とその性能評価

ジグソーパズル解法は、コンピュータビジョンの分野で盛んに研究されているテーマである。暗号化後のデータに相関を残す圧縮可能な暗号化法に対して、ジグソーパズル解法を用いた攻撃が可能であることを指摘していた．最先端のジグソーパズル解法を調査し、十分な数の画像データを用いたコンピュータ・シミュレーション実験によって，暗号化法に攻撃法として適用し、暗号化の安全性に関する基礎的なデータを収集した．さらに、暗号化特有の幾何変換処理の影響を考慮した新しいジグソーパズル解法を提案し、その方法を攻撃法として用いて耐性評価を行った。

次に、それら調査データに基づき、高い攻撃耐性を有するための暗号化法の条件について考察した。その考察から、以下に示すグレイスケール画像に基づく画像暗号化法が、高い攻撃耐性を有する新しい暗号化として提案された。

（２）　グレイスケール画像に基づく画像暗号化法の提案

本研究の目的は、JPEG 圧縮可能でありかつ高い安全性を有する画像暗号化法の開発である。この２つの要件を満たす新しい暗号化法として、グレイスケール画像に基づく画像暗号化法を提案した。提案された方法は、JPEG 圧縮時に選択される色間引き条件などの影響も考慮されて

おり、種々の条件の下で上述の２つの要件を十分満たすことが確認された。

図２は、提案法により生成された暗号化画像例である。図３は、JPEG 圧縮特性を非暗号化画像と比較した例である。画像の持つ視覚情報が保護され、圧縮特性への暗号化の影響がほぼないことが分かる。

(a) Original image　　(b) Grayscale-based encrypted image

図２　Example of encrypted image

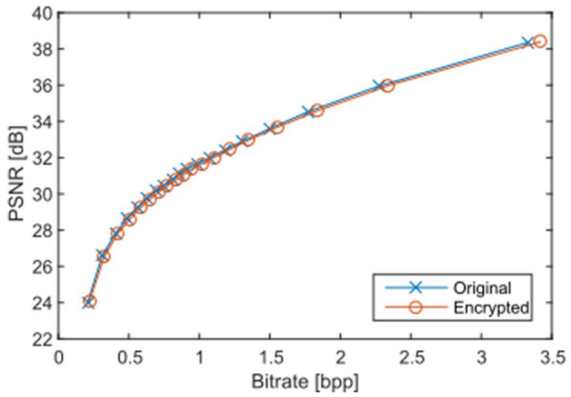

図３　Compression performance of original images and encrypted ones

（３）　暗号化画像の機械学習への応用

本研究は、圧縮可能な暗号化法の開発を目的に研究を進められた。提案法によって暗号化された画像は、幾つかの条件のもとで、機械学習に直接適用できることが発見された。この発見は、視覚情報を保護した形式で、機械学習におけるモデルの学習の実行やテスト画像が生成できる可能性を示唆している。研究としては、まだ多くの検討事項を残しているが、圧縮可能でかつ学習可能な暗号化という、新しい展開の可能性が明らかになった。

（４）　今後の展開

上述したように、圧縮可能な暗号化の研究は、学習可能な暗号化という今後の展開に繋がる多くの有益な示唆を提供した。サポートベクターマシンやランダムフォレストに代表される統計的な機械学習法はもちろん、深層学習などにおいても暗号化画像が直接モデルの学習やテストデータとして使える可能性がある。このことは、機械学習に必要となるデータの確保を容易にし、さらにその応用範囲を広げることが期待できる。今回の研究成果を再度整理して考察し、機械学習のための暗号化法に向けて準備を開始する計画である。

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　11件／うち国際共著　5件／うちオープンアクセス　8件）

