D108

走査方式を考慮した双直交ウェーブレット多重解像度解析に基づく鍵画像の視認困難性、秘匿性を向上したデータハイディング

新井 康平[○](佐賀大学), 瀬戸 要((株)サインズ)

A data hiding method based on bi-orthogonal wavelet Multi-Resolution Analysis: MRA taking into account scanning scrambling for improvement of invisibility and confidentiality of hidden images

Kohei ARAI and Kaname SETO

ABSTRACT

A data hiding method based on bi-orthogonal wavelet Multi-Resolution Analysis: MRA is proposed for improvement of invisibility of hidden images by taking scanning scrambling with Hilbert scan scheme into account is proposed. The experimental results show the effect of Hilbert scanning for the key image on the hidden images in terms of invisibility and confidentiality.

Keywords: Watermarking, data hiding, Multi-Resolution Analysis, Hilbert scan, wavelet analysis.

1. 緒 論

データハイディングは透かし技術やステガノグラフィ技術の総称であり1) 外に表れた画像情報は原画像と呼ばれ2) 外には表れない画像情報は鍵画像と呼ばれる。データハイディング手法3)、4)、5)は、

- ・原画像の実空間上において鍵画像を埋め込む手法6)
- ・原画像の周波数空間上において鍵画像を埋め込む手法7)

に大別できる。埋め込み後の画像に対して圧縮等の処理を施されても原画像の比較的影響を受けにくい特定の周波数に鍵画像を埋め込むことが可能であるという観点から、前者に比べ後者は鍵画像の情報を隠蔽する能力が相対的にある。前者は原画像のエッジ部分等を操作して鍵画像を埋め込む工夫が必要となる。後者は鍵画像を埋め込むべき原画像の周波数帯の決定が必要となる。また、カラーの原画像を用いたデータハイディング手法7)、8)も提案されている。原画像の情報量の観点から、カラー原画像を用いたデータハイディングはカラー以外の原画像を用いたデータハイディングに比べ、鍵画像の情報を隠蔽する能力がある。

カラー原画像を用いたデータハイディングは、原画像のある成分に対して鍵画像を埋め込む手法が用いられる。例えば、原画像のRGBの成分のうち、G成分に鍵画像を埋め込む手法8)や原画像の主成分変換後の第1固有画像成分に鍵画像を埋め込む手法9)が採用される。しかしな

がら、以上の報告は、鍵画像を原画像に挿入する際の走査方式の影響に関して考慮されていない。すなわち、データハイディングにおいて埋め込み画像における鍵画像の視認性が問題(通常のラスタ走査によって鍵画像を走査して原画像に埋め込む場合、埋め込み画像における鍵画像の視認が容易)である。本論文では、鍵画像情報の保護の観点から鍵画像を挿入する際の走査方式を通常のラスタ走査から他の走査方式に変更することにより、埋め込み画像における鍵画像の視認困難性を向上している。複数の性質の異なる画像を用いて提案方法の有効性を確認したのでここに報告する。

2. 提案方法

2.1 多重解像度解析(Multi-Resolution Analysis: MRA)に基づくデータハイディング

二次元信号に対してウェーブレット分解を行うと4成分、低周波成分LL1成分と3つの高周波成分LH1、成分HL1、成分およびHH1成分が生成される。また、LL1成分に対してウェーブレット分解を行うと4成分、LL2成分・LH2成分・HL2成分・HH2成分がさらに生成される。与えられた2次元信号はレベル0と呼ばれ、ウェーブレット分解を行うにしたがいレベル数が1ずつ増加する。これをMRAと呼ぶ。Fig.1はMRAの概念を示す。Fig.2はウェーブレット分解を3回まで施した例である。

MRAに用いるウェーブレット基底関数に双直交ウェーブレットを採用し、かつ、ウェーブレット分解後の4成

分が存在すれば、誤差零で与えられた二次元信号は復元される。直交ウェーブレットは、双直交ウェーブレットの1種である。すなわち、双直交ウェーブレット変換は逆変換可能である。

次に、MRAに基づくデータハイディングの手法の概要を示す。データハイディングは、

- 1) 原画像に対してウェーブレット分解を行う(Fig.2)。
- 2) ウェーブレット分解後の高周波成分に鍵画像を挿入する(Fig.3(a))。
- 3) ウェーブレット再構成によりデータハイディング画像を生成する(Fig.3(b))。

