様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　3 月 31 日現在

機関番号：１７１０４
研究種目：基盤研究（C）
研究期間：２０１０　～　２０１２
課題番号：２２５６０３８２
研究課題名（和文）　可逆的情報ハイディングを利用した安全、便利な QR コードシステムの研究開発
研究課題名（英文）　Secure and useful QR-code system based on reversible information hiding
研究代表者
新見　道治（NIIMI MICHIHARU）
九州工業大学・情報工学研究院・准教授
研究者番号：２０２６９０８８

研究成果の概要（和文）：
圧縮ベースの二値画像に対する可逆的情報ハイディング技術を開発し、ハイディングの評価手法について考察した。QR コードに対する情報重畳方式として、提案した二値画像に対する可逆的情報ハイディングを利用する方式、終端コード以降に配置する方式、Wet Paper 符号を利用する方式の 3 つを検討した。さらにと RSA 公開鍵暗号併用した成績情報開示システムを試作した。

研究成果の概要（英文）：
A technique for reversible information hiding that is based on compression for binary images was proposed and a method for steganalysis to evaluate information hiding techniques were studied. Three information-hiding techniques for QR codes were investigated. One of them is based on the proposed reversible information hiding, and other two methods are based that message we want to embed is put after the terminate code of QR code, and Wet paper code is used to represent the message. In addition, the secure release system of examination score which is based on RSA public key crypto system and information hiding for QR code was studied.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,300,000	390,000	1,690,000
2011 年度	1,200,000	360,000	1,560,000
2012 年度	900,000	270,000	1,170,000
年度	0	0	0
年度	0	0	0
総　計	3,400,000	1,020,000	4,420,000

研究分野：工学
科研費の分科・細目：電気電子・通信・ネットワーク工学
キーワード：暗号・セキュリティ・情報ハイディング

１．研究開始当初の背景

画像に対する情報ハイディングとは、何らかの情報をディジタル画像中に隠す技術であり、電子透かしやステガノグラフィ（秘匿通信）を実現する一つの手段として考えられてきた。カバー画像とはメッセージを埋め込むために使用する画像で、メッセージが埋め込まれた画像はステゴ画像と呼ばれている。従来の情報ハイディングでは、ステゴ画像は、埋め込みにより少なからず画質が劣化する。このような従来の情報ハイディングに対して、埋め込んだ情報を抽出した後にオリジナ

ルのカバー画像を完全に復元できる技術として可逆的情報ハイディング（reversible information hiding or lossless information hiding）が提案された。ステゴ画像から埋め込んだメッセージを抽出した後に「復元されたカバー画像」は、オリジナルの「カバー画像」と１ビットの違いもなく完全に一致する。

可逆的情報ハイディングは、画像の改ざん検出に応用可能である。具体的には、カバー画像のハッシュ値を埋め込んでおき、ステゴ画像から抽出されたハッシュ値と復元されたカバー画像から計算されたハッシュ値を比較すれば、簡単に改ざん検出ができる。

ＱＲコードは、英数なら最大約４０００文字も表現でき、高速読み取り可能な二次元コードである。URL を記録したＱＲコードはもっとも広く普及している利用方法であるが、名刺、航空券、野球のチケット、ＪＲＡの投票券等、その利用分野は拡大しつつある。その一方で、ＱＲコードを悪用したフィッシング攻撃が確認され始めている。この手口は、カメラで撮影するだけでアクセスできるというＱＲコードの特徴を悪用したもので、偽サイトや悪意あるサイトに飛ぶように設定されたＱＲコードを既存のＱＲコードに重ねて貼り、個人情報を搾取しようとするものである。

２．研究の目的

以下の 4 つの項目を目標として、研究を行った。

(1)二値画像に対する可逆的情報ハイディング技術の開発

(2) ハイディングの評価手法の開発

(3) ＱＲコードの改ざん検出機能の実現（安全な QR コードシステムの開発）

(4) 付加情報をＱＲコードに持たせた応用システムの開発（便利な QR コードシステムの開発）

３．研究の方法

QR コードの構造について述べておく。QR コードでは指定された情報から 0 と 1 の 1 次元情報が作成され、この 0、1 をそれぞれ二次元平面上の白および黒の正方形としている。この正方形はモジュールと呼ばれ、1 ビットが 1 モジュールに相当し、QR コードはモジュールの集まりで構成されている。QR コードには大きさを表す 1 から 40 までの番号があり、その番号は型番と呼ばれる。型番 1 は 21 x 21 モジュールで、型番が 1 上がると幅、高さが 4 モジュール分増え、型番 40 では 177 x 177 モジュールになる。QR コードはデータの復号を補助する QR コード位置の検索や特性の識別に必要な機能パターンとデータコード語及び誤り訂正コード語に使われる符号化領域から構成されている。

