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　３ 年　 ５ 月 ３０ 日現在

機関番号：１２５０１
研究種目：研究活動スタート支援
研究期間：2019～2020
課題番号：１９Ｋ２３０７０

研究課題名（和文）文化財画像の利活用促進に資する画像保護システムの開発

研究課題名（英文）Image protection system for accelerating use of archive images of cultural properties

研究代表者
今泉　祥子（Imaizumi, Shoko）

千葉大学・大学院工学研究院・准教授

研究者番号：８０５３５０１３

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：本研究では，ディジタル化された画像としての文化財の円滑な利活用を目的として画像保護システムを開発した．本システムでは，原画像に対して著作権などの情報を埋め込み，その後，暗号化処理を施すことで出力画像を生成する．埋め込まれた情報は，暗号を解除することなく抽出することができる．一方，暗号化処理を施した後，サーバにおける管理情報などの付加情報を埋め込み，出力画像を生成することも可能である．このとき，埋込み情報は，暗号解除後でも抽出することができる．

研究成果の学術的意義や社会的意義
本研究では，デジタルアーカイブ化が急速に進められている文化財について，ディジタル画像としての文化財の利活用促進を目的とし，著作権やプライバシの情報漏洩，および，不正な二次利用を抑制するための画像保護システムについて検討した．一般に，画像に対する暗号化および情報埋込み技術の適用は，画像の品質低下，データ量の増加，画像検索の困難性などを伴い，円滑な利活用の妨げとなる．これらの課題を解決し，文化財画像の利活用促進に貢献することは，学術的にも社会的にも意義がある．

研究成果の概要（英文）：In this research, we developed an image protection system for archive images of cultural properties. This system first embeds copyright information into an original image and then encrypts the marked image. The hidden information can be extracted in the encrypted domain, i.e., without decryption. Our system has another option, which first encrypts an original image and then embeds additional information into the encrypted image. In this case, it is possible to extract the hidden information in the plain domain, i.e., after decryption.

研究分野：メディアセキュリティ

キーワード：画像暗号化　情報埋込み　著作権保護　プライバシ保護　デジタルアーカイブ

１．研究開始当初の背景

現在，国内外において，文化財のデジタルアーカイブ化は急速に進められており，国内におけるディジタル画像としての文化財画像の利活用の促進は，欧米・アジア諸国の状況と比較しても，早急に対応すべき重要な課題となっている．日本の文化財は，個人が所有する財産である場合が多く，画像の利活用においては，著作権やプライバシの情報漏洩，不正な二次利用などの問題が常にハードルとなっている．一方で，画像に対してセキュリティ対策を施すことで，画像の品質が低下する，画像の情報量が増加する，所望の画像を検索することが困難となることは円滑な利活用の妨げとなる．そこで，画像の性質を変えることなく，いかに安全に画像を保護できるか，すなわち，安全かつ円滑な文化財画像の利活用促進が問われている．

２．研究の目的

このような状況に鑑み，本研究は，特に大容量の文化財画像を考慮して，画像保護システムを構築し，画像利活用の促進に資することを目的とする．本研究では，画像保護技術である，暗号化および情報埋込みの二つの技術を有する画像保護システムについて研究する．具体的には，画像に対して著作権などの情報を見えないように埋め込むと同時に，暗号化処理を施すことで画像の内容を秘匿するシステムを構築する．このとき，①情報が埋め込まれた画像に，人間の目で認識できるほどの劣化が生じないこと，②情報を埋め込んだ後に暗号化処理を施した場合でも，暗号を解除することなく埋め込まれた情報が抽出できること，③暗号化処理がその後の画像圧縮の圧縮効率に著しい影響を与えないこと，④暗号を解除することなく，画像データベースから所望の画像を検索可能であること，を同時に実現するシステムの開発を行う．

これらの条件について，これまで，個々には活発に研究が行われている一方，これらを同時に実現する研究成果は発表されていない．これは，暗号化された画像から先に埋め込まれた情報を抽出する技術，および，内容が秘匿されている暗号化画像について画像検索を有効とする技術の実現は困難なためである．本研究は，この課題を解決し，複数の条件を一つのシステムの中に並立させるようとするものである．

３．研究の方法

本研究では，上述した四つの条件を同時に実現する画像保護システムを研究した．

まず，①および③に挙げた情報埋込みと暗号化処理に対する各条件に関しては，申請者がこれまで行ってきた成果である情報埋込み法と，Encryption-then-Compression(EtC)システムのブロックベース暗号化法をそれぞれ応用した．いずれの手法も，画像の性質に大きな影響を与えずに処理できる特長をもつ．そのため，以下で述べる，②と④の条件を満たすためのアルゴリズムに基づき，これらを併合することで，埋込み画像の画質，および，暗号化画像の圧縮効率をいずれも保持することが可能となった．

