様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １９ 日現在

機関番号：２２６０４
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５６０４６８

研究課題名（和文）データ圧縮された領域でのセキュリティを考慮した画像・ビデオ信号処理法

研究課題名（英文）secure image and video signal processing in the compressed domain

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）　　4,200,000円

研究成果の概要（和文）：ディジタルデバイスやソーシャルメディアの普及に伴い、画像やビデオ映像のデータ量は急速に増大し、世界中で保存されている。また画像やビデオ信号は、多くの場合、個人情報や著作権を含み、その取扱いは容易ではない。このような背景から、本研究では、画像圧縮法と親和性の高い、画像の視覚的暗号化法の開発と、暗号化された領域での信号処理法の開発を目的に行われた。得られた主な成果は、（１）暗号化領域でのJPEG2000画像の同定、（２）プライバシー保護と著作権保護を考慮した画像流通システムの開発、（３）プライバシー保護と著作権保護を考慮した画像流通システムの高性能化、の三点である。

研究成果の概要（英文）：With the development of digital devices and social media, tons of image and video signals have been generated and stored all over the world. These signals are often privacy sensitive data such as videos in surveillance systems, medical records, and face images, or commercially sensitive such as digital cinema movies. To overcome such situations, this research was done to develop visually image encryption methods and signal processing in the encrypted domain. The research outcomes are mainly as follows: (1) Image identification schemes in the encrypted domain for JPEG2000 images, (2) Development of copyright- and privacy-protected image trading systems, (3) Copyright- and privacy-protected image trading systems with enhanced performance.

研究分野：工学

キーワード：情報通信工学　情報システム

## １．研究開始当初の背景

カメラやインターネットの普及に伴い、画像やビデオ映像の利用は急速に増大し、かつその利用形態は多様化している。また画像やビデオ信号は、そのデータ量が膨大なために、一般にデータ圧縮された形式で蓄積・伝送される。さらにそれらは、多くの場合個人情報や著作権持つ内容を含むために、不適切利用回避の観点から暗号化処理が不可欠となる。しかしながら、従来の画像・ビデオ信号処理法では、圧縮されかつ暗号化され蓄積されたデータを一旦復号してそれらの検索や各種の加工処理を実行する必要があった。

## ２．研究の目的

監視カメラ映像やディジタルシネマに代表されるように、画像やビデオ信号は、そのデータ量が膨大なために、一般にデータ圧縮された形式で蓄積・伝送される。さらにそれらは、多くの場合個人情報や著作権持つ内容を含むために、不適切利用回避の観点から暗号化処理が不可欠となる。しかしながら、従来の画像・ビデオ信号処理法では、圧縮されかつ暗号化され蓄積されたデータを一旦復号してそれらの検索や各種の加工処理を実行する必要があった。以上の背景から、本研究は、以下の２点を主な目的として行われた。

（１）　画像圧縮法と親和性の高い、画像の視覚的暗号化法の開発。

広く普及している国際標準規格の圧縮方式の使用を前提して、それら圧縮法と親和性を持つ暗号化法を開発する。既存のほとんどの暗号化法は、画像圧縮方式との親和性は低く、圧縮かつ暗号化された領域での処理には適さない。

（２）暗号化された領域での信号処理法の開発。

（１）の開発に続き、画像圧縮手法と親和性が高く、かつ視覚的に暗号化された画像信号に対して、信号処理を施すことを考察する。特に、著作権保護や種々の応用を持つデータハイディング法を、暗号化された領域で適用することを中心に開発を行う。

画像圧縮の主流は、データの可逆性を保証しない、非可逆符号化である。しかし、暗号化法に代表されるように、セキュリティ技術の多くはデータの非可逆性を前提にしてはいない。本研究では、可逆性の保証を前提にしないセキュリティ技術を発展・融合させることを目標とする。

## ３．研究の方法

研究方法は、理論的考察とコンピュータによるシミュレーション実験・検証が中心である。さらにその成果を国内外の学会に発表し、専門家の評価を受ける。最後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投稿する、という手順を想定した。