１．著者名 CHUMAN Tatsuya、KIYA Hitoshi	４．巻 E101.A
２．論文標題 Security Evaluation for Block Scrambling-Based Image Encryption Including JPEG Distortion against Jigsaw Puzzle Solver Attacks	５．発行年 2018年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 2405～2408
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transfun.E101.A.2405	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Shoko IMAIZUMI and Hitoshi KIYA,	４．巻 E101-D, no.12
２．論文標題 A Block-Permutation-Based Encryption Scheme with Independent Processing of RGB Components	５．発行年 2018年
３．雑誌名 IEICE Trans. Inf. & Sys.,	６．最初と最後の頁 3150, 3157
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transinf.2018EDT0002	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Tatsuya CHUMAN, Kenta IIDA, Warit SIRICHOTEDUMRONG, and Hitoshi KIYA	４．巻 E102-D, no.1
２．論文標題 Image Manipulation Specifications on Social Networking Services for Encryption-then-Compression Systems	５．発行年 2019年
３．雑誌名 IEICE Trans. Inf. & Sys.,	６．最初と最後の頁 11, 18
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transinf.2018MUP0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Warit SIRICHOTEDUMRONG and Hitoshi KIYA	４．巻 8, no.E7
２．論文標題 Grayscale-based Block Scrambling Image Encryption using YCbCr Color Space for Encryption-then-Compression Systems	５．発行年 2019年
３．雑誌名 APSIPA Trans. Signal and Information Processing	６．最初と最後の頁 1, 15
掲載論文のDOI（デジタルオブジェクト識別子） doi.org/10.1017/ATSIP.2018.33	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Tatsuya CHUMAN, Warit SIRICHOTEDUMRONG, and Hitoshi KIYA	４．巻 14, no.6
２．論文標題 Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images	５．発行年 2019年
３．雑誌名 IEEE Trans. on Information Forensics and Security	６．最初と最後の頁 1515, 1525
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2018.2881677	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Anu Aryal, Shoko Imaizumi, Takahiko Horiuchi and Hitoshi Kiya 3	４．巻 vol.4, no.1
２．論文標題 Integrated Model of Image Protection Techniques	５．発行年 2018年
３．雑誌名 Jounal of Imaging	６．最初と最後の頁 1-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/jimaging4010001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tatsuya CHUMAN, Kenta KURIHARA, and Hitoshi KIYA	４．巻 vol.E101-D, no.1
２．論文標題 On the Security of Block Scrambling-based EtC Systems against Extended Jigsaw Puzzle Solver Attacks	５．発行年 2018年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 37-44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2017MUP0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Sirichotedumrong Warit、Kinoshita Yuma、Kiya Hitoshi	４．巻 7
２．論文標題 Pixel-Based Image Encryption Without Key Management for Privacy-Preserving Deep Neural Networks	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 177844～177855
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2959017	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 MAEKAWA Takahiro、KAWAMURA Ayana、NAKACHI Takayuki、KIYA Hitoshi	4．巻 E102.A
2．論文標題 Privacy-Preserving Support Vector Machine Computing Using Random Unitary Transformation	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1849～1855
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transfun.E102.A.1849	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 IIDA Kenta、KIYA Hitoshi	4．巻 E103.D
2．論文標題 Image Identification of Encrypted JPEG Images for Privacy-Preserving Photo Sharing Services	5．発行年 2020年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 25～32
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019MUP0006	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Sirichotedumrong Warit、Kinoshita Yuma、Kiya Hitoshi	4．巻 7
2．論文標題 Pixel-Based Image Encryption Without Key Management for Privacy-Preserving Deep Neural Networks	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 177844～177855
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2959017	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　13件）

1．発表者名 Warit SIRICHOTEDUMRONG, Tatsuya CHUMAN, and Hitoshi KIYA
2．発表標題 Compression Performance of Grayscale-based Image Encryption for Encryption-then-Compression Systems
3．学会等名 International Technical Conference on Circuits/Systems, Computers and Communications（国際学会）
4．発表年 2018年

１．発表者名
Warit SIRICHOTEDUMRONG, Tatsuya CHUMAN, Shoko IMAIZUMI, and Hitoshi KIYA

２．発表標題
Grayscale-based Block Scrambling Image Encryption for Social Networking Services