次に，②の暗号解除不要な埋込み情報の抽出については，情報埋込み法のうち，画像のヒストグラムに基づく埋込み手法を導入した．これは，図１に示すように，まず，画像のヒストグラムから出現頻度の最も高い二つの画素値 I_R と I_S を検出し，その右あるいは左に位置するすべての画素値を１ずつ移動することで I_R と I_S に隣接する画素値を空にする．次に，画素値 I_R と I_S をもつ画素を対象に１ビットごとの情報埋込みを施す．例えば，画素値 I_R をもつ画素 p について，埋込み情報が１の場合，p の画素値は I_R+1 に変更される．一方，埋込み情報が０の場合，p の画素値は I_R のままとなる．これにより，画素値をわずかに変化させるだけで，情報を埋め込むことができ，また，暗号化前後でヒストグラム形状が不変であるという条件のもとで，暗号を解除することなくあらかじめ埋め込まれた情報の抽出が可能となる．

さらに，④の暗号化画像の検索については，②を応用することで実現した．画像検索のため，一旦暗号を解除することは，安全性を損なうことに繋がる．そこで，あらかじめ各画像に関連する情報を画像内に埋め込み，暗号化処理を行う．画像検索に際しては，暗号化画像から埋め込まれた関連情報を抽出することで，暗号を解除することなく，暗号化領域での画像検索を有効とすることができる．

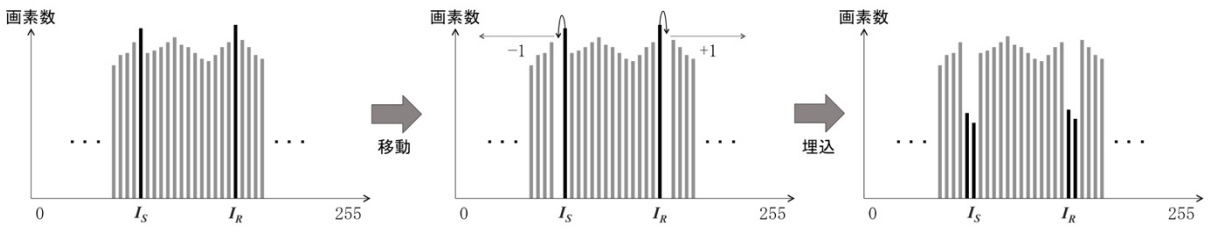

図１　ヒストグラム移動に基づく情報埋込み

４．研究成果

具体的な成果を以下に述べる．

(1) 処理領域選択可能な暗号化画像に対する可逆情報埋込み法の実現

原画像に対してあらかじめ埋め込んだ情報を，暗号化処理後の出力画像から抽出することが可能な可逆情報埋込み法を提案した．提案法の概略を図 2 に示す．同図において，*PP*/*ZP* は，画像ヒストグラムにおいてそれぞれ最大または最小頻度となる画素値を示す．まず，原画像をブロックに分割した後，各ブロック内の画素値やその配列に応じて埋込みブロックの順番を決定し，ヒストグラム移動を用いた可逆情報埋込み処理を行う．その後，情報埋込み時に分割したブロックを単位として，EtC システムによる暗号化を施す．これにより，出力画像から，暗号を解除することなく，原画像に埋め込んだ情報を抽出することができる．このことは，暗号化処理が施された出力画像からあらかじめ埋め込まれたその画像自身の情報を抽出することで，暗号を解除することなく画像検索を可能とする．一方で，提案法は，暗号化後に情報を埋め込み，暗号を解除した後でその情報を抽出することも可能であり，埋込み領域を選択できる手法である．

さらに，上記の手法を図 3 に示すように拡張し，暗号化前後，すなわちプレーン領域と暗号化領域の両領域に対して埋込み可能な手法について検討した．これにより，ユーザ権限が拡張され，領域 A または B の情報抽出のみ，領域 A または B の情報抽出と暗号解除など柔軟に権限を与えることができるとともに，さまざまなモデルに応用が期待できる．