（１）　初年度の研究計画は、国際標準規一つである JPEG2000 を研究対象として、暗号化されたデータからの画像検索法及び画像同定法の研究を行う。同時に、広く普及している国際標準規格の圧縮方式の使用を前提して、それら圧縮法と親和性を持つ暗号化法を検討する。

（２）　次年度以降は、暗号化領域でのデータハイディング法を考察し、画像提供者と購入者のプライバシー保護をした画像流通システムのフレームワークを検討する。さらにその際に、画像圧縮の適用を前提とし、研究を進める。

（３）　最終年度は、本研究テーマを仕上げ、論文発表を行うことによって、広く研究成果を公開する。また残された研究を総括して、新たな研究テーマの設定を行う。

## ４．研究成果

研究成果は、以下のように総括される。

（１）　暗号化領域での JPEG2000 画像の同定

国際標準規格方式の一つである JPEG2000 により圧縮された画像に対して、ボディデータとヘッダー情報共に暗号化した状態で、画像同定を行う方式を開発した。画像はデータ量が膨大であり、一般にデータ圧縮されかつセキュリティの観点から暗号化された形式で保存される。本研究では、暗号化及び圧縮された領域で直接画像同定を行うことを考察する。先行研究では、ボディデータの暗号化に限定されており、ヘッダー情報の暗号化を可能にした点に新規性がある。ヘッダー情報には画像に関する有益な情報が多く含まれており、それらを暗号化することは、セキュアな画像保存において必須である。本研究によって、それが可能となった。

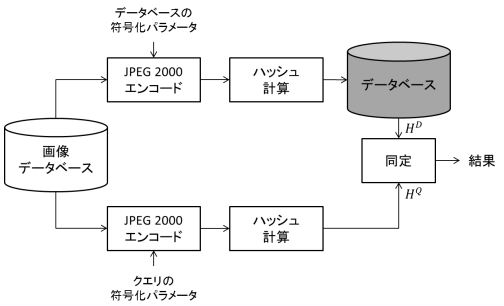



図１　JPEG2000 画像の同定システムの概要

図１は、提案された画像同定システムの概要である。ディジタルシネマなどの JPEG2000 画像は、ヘッダー情報からゼロビットプレーン数（NZBP）という特徴量を抽出した後、暗号化される。NZBP は、提案された優先順位に従い整理され、一方向性関するであるハッシュ関数に入力され、ハッシュ値に変換され、

暗号化画像と一緒にデータベースに保存される。一方、クエリ画像に対しては、その JPEG 画像から NZBP 及びハッシュ値を計算し、データベース中の値と照合する。

提案された画像同定法は、以下の特徴を有することが理論的及び実験的に確認された。

・ボディデータとヘッダー情報共に暗号化した状態で、画像同定が実行可能である。

・データベース中の画像とクエリ画像との間で、圧縮率などの符号化条件が異なる場合でも、同定性能を保持したまま、同定処理が実行可能である。

・同定処理が単にハッシュ値の比較のみで実行可能であるため、高速な処理が達成される。

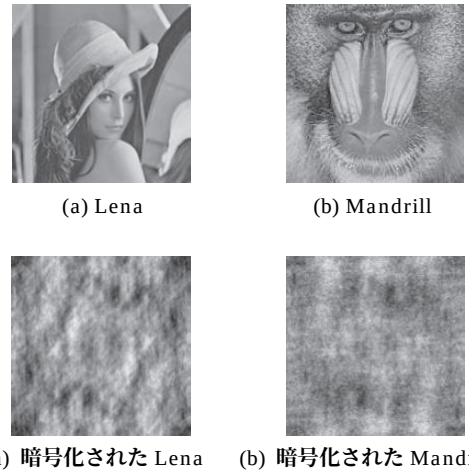
今後の課題としては、提案された手法は、JPEG2000 に限定された手法であるため、他の圧縮法への理論的拡張があげられる。

