二次元コードの電子透かしと応用

小林 哲二 †

日本工業大学 †

１． はじめに

二次元コードのアプリケーションのセキュリティ向上のために，暗号，認証，及び電子透かしを適用できる[1],[2],[3],[4]。本稿では，二次元コードの改ざん対策のために，電子透かしデータとして，認証子（メッセージ認証子又はディジタル署名）の重複データを用いる方式を提案し，考察する。次に，紙幣又は金券に二次元コードを付加し，ネットワークを用いて二次元コードの情報をサーバに送信することによって，紙幣や金券の偽造対策を行う方法を提案し，考察する。

２． 二次元コードへの電子透かしの分類

（1） 二次元コード格納内容に電子透かしのデータを埋め込む方式： 画像等を二次元コードにエンコードする前に透かしデータを埋め込み，二次元コードにエンコードする。二次元コードをデコードしてから，画像に埋め込まれた透かしデータの正当性をチェックする。この方式では，二次元コード格納内容が，画像等の透かしを付加できる情報を含む必要がある。透かしのアルゴリズムは任意のものを使用できる。

（2） 二次元コード（二値画像）に電子透かしを埋め込む方式： 二次元コードの印刷形式の二値画像に電子透かしを埋め込み，透かしの検出はその二値画像から行う。二次元コード格納内容に依存せずに透かしデータを埋め込める。この方式では，透かしのアルゴリズムは，二次元コードに固有のものになるので，次の章では，この場合を考察する。

３． 二次元コードへの重複データ電子透かし

二次元コードの二値画像への埋め込みデータとして，ノイズ対策等のために，重複データを付加する方式を考察する。画素は白画素又は黒画素であり，画素値がビット値に対応する。

３．１ 処理手順

（1） 二次元コードの生成

二次元コードに格納する情報の内容を定め，エンコードする。二次元コード格納内容についての認証子Q（メッセージ認証子又はディジタル署名）を作成し，認証用秘密鍵を保管する。

A Watermarking Method for a Two-dimensional Symbol and Its Application

† Tetsuji KOBAYASHI
Nippon Institute of Technology
Dept. of Computer and Information Engineering,
4-1-1-Joho-Building, Gakuendai, Miyashiro-machi,
Saitama-ken, 345-8501 Japan

（2） 透かしデータの埋め込み

①透かしデータＳを，認証子Qとその重複データで構成する。

Ｓ＝｛Q，Q，・・・，Q｝

例えば，追加の重複データ数が２個のとき，

Ｓ＝｛Q，Q，Q｝ となる。

②透かしデータＳの個々のビットを二次元コードに埋め込むための秘密情報を，画素アドレス群とその順序

Ka ＝｛A1，A2，・・・，An｝ とする。

③ 秘密情報Ka に従って，埋め込み位置の個々の画素に，透かしデータＳに対応した画素値を上書きする。

（3） 透かしデータの検出

①二次元コード（二値画像）を得る。

②秘密情報Ka を使用して，埋め込み位置の画素値を求め，埋め込みデータを得る。得られた埋め込みデータを，

Ｕ＝｛U0，U1，・・・，Um｝，とする。

③二次元コードをデコードして，格納内容から認証子（メッセージ認証子又はディジタル署名）を計算し，Ｒとする。

Ｕの要素U0，U1，・・・，Um が，１つ以上，計算値Ｒと一致すれば，二次元コードは正しい。

３．２ 考察

（1）透かしデータ量： 認証子の重複データを埋め込むので，透かしデータのデータ量が，複製の個数だけ増加する。

（2）埋め込み画素数： 二次元コードの誤り訂正能力を二次元コード全体の画素数WのＰ（%）とすると次式が成立する。

Ｗ・Ｐ／１００ ≧ [透かしデータ画素数] ＋ [ノイズ画素数N] － [透かしデータとノイズの重複画素数]

（3）埋め込みデータのビット誤り対策： 二次元コードをデコードするときの誤り訂正機能から見ると，二次元コードの二値画像に上書きされた埋め込みデータはノイズであるので，埋め込みデータのビット誤りを訂正できない。埋め込みデータも，二次元コードの汚れ・傷などのノイズの影響を受けるので，埋め込みデータのビット誤り対策として，透かしデータに，複製を規定個数付加して埋め込み用データを作成する。従って，埋め込み用データを別の誤り訂正符号で符号化する必要性がない。

（4）攻撃者が，二次元コードの内容を改ざんして，偽造の二次元コードを生成し，透かしデータを埋め込む攻撃への対策：

正当な透かし付き二次元コードをデコードした出力データを，再度エンコードすると，透かし及びノイズのない二次元コードが得られる。この透かしのない二次元コードと，透かし付きの