の手順で行われる。なお、Fig.3においては鍵画像をLH1成分に挿入した例示である。鍵画像はHL1成分やHH1成分やHH2成分等に挿入することも可能である。

Fig.1 A conceptual illustration of Multi-Resolution Analysis: MRA (Laplasian Pyramid)

(a) First stage

(b) Second stage

Fig.2 Examples of Laplasian pyramid

(a) Key image is hidden in LH1 component

(b) Key image is visible in Embedded image

Fig.3 An example of visibility of the key image that is hidden in the embedded image

2.2 鍵画像の走査方法

本論文では走査方式としてラスタ走査方式とヒルベルト走査方式およびランダム走査方式を取り上げる。ランダム走査方式の場合、送受当事者間においてランダム走査に係る乱数発生規則情報を共有しているものとする。また、順列変換行列(画素順序入れ替え)による走査方式はランダム走査方式に含まれる。

各走査方式ともに次元空間データを辞書式配列(次元データに変換、保存するものである。鍵画像を挿入する際の走査方式の情報を第3者が入手することは困難である。そのため、当該鍵画像の秘匿性が増すことになる。すなわち、鍵画像を挿入する際の走査方式を変更することにより、鍵画像情報の保護能力の向上を図ることができる。と考える。

3. 実験

3.1 使用データ

原画像に使用するデータをFig.4に示す。これは米国NASA(航空宇宙局)から打ち上げられたLandsat4号搭載のTM(Thematic Mapper)が捉えた佐賀地域画像である。TMは7バンドから構成されているが、ここではバンド3(650nm)波長域データを用いた。また、鍵画像をFig.5に示す。原画像の画素サイズは128x128画素であり、階調数は256(8ビット)である。一方、鍵画像の画素サイズは64x64画素であり、階調数は原画像と同じく256である。

Fig.4 Original image of Landsat-4/TM image(Band 3)

Fig.5 Key image which is to be hidden in the original image

3.2 実験方法

鍵画像の平均は零であるとする。鍵画像を原画像のHH1成分のみに代入することによりハイディングを行う。本実験の目的は、走査方式を変更することの有効性を実証することである。したがって、HH1成分画像サイズと鍵画像サイズを一致させ、HH1成分のみに代入することによりハイディングを行う。ハイディングする成分を1成分に限定することにより、走査方式によるハイディング手法の比較が可能になると考える。HH1成分画像サイズと鍵画像サイズを一致させることにより、鍵画像の情報量が多い場合の実験を設定する。シグニチャ等が鍵画像の場合は、一般には、鍵画像の情報量は少ない。鍵画像の情報量の少ない例として、鍵画像が二値画像の場合、画像の最下位ビットに鍵画像を挿入する工夫も可能である。複数の鍵画像が存在する場合も本実験の内容に含まれる。すなわち、Fig.5は複数の鍵画像を結合したビット列のデータであるとみなせばよい。双直交ウェーブレット変換が逆変換可能であることにより、鍵画像を復元可能である。

3.3 実験結果

Fig.6に原画像(すべての画素値を0とした)をMRAに基づき4つの成分画像に分解し、HH1成分画像に鍵画像にて置き換えた後に原画像を再構成によって復元した画像、すなわち、埋め込み画像を示す。Fig.6(a),(b),(c)は、それぞれ、ラスタ、ヒルベルト、ランダム走査によって鍵画像をあらかじめ走査し、それぞれの走査画像を鍵画像として改めて定義しなおしてHH1成分画像と置き換えた。したがって、これら埋め込み画像には鍵画像が現れてはならないものであるが、図を見ると明らかなように、ラスタ走査の場合等は特に、鍵画像が視認できる。

(a)Raster scan (b)Hilbert scan (c)Random scan

Fig.6 Reconstructed images in which the key image is hidden in the HH1 component image based on MRA (the key image is scanned with raster, Hilbert and random scanning schemes as a preprocessing) in case that all the pixels are zero in the original image.