QR コード上のデータ及び誤り訂正コード語について概説する。データ及び誤り訂正コード語は QR コードに埋め込むデータとそれに対する誤り訂正コード語を持つ領域である。この領域に 2 値化した入力データのビット列を埋め込む。埋め込むデータのビット列は入力データを 2 値化する方法を示すモード指示子、文字列の長さを示す文字数指示子、2 値化されたデータと終端パターン、埋め草ビット、埋め草コードから構成された埋め草キャラクタを付加したものである。終端パターンはデータの終了を表す「0000」の 4 ビットである。データの容量が 4 ビット未満の場合は「0」のビット列を短縮する。終端パターンを付加させても容量を満たせない場合は情報量が 8 の倍数になるように「埋め草ビット」として「0」を後ろに 7 ビット未満付加する。容量がまだ余っている場合は「埋め草コード語」として「1110 1100」と「0001 0001」を交互に付加し、容量を満たす。

QR コードの復号化は符号化の過程の逆の処理を行う。QR コードの大きさ又は型番情報から型番を取得する。形式情報から誤り訂正レベルとマスクパターン情報を取得する。マスクパターン情報からマスクを解除し、データ及び誤り訂正コード語を抽出する。リード・ソロモン符号の誤り訂正を行い、データコード語を抽出する。データコード語を連結し、データのビット列に戻す。データのビット列の終端パターンが現れるまでモード指示子、文字数指示子により 2 値化されたデータを文字列に戻す。以上によりデータの読み取りが終了する。

４．研究成果

(1) 二値画像に対する可逆的情報ハイディング

埋め込むメッセージだけではなく、カバー画像を復元するための情報を圧縮したデータも埋め込む必要がある。以下の手順により、画質の劣化を抑えながらも、より大容量の秘密情報を埋め込むことができる。

①埋め込み用ブロック候補の選択

まず、カバー画像をｍｘｍ画素のブロックに分割する。次に、各ブロックの複雑さを計算し、閾値以上の複雑さを持つブロックを埋め込み用ブロック候補とする。この閾値処理で抽出された埋め込み用ブロック候補はノイズ状のブロックであり、画素の変化が発生しても視覚的に影響が出にくい領域であり、埋め込みに適している。

②埋め込み用画素候補の選択

埋め込み用ブロック候補において、ブロッ

ク中の半分の画素を埋め込み用画素候補とする。埋め込み用画素候補は、ブロック左上の画素を含む市松模様状に配置された画素である。このように埋め込み用画素候補を市松状に配置するのも、画素の変化による視覚的な影響を抑えるためである。

③埋め込み用画素の決定
　埋め込み用画素候補のうち、特定の近傍のビットパターンを持つものを埋め込み用画素とする。近傍ビットパターンが同じ画素は、同じ画素値を持つ可能性が高い。よって、それらの画素を並べて生成したビット列は圧縮が可能となり、秘密情報を埋め込むスペースを確保することができる。近傍ビットパターンは、2 近傍、3 近傍、4 近傍あわせて、合計 64 パターン存在する。

④埋め込み用ブロックの決定
　ある埋め込み用ブロック候補に対して埋め込みを行うと、そのブロック中の埋め込み用画素は変化し、埋め込み用ブロック候補の複雑さも変化する。埋め込みに適したノイズ状のブロックを抽出し、埋め込み用ブロック候補とした。同じように埋め込み用のブロックの複雑さは、埋め込みによって画素の変化が生じたとしても、必ず閾値以上にならなければならない。よって、埋め込み用ブロック候補において、埋め込み用画素をどのように変化させても、その複雑さが常に閾値以上となるブロックを埋め込み用ブロックとする。

⑤圧縮情報の生成と埋め込み
　画像中の全ての埋め込み用画素をラスタスキャン順に並べてビット列を生成する。このビット列を算術符号化により圧縮したものを圧縮情報とする。圧縮情報がビット列より小さいとき、圧縮情報と秘密情報からなるビット列と埋め込み用ブロック内の埋め込み用画素の値を書き換えることで、埋め込みを実現する。

⑥評価
　背景、全景から構成される二値画像、ディザ画像のような二値画像に対して種々の埋め込み抽出実験を行ったところ、従来手法と比較して、同程度のメッセージビットを埋め込んでも、カバー画像のビット変化を抑えられることを確認した。