３．学会等名
IEEE International Conference on Multimedia and Expo（国際学会）

４．発表年
2018年

１．発表者名
Warit SIRICHOTEDUMRONG, Tatsuya CHUMAN, and Hitoshi KIYA

２．発表標題
Grayscale-Based Image Encryption Considering Color Sub-sampling Operation for Encryption-then-Compression Systems

３．学会等名
IEEE Global Conference on Consumer Electronics（国際学会）

４．発表年
2018年

１．発表者名
Yusuke Izawa, Shoko IMAIZUMI, and Hitoshi KIYA,

２．発表標題
A Block-Permutation-Based Image Encryption Allowing Hierarchical Decryption

３．学会等名
APSIPA Annual Summit and Conference（国際学会）

４．発表年
2018年

１．発表者名
Takahiro Maekawa, Ayana KAWAMURA, Yuma KINOSHITA, and Hitoshi KIYA

２．発表標題
Privacy-Preserving SVM Computing in the Encrypted Domain

３．学会等名
APSIPA Annual Summit and Conference（国際学会）

４．発表年
2018年

１．発表者名
Tatsuya CHUMAN, Kenta KURIHARA, and Hitoshi KIYA

２．発表標題
Security Evaluation for Block Scrambling-based ETC Systems against Extended Jigsaw Puzzle Solver Attacks

３．学会等名
IEEE International Conference on Multimedia and Expo（国際学会）

４．発表年
2017年

１．発表者名
Tatsuya CHUMAN and Hitoshi KIYA

２．発表標題
On the Security of Block Scrambling-Based ImageEncryption Including JPEG Distorsion against Jigsaw Puzzle Solver Attacks

３．学会等名
International Workshop on Signal Design and its Applications in Communications（国際学会）

４．発表年
2017年

１．発表者名
Tatsuya CHUMAN, Kenta IIDA, and Hitoshi KIYA

２．発表標題
Image Manipulation on Social Media for Encryption-then-Compression Systems

３．学会等名
APSIPA Annual Summit and Conference（国際学会）

４．発表年
2017年

１．発表者名
W Sirichotedumrong, T Maekawa, Y Kinoshita, and H Kiya

２．発表標題
Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain

３．学会等名
IEEE International Conference on Image Processing（国際学会）

４．発表年
2019年

１．発表者名
W Sirichotedumrong, Y Kinoshita, and H Kiya

２．発表標題
On the Security of Pixel-Based Image Encryption for Privacy-Preserving Deep Neural Networks

３．学会等名
IEEE 8th Global Conference on Consumer Electronics（国際学会）

４．発表年
2019年

１．発表者名
Warit Sirichotedumrong, Yuma Kinoshita, and Hitoshi Kiya

２．発表標題
Privacy-Preserving Deep Neural Networks Using Pixel-Based Image Encryption Without Common Security Keys

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference（国際学会）

４．発表年
2019年

１．発表者名
Masaki Kitavama, and Hitoshi Kiva

２．発表標題
Irreversible Privacy-Preserving Images Holding Spatial Information for HOG Feature Extraction

３．学会等名
IEEE International Symposium on Intelligent Signal Processing and Communication System（国際学会）

４．発表年
2019年

１．発表者名
Kenta Iida, and Hitoshi Kiya

２．発表標題
An Image Identification Scheme Of Encrypted Jpeg Images For Privacy-Preserving Photo Sharing Services

３．学会等名
IEEE International Conference on Image Processing（国際学会）

４．発表年
2019年

１．発表者名
Kenta Iida, and Hitoshi Kiya

２．発表標題
Image Identification of Grayscale-Based JPEG Images for Privacy-Preserving Photo Sharing Services

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Kiya and Siota Research Lab.
http://www-isys.sd.tmu.ac.jp/Papers-en

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	渡邊　修 (Watanabe Osamu) (30384697)	拓殖大学・工学部・准教授 (32638)	