### （２） プライバシー保護と著作権保護を考慮した画像流通システムの開発

画像コンテンツなどの著作権保護法の一つに、画像中に著作権情報を埋め込む電子透かし技術がある。一般に画像流通システムにおいて、画像提供者と画像購入者の間に、第三者機関が介在し、画像中への情報の埋め込み及びそれらデータの管理を行うモデルが広く使われている。しかしこのモデルは、第三者機関が画像に加え個人情報を持ち得る、すなわち、著作権保護に加えプライバシー保護も担うため、第三者機関の信頼性を仮定せざるをえず、プライバシー保護の観点から課題が指摘されている。このような背景から、本研究では、第三者機関の信頼性を仮定せずに、著作権の保護とプライバシーの保護とを実現する方法を考察した。

第三者機関の信頼性を仮定しない画像流通システムの先行研究に、視認性を制御する視覚的暗号化が施された画像を用いるモデルがある。しかしこれらは、プライバシー保護能力を向上させるが、視覚的暗号化処理が電子透かしと画像圧縮の性能を劣化させている。したがって、電子透かしと画像圧縮の性能を維持することを可能とする、新しい視覚的暗号化法及び画像流通システムの検討が期待されている。本研究では、画像の位相成分と視認性の関係に着目して、画像の位相制御に基づく視覚的暗号化法を提案して、画像流通システムにおけるその有効性を評価する。

代表的な画像の視覚的暗号化法に、離散フーリエ変換（DFT）あるいは離散コサイン変換（DCT）に基づき定義される振幅限定画像の利用がある。しかし、この暗号化法を画像流通システムに応用した場合、振幅限定画像が持つ広いダイナミックレンジが、電子透かし及び画像圧縮の適用において悪影響を与えることが指摘されている。本研究では、ダイナミックレンジの広がりを抑えた振幅限定画像の生成法を二つ提案し、その画像流通システムへの適用法を考察した。一つは、画像の位相項のランダム化に基づいていることに、他の一つは、二次元画像に対して一次元変換法を適用する方法である。従来法も含め実験的に評価を行い、それらの有効性及び特徴を確認した。図２は、提案法の視覚的暗号化法を例示している。画像の視認性が保護されており、画像の内容を視覚的に理解することが困難となっていることがわかる。



(a) Lena　(b) Mandrill

(a) 暗号化された Lena　(b) 暗号化された Mandrill

図２　視覚的暗号化された画像例

### （３） プライバシー保護と著作権保護を考慮した画像流通システムの高性能化

（２）の研究背景及び原理に基づき、第三者機関の信頼性を仮定せずに、著作権の保護とプライバシーの保護とを実現する画像流通システムに対して、高性能化を行った。特に、使用する画像圧縮方式を限定することによって、その条件のもとで高い性能を有する画像流通システムを提案することを目指した。画像圧縮の国際標準規格の一つである JPEG 2000 の使用を想定し、JPEG 2000 の要素技術の一つである離散ウェーブレット変換に対する考察を通して、離散ウェーブレット変換係数の符号をランダムに制御する方法を提案して、視覚的暗号化と同時に、効率的な圧縮特性を維持してかつ高い電子透かし性能を有する画像流通システムを構築する基礎を考察した。透かし情報の抽出率や復元される画質の観点から提案法を評価し、画像圧縮方式を特定しない方式に比べ、さらに高い性能を有することを確認した。

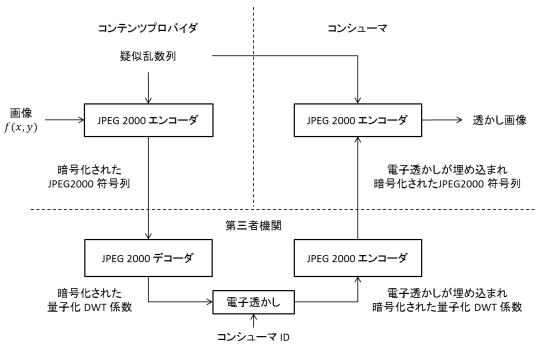



図３　第三者機関の信頼性を仮定しない画像流通システム

図３は、提案された画像流通システムである。JPEG2000 の使用を想定することに加え、ウェーブレット変換領域において直接電子透かし（データハイディング）を実行することに、その特徴がある。暗号カギは、第三者機関に配送せず、画像購入者に直接配送される。今回の研究では、JPEG2000 の使用を想定したが、他の圧縮法の場合にも容易に拡張可能であり、引き続き研究を進める予定である。