(2)情報ハイディングの評価手法（ステガナリシス）
　ハイディングの評価の１つとしてステガナリシスへの頑健性が挙げられる。スパースコーディングを利用したステガナリシスについて考察した。ハイディングを行った場合、少なからずカバー画像は劣化する。この劣化が、スパースコード上のガウス性ノイズとして現れることを仮定し、痕跡検出手法を構築し、評価した。濃淡画像をカバーとする場合には、従来手法と比較して、高い検出性能を示した。

(3) (1)を利用したQRコードに対する情報重畳
　カバー画像を QR コードとした場合の性能を調査した。実験の結果、原画像を復元するための情報を効率的に圧縮できず、可逆的には埋め込むことが困難であることがわかった。これは、原画像を復元するための情報が、もともとノイズ状パターンであり、圧縮できなかったことが原因である。そこで、別なアプローチにより QR コードへの情報重畳を試みた。

(4) 終端コード以降のスペースを利用した情報重畳
　ＱＲコードの復号化の過程で、データビット列から文字列に戻す過程に着目する。この過程において、終端パターン「0000」が現れたら文字列の取得は終了し、同時にＱＲコードの復号も終了する。終端パターン以降のビットは読み込まれない。本来、埋め草ビット、埋め草コード語は、データ容量を埋める為のものであり、他に意味はない。データコード語において、終端パターン以降はどのようなパターンでも構わないことになる。
　この特性を利用し埋め込みを実現した。終端パターン以降の部分をオリジナルメッセージのハッシュ値の埋め込み領域とする。データに関する部分の後にあるので、データには干渉せず、データの劣化がない。さらに、終端パターンでＱＲコードの復号は終了するので、復号アプリケーションでは埋め込みの存在は確認できない。
　ハッシュ値の配置領域の確保は、ＱＲコードの符号化の中の「パラメータの決定」の過程の「型番の決定」の部分で行えばよい。簡単にいえば、データ容量を強制的に大きくすることで埋め込み領域を確保する。通常は、モード指示子、文字数指示子、２値化データのビット長が収まる最小のデータコード語数を持つ型番に決定する。確保においては、型番の決定の前の段階でハッシュ値を生成しておく。そして、モード指示子、文字数指示子、２値化データのビット長に加え、終端パターンの 4[bit]、ハッシュ値のビット長が収まる最小の型番に決定する。以上により、ハッシュ値の配置領域の確保を行う。
　改ざん検出のステップでは、まずオリジナルメッセージを抽出しハッシュ値を計算する。さらに、終端コード以降に埋め込まれたハッシュ値を取り出し、比較することで、改ざん検出を行う。

(5) Wet Paper 符号を利用した情報重畳

さらに別なアプローチも考察した。QR コードは白黒二値パターンが表現する情報（見た目の情報であり、以下、表の情報と呼ぶ）と、そこから抽出された誤り訂正語によって復号化される本来伝えたい情報（見た目には分からないので、以下、裏の情報と呼ぶ）から構成されていると考えることができる。ここでは、表の情報を操作することで情報重畳を行い、RSA 公開鍵暗号を利用したディジタル署名により QR コードの改ざん検出を実現する。

まず、QR コードの提供者は RSA 公開鍵暗号の公開鍵、秘密鍵を作成する。つづいて、裏の情報のハッシュ値を計算し、RSA 暗号の秘密鍵で暗号化する。裏の情報、型番および誤り訂正レベルを指定して QR コードを生成する。ディジタル署名は、QR コードの右下からデータ及び誤り訂正コード語の領域に Wet Paper 符号を利用して埋め込む。この領域に対して、暗号化されたハッシュ値を Wet Paper 符号により埋め込む。

QR コードの検証者は提供者から RSA 暗号の公開鍵を入手する。読み取った裏の情報からハッシュ値を計算し、さらに表の情報から暗号化されたハッシュ値を抽出する。入手した公開鍵でハッシュ値を復号化し、計算したハッシュ値と比較することで、改ざん検出することができる。なお提案手法により生成された QR コードでは、改ざん検出しない場合は通常の QR コードと同様な利用が可能である。

(6) QR コードを利用した成績開示システム

QR コードに対する情報ハイティングと公開鍵暗号を利用した情報伝達システムの一つの例として成績確認システムを試作した。QR コードに成績情報を秘匿し、成績情報の安全性を確保するために、RSA 暗号化も併用する方法である。

①秘匿情報の埋込領域

成績情報を QR コードに隠すため、終端パターン以降の空きスペースを利用する。QR コードの復号化は終端パターン「0000」が現れたところで終了するので、終端パターン以降の埋め草キャラクタは読み込まれない。従って、付加情報を埋め込む場所となり得る。