シミュレーションにより，提案法で生成された出力画像について，秘匿性能と圧縮特性の観点から評価を行い，提案法の有効性を確認した．

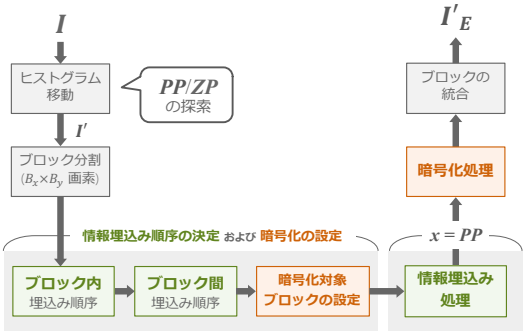

図 2　基本手法の処理フロー

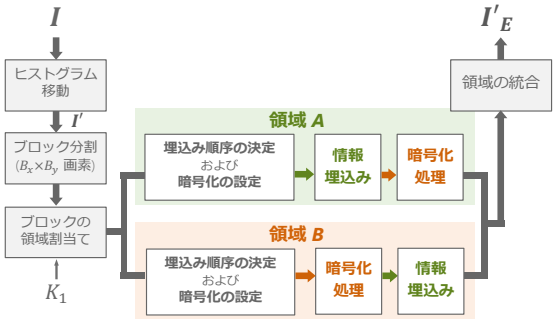

図 3　拡張手法の処理フロー

(2) LSB 置換による制約の緩和

(1)の手法に対して，さらに柔軟な情報埋込み/抽出を実現するため，EtC システムで生成される暗号化画像に対して，処理順序や位置など複雑な制約を伴わない情報埋込みの導入を提案した．この手法では，まず，原画像を，上位 7 ビットと最下位ビット(LSB)のビットプレーンに分解した後，前者に対して，EtC システムによる暗号化を施す．一方，暗号化対象とならない後者，すなわち，LSB は，情報埋込み領域となり，埋込み情報に置換される．このように，暗号化領域と情報埋込み領域があらかじめ独立して指定されることで，複雑な条件を必要とせず，柔軟な情報埋込み・抽出が可能となる．ただし，この手法は，(1)と異なり可逆性を考慮しておらず，非可逆な処理となる．したがって，情報抽出が行われた後も原画像の復元は困難となる．

生成された出力画像は図 4 のようになる．出力画像について，圧縮特性，画質，および，秘匿性能を評価し，提案法の有効性を確認した．

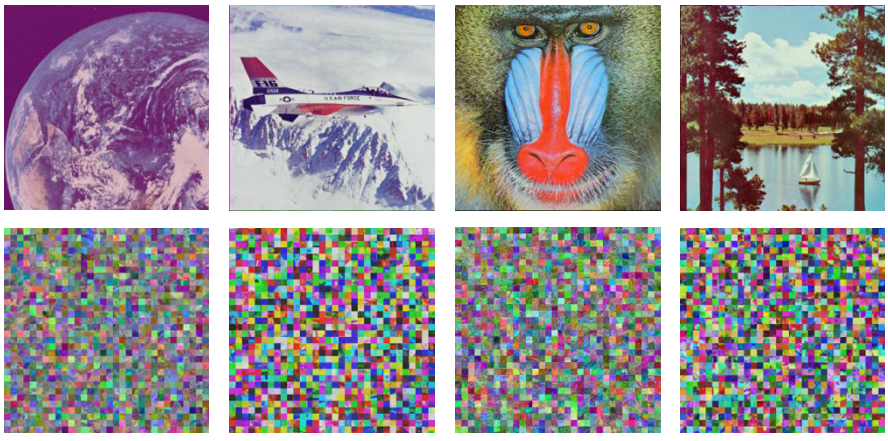

図 4　実験結果（上段:原画像，下段:出力画像）

(3) MSB 予測を用いたキャパシティの向上

暗号化画像を対象とした可逆情報埋込み法では，これまで最大でもキャパシティが 0.5 bpp 程度と非常に小さい．そこで，本研究では，最上位ビット(MSB)を用いた予測を行うことにより，大容量かつ可逆性を実現可能な，暗号化画像に対する可逆情報埋込み法を提案した．本手法の処理手順は図 5 のとおりであり，MSB 予測における条件を正確に与えるとともに，埋込み処理の前処理として，埋込み情報と暗号化画像に対してマーカとフラグをそれぞれ設定する．これらの処理により，提案法は，高い埋込み容量を実現するとともに，十分な可逆性を保証することができる．図 6 に出力画像の例を示す．シミュレーションでは，可逆性と埋込み容量について評価を行い，提案法が可逆性を保証できること，1 bpp に近いキャパシティを実現することを確認した．