Fig.7には、原画像に前出のLandsat/TM画像を用いた場合の再構成画像を示す。Fig.7(a),(b),(c)に、それぞれ、ラスタ、ヒルベルト、ランダム走査による鍵画像の走査の場合の再構成画像を示す。

これら再構成画像、または、鍵画像が埋め込まれた埋め込み画像は流通画像である。秘匿性高く守らなければ

ならない画像は真に鍵画像である。MRAに基づくデータハイディングにおいて、この鍵画像を流通画像から現出させる安直な方法は流通画像にウェーブレット変換を施してみることである。Fig.8はFig.7の埋め込み画像にウェーブレット変換を施して得られた画像を示す。ここでFig.8(a),(b),(c)は、それぞれ、ラスタ、ヒルベルト、ランダム走査により鍵画像を走査した後に原画像のMRA後のHH1に置き換え、再構成した画像にウェーブレット変換を施した画像である。これらを見て明らかなようにラスタ走査の場合は鍵画像そのものが現出してしまい、秘匿性はまったくない。その点、ヒルベルト走査は横縞状のストライプノイズしか現出しておらず、また、ランダム走査の場合もランダムノイズのみが現出するだけであるので鍵画像の視認は困難であることが分かる。さらに、ランダム走査、ヒルベルト走査における走査順序生成法に係るパラメータを送受の当事者間のみで了解することにより、当事者のみが当該鍵画像を知り得ることになり、秘匿性、機密性を向上させることができる。

(a)Raster scan

(b)Hilbert scan

(c) Random scan

Fig.7 Reconstructed images in which the key image is hidden in the HH1 component image based on MRA (the key image is scanned with raster, Hilbert and random scanning schemes as a preprocessing) in case that original image is Landsat/TM.

4. 結言

画措置がすべて0であるシミュレーション原画像および地球観測衛星データによる実験において、走査方式をラスタ走査からヒルベルト、または、ランダム走査に変更することにより鍵画像をMRAによって原画像に埋め込む際の鍵画像の秘匿性および視認困難性の向上を確認した。すなわち、鍵画像の情報の保護の観点から提案手法

の有効性を確認した。

(a) Raster scan

(b) Hilbert scan

(c) Random scan

Fig.8 Resultant images after the Wavelet transformation of Fig.7 of reconstructed images in which key image is hidden in HH1 component that is derived from MRA of the original image of Landsat/TM image.

本論文ではDaubechies基底関数を採用したが、双直交ウェーブレットであれば鍵画像情報を完全に復元できる。なお、双直交ウェーブレットの種類を隠蔽することによっても鍵画像情報を保護することができる。この場合、画像の横方向の双直交ウェーブレットと縦方向の双直交ウェーブレットとが同じものである必要はない。また、本論文では鍵画像をHH1成分のみに挿入することにより実験を行ったが、鍵画像のビット列を分割してHH1成分以外の高周波成分にも鍵画像情報を挿入することも可能である。

参考文献

- 1) 松井甲子雄、電子透かしの基礎、森北出版、2000
- 2) 川合淳郎、透かしー本物の証・紙のすき入れ（透かし）、画像電子学会誌、31,2,253-260,2002.
- 3) 河口英二・野田秀樹・新見道治、ディジタル・ステガノグラフィ技術について、画像電子学会誌、31,3,414,420,2002.
- 4) 岡本晃宏・宮崎明雄、モルフォロジカル信号処理を利用した電子透かし方式、電子情報通信学会論文誌A、J84-A,8,1037-1044,2001.
- 5) L.J.Cox, J.Killian, T.Leighton and T.Shanon, Secure spread spectrum watermarking for multimedias, IEEE Trans.,Image Process., 6,12, 1673-1687, 1997.
- 6) 井上尚・宮崎明雄・島津幹夫・桂卓史、ウェーブレット変換を用いた画像信号に関する電子透かし方式、映像情報メディア学会誌、52,12,1832-1839,1998.
- 7) R.Oullette, H.Noda, M.Niimi and E.Kawaguchi, Topological ordered color table for BPCS steganography using indexed color images, IPSJ Journal, 42,1,110-113,2001.
- 8) 瀬戸英俊・森多雄司・姜錫・青木由直、画像圧縮におけるフレネル変換を用いたカラー画像電子透かし法、信学技報、43-48,2000.
- 9) 新井康平・瀬戸要、固有値展開による情報の偏りを利用した多重解像度解析に基づくデータハイディング、可視化情報学会、23, 8, 72-79,2003.
- 10) 新井康平・瀬戸要、ウェーブレット多重解像度解析に基づくデータハイディング、第 回可視化情報シンポジウム講演論文集, Vol.22, Suppl.No.1, 229-232, 2002. 2002.
- 11) 新井康平・瀬戸要、座標変換に基づく情報ハイディング手法、可視化 情報学会誌、25、Suppl.No.1, 55-58,(2005)