②データコード語の生成

学生の成績情報を符号化する。次は、科目名、担当教師などの公開メッセージを符号化し、終端パターンを加え、成績情報符号を付加するとデータコード語の生成が完了となる。

③成績情報の符号化

各学生の成績データを文字列化する。続いて、各成績の文字列を ASCII コードで 2 進数表現する。その後、2 値化した成績データのビット列を対応した各学生の公開鍵で RSA 暗号化し、すべての成績暗号を足しあわせ、秘匿データを生成する。最後に、秘匿データの先頭に秘匿データのビット数を付加する。

④RSA 暗号化

成績情報は 0ー100 の値であり、ACSII コードで一つの数字を 8 ビットで表現する。つまり、1 人の学生の成績データを 24 ビットで表すことになる。RSA 公開鍵は 40 ビットとし、この 24 ビットのデータに対して暗号化を行う。暗号化データは 40 ビットとなる。

⑤成績情報の復号化

データコード語から秘匿データのビット数を取得する。そのビット数の秘匿データを取得し、秘匿データを 40 ビットずつ分割する。各分割のビット列は学生の成績暗号である。入力された 1 つの秘密鍵ですべての暗号分割のビット列を復号化し、24 ビットの成績の 2 値データを取得する。そして、24 ビットの成績データを ASCII コードで文字列化する。最後に、文字列化した平文は 1ー100 の数値であることを検証する。検証した唯一の正解を出力すれば、自分の成績データを得ることができる。

⑥検証

他人の成績データが復元できる可能性があるのか否かシミュレーションをした。鍵長が 40 ビットの場合、4 万回の試行でも、0ー100 の数値データを復元することはできなかった。つまり、RSA 暗号によって安全性は担保されている。100 人程度のクラスに対して、QR コード 1 つで簡単で安全に個人情報を公開することができるシステムを構築した。

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 3 件）

①Michiharu Niimi, Fuyuki Masutani and Hideki Noda, Protection of privacy in jpeg files using reversible information hiding, Proceedings of International Symposium on Intelligent Signal Processing and Communications Systems 2012, 査読有, 2012, 441-446

②Michiharu Niimi and Hideki Noda, An application of steganalysis based on sparse code shrinkage to watermarking attack, Proceedings of 2012 International

Workshop on Advanced Image Technology, 査読有,2012, 616-621

③Michiharu Niimi and Hideki Noda, An application of sparse code shrinkage to image steganalysis based on supervised learning, Proceedings of the IEEE International Conference on Image Processing 2011, 査読有, 2011, 1981- 1984

〔学会発表〕(計 6 件)
①新見 道治, 野田 秀樹、Wet Paper 符号を利用した QR コードへの情報重畳、マルチメディア情報ハイディング・エンリッチメント研究会、2013 年 3 月 7 日、NICT（京都）

②桝谷 冬樹, 新見 道治, 野田 秀樹、再符号化に耐性を持つ可逆的情報ハイディングを利用した JPEG 画像のプライバシー保護、マルチメディア情報ハイディング・エンリッチメント研究会、2013 年 3 月 7 日、NICT（京都）

③新見 道治, 野田 秀樹、Wet Paper 符号と情報ハイディングを利用した QR コードの改ざん検出、平成 24 年度電気関係学会九州支部連合大会、2012 年 9 月 24 日, 長崎大学(長崎)

③桝谷 冬樹, 新見 道治, 野田 秀樹、脆弱型可逆的情報ハイディングを利用した JPEG 画像のプライバシー保護、平成 24 年度電気関係学会九州支部連合大会、2012 年 9 月 24 日, 長崎大学（長崎）

④桝谷 冬樹, 新見 道治, 野田 秀樹、可逆的情報ハイディングを利用した JPEG 画像のプライバシー保護、マルチメディア情報ハイディング・エンリッチメント研究会、2012 年 3 月 16 日、大阪大学（大阪）

⑤田畑 克宜, 新見 道治, 野田 秀樹、スパースコード縮小の画像ステガナリシスへの応用、平成 22 年度第 63 回電気関係学会九州支部連合大会 、 2010 年 9 月 25 日、九州産業大学（福岡）

⑥新見 道治, 田畑 克宜, 野田 秀樹、画像のスパース表現を利用したステガナリシス、第１０回マルチメディア情報ハイディング研究会、2010 年 6 月 9 日、北海道大学（札幌）

〔図書〕(計 1 件)
①Michiharu Niimi and Hideki Noda, IGI Global, Introduction to Image Steganography and Steganalysis in Multimedia Information Hiding Technologies and Methodologies for Controlling Data, 2012 年 10 月, 29 pages. DOI: 10.4018/978-1-4666-2217-3.ch010

６．研究組織
(1)研究代表者
新見 道治 (NIIMI MICHIHARU)
九州工業大学・情報工学研究院・准教授
研究者番号：２０２６９０８８