上述の手法では，暗号化に XOR 演算または任意のストリーム暗号を用いる．したがって，出力画像の圧縮性能は考慮されていない．一方，(1)の手法では，キャパシティが最大で 0.1 bpp 程度であるため，今後は，本手法に EtC システムによる暗号化を導入することで，(1)をさらに拡張するアルゴリズムを検討する．

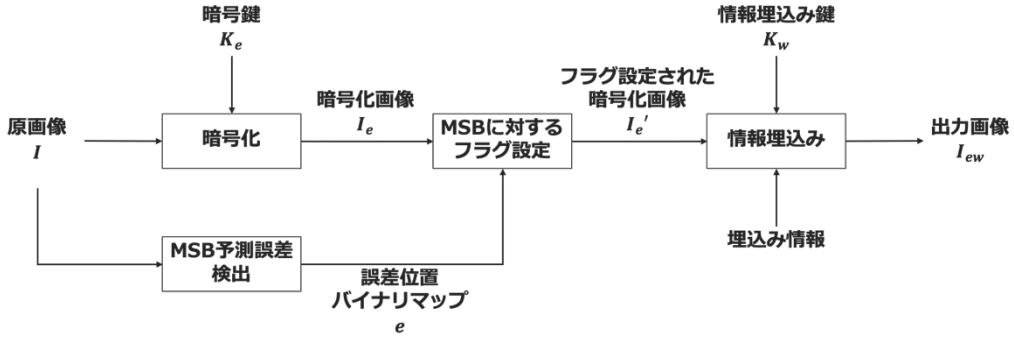

図 5　MSB 予測型可逆情報埋込み法の処理フロー

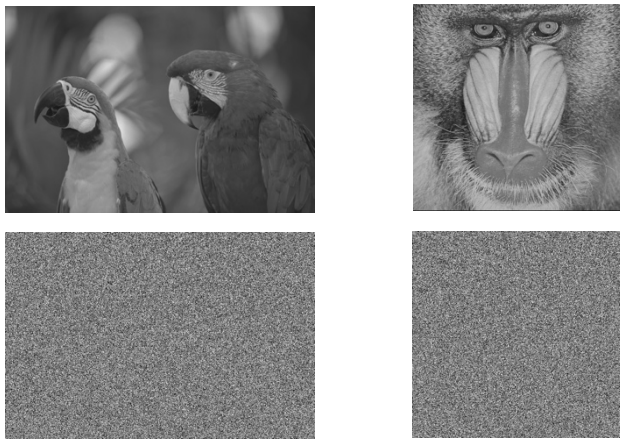

図 6　実験結果（上段:原画像，下段:出力画像）

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Shoko Imaizumi, Yusuke Izawa, Ryoichi Hirasawa, Hitoshi Kiya	４．巻 E103-A
２．論文標題 A Reversible Data Hiding Method in Compressible Encrypted Images	５．発行年 2020年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 1579-1588
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020SMP0029	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 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Ryoichi Hirasawa, Shoko Imaizumi, Hitoshi Kiya
２．発表標題 An MSB Prediction-Based Method with Marker Bits for Reversible Data Hiding in Encrypted Images
３．学会等名 IEEE Global Conference on Life Sciences and Technologies（国際学会）
４．発表年 2021年

１．発表者名 山村昂太朗，平澤凌一，今泉祥子，貴家仁志
２．発表標題 線形回帰を用いた暗号化画像に対するMSB予測型可逆情報埋込み法
３．学会等名 電子情報通信学会 EMM研究会
４．発表年 2021年

１．発表者名 平澤 凌一．今泉 祥子，貴家 仁志
２．発表標題 暗号化画像に対するMSB予測型可逆情報埋込み法の拡張
３．学会等名 電子情報通信学会 EMM研究会
４．発表年 2021年

１．発表者名
Ryoichi Hirasawa, Shoko Imaizumi, Hitoshi Kiya

２．発表標題
Flexible Data Hiding and Extraction in EtC Images

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

４．発表年
2020年

１．発表者名
平澤 凌一．今泉 祥子，貴家 仁志

２．発表標題
柔軟な情報埋込みと抽出を可能とする拡張されたEtC画像

３．学会等名
電子情報通信学会 EMM研究会

４．発表年
2020年

１．発表者名
井澤 佑介，平澤 凌一，今泉 祥子，貴家 仁志

２．発表標題
埋込み領域選択可能な暗号化画像のための可逆情報埋込み法

３．学会等名
電子情報通信学会 SIS研究会

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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
研究協力者	貴家　仁志 (Kiya Hitoshi) (40157110)	東京都立大学・システムデザイン学部・教授 (22604)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関