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 Wannida SAE-TANG, Shen Chuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA, A Copyright- and Privacy-Protected Image Trading System Using Fingerprinting in Discrete Wavelet Domain with JPEG 2000, IEICE Trans. Fundamentals, 査読有、vol.E97-A , no.11, pp.2107-2113, November 2014.
② Shen Chuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA, A Cheat-Prevention Visual Secret Sharing Scheme with Efficient Pixel Expansion, IEICE Trans. Fundamentals, 査読有 vol.E96-A, no.11, pp.2134-2141, November 2013.
③ Shen Chuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA, An Image Trading System Using Amplitude-Only Images for Privacy- and Copyright-Protection, IEICE Trans. Fundamentals, 査読有、vol.E96-A, no.6, pp.1245-1252, June 2013.
④ Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, A Generation Method of Amplitude-Only Images with Low Intensity Ranges, IEICE Trans. Fundamentals, 査読有、vol.E96-A, no.6, pp.1323-1330, June 2013.


〔学会発表〕（計８件）


① Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, Efficient Data Hiding in Encrypted JPEG 2000 Codestreams, Proc. IEEE International Symposium on Intelligent Signal Processing and Communication Systems, Kuching, Sarawak, Malaysia, 2nd December, 2014.
② Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, Effects of Random Sign Encryption in JPEG 2000-Based Data Hiding, Proc. IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing,no.A3-05, pp.516-519, Kitakyushu International Conference Center（Kitakyushu）, Japan, 27th August, 2014.
③ Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, Evaluation of Amplitude-Only Images for Copyright- and Privacy-Protected Image Trading Systems,Proc. International Technical Conference on Circuits/Systems, Computers and Communications,no.1069, pp.113-116, Phuket, Thailand, 4th July, 2014.
④ Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, An Image Trading System with JPEG 2000 Using Fingerprinting in Visually Protected Domain, Proc. IEEE International Symposium on Intelligent Signal Processing and Communication Systems, no.WM1-B-2, pp.32-37, Okinawa Jichi-Kaikan（Okinawa）, Japan, 13th November, 2013.
⑤ Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA, An Intensity Range Reduction Method for the Image Trading System with Digital Fingerprinting in Visually Protected Domain, Proc. IEEE International Symposium on Communications and Information Technologies,no.B2-2.2, pp.423-428, Samui Island, Thailand, 6th September, 2013.
⑥ Wannida SAE-TANG, Masaaki FUJIYOSHI, Hiroyuki KOBAYASHI, and Hitoshi KIYA, Intensity Range Reduction for Amplitude-Only Images," Proc. International Workshop on Advanced Image Technology,no.5A-1, pp.322-327, Nagoya University (Nagoya), Japan, 8th January, 2013.
⑦ Toshiyuki DOBASHI, Osamu WATANABE, Takahiro FUKUHARA, and Hitoshi KIYA, Hash-Based Identification of JPEG 2000 Images in Encrypted Domain, Proc. IEEE International Symposium on Intelligent Signal Processing and Communication Systems, no.D2.4, pp.469-472, New Taipei City, Taiwan, R.O.C., 6th November, 2012.
⑧ Shen Chuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA, A Commutative Scheme of Perceptual Cryptography and Image Compression for JPEG 2000, Proc. International Technical Conference on Circuits/Systems, Computers and Communications,no.E-W1-04, Sapporo Convention Center（Sapporo）, Japan, 18th July, 2012.

６．研究組織

(1)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