二次元コードで排他的論理和の演算を行うと，透かし位置とノイズだけを黒画素とする二値画像が得られる。この二値画像については，秘密情報のビットの順番が不明であること，秘密情報の白画素の位置は分からないこと，及びノイズがあることから，攻撃者には透かしデータの内容は分からない。しかし，排他的論理和で得た画像は，透かしパターンを含んでいるので，二次元コードにするデータを偽造し，エンコードして得た二次元コード(二値画像)と透かしパターンの論理和（AND）の演算を行うと正規の透かしのある改ざん二次元コードが得られる。

【対策】　本稿の方式では，二次元コード内容の認証子（メッセージ認証子又はディジタル署名）を二次元コードの透かしデータとしている。攻撃者が二次元コード格納内容を改ざんしても，認証子を作成するための秘密鍵が分からないから，改ざん内容に対応した透かしパターンを作成できない。別の対策案として，二次元コードのエンコード，又はデコードのアルゴリズムを秘密にして，攻撃者には二次元コードに格納された内容が取得できないようにする方式が考えられるが，実現のためには，秘密の二次元コードのアルゴリズムを用いる必要がある。

（5）認証子Q（メッセージ認証子又はディジタル署名）の格納場所について，本稿のように二次元コードの二値画像の透かしデータにする方式と，二次元コード内容に含めて，透かしを使用しない方式がある。これらを比較すると，本稿の方式は，二次元コード格納内容のデータ量増加がないこと，及び透かしの埋め込みのための秘密情報Kaによって，更に安全性を高めることができるという長所がある。

4．紙幣または金券の二次元コードによる偽造対策

4．1　目的

現在の紙幣又は金券は，印刷技術に頼って偽造対策を行っているので，如何に工夫しても，偽造したものが出現する可能性がある。この対策の1つとして，二次元コードは紙に付加できるという特徴を活用し，更にはネットワークも利用することによって偽造を迅速に検出することが目的である。

4．2　二次元コードによる偽造対策

紙幣又は金券にセキュリティ対策を付加した二次元コードを付与しておく。紙幣又は金券を受理した人または機器は，二次元コードをCCDカメラで読取り，その画像又は内容をサーバ（又はセンタ）のコンピュータに送信する。サーバでは，受信した情報によって，紙幣又は金券の偽造の有無を判定する。

4．3　適用モデルと考察

（1）二次元コードの内容：　金額，発行日付，シリアル番号，発行機関名称，その他

（2）　発行者：　紙幣又は金券を印刷時に，その用紙上に，二次元コードも印刷する。

（3）販売者等での利用方法：　利用者が物品購入のために紙幣又は金券を使用した時に，CCDカメラで二次元コードを読取って，発行者サーバに送信することによって，偽造チェックを行える。このことは，任意であるが，偽造の紙幣又は金券で被害を受けるのは販売者等であるから，被害防止のため，実施した方がよい。

（4）一般利用者：　二次元コードをCCDカメラで読取り，その二値画像又は内容を発行者のサーバに送信することによって，偽造チェックを行える（任意）。

（5）発行者の利用方法：　紙幣又は金券を発行後，発行者に還流してきたときに，二次元コードにより，偽造チェックを半自動的に行える。

（6）発行者のサーバ（又はセンタ）：　紙幣又は金券の所有者から，問合せの二次元コードを受信して，それが付与されている紙幣又は金券の正当性を検証して，問合せ者に応答する。シリアル番号の監視を次のように行う。

①二次元コードから無効なシリアル番号が得られた場合，偽造である。

②1つのシリアル番号が，複数回，概ね同じ時刻に，1つ又は複数の端末から送信された二次元コードから検出された場合，少なくとも一方は偽造である。

③1つのシリアル番号が，一定時間内に，その時間内では移動できない場所にある複数の端末から送信された二次元コードから検出された場合，少なくとも一つは偽造である（サーバには接続されている端末の位置及び各端末設置場所の間の最小移動時間を事前に登録しておく必要がある）。

（7）二次元コードには暗号，認証及び電子透かしを併用する。

（8）二次元コードの受信が行われるサーバには，紙幣・金券の所有者は不明であるので，プライバシーに関することは，従来と同じであり，問題ない。

5．むすび

二次元コードの電子透かしに，重複透かしデータを利用する方式を提案し，考察した。二次元コードを紙幣または金券の偽造対策に用いる方法を，適用モデルによって考察した。

参考文献

［1］小林哲二：“証紙類の部分的電子化とセキュリティ”，電子情報通信学会，1999年暗号と情報セキュリティシンポジウム予稿集，W4-3.8，pp. 395-400，Jan. 1999.

［2］小林哲二，増田貴浩，大川貴史：“二次元コードによる学生証のセキュリティ向上”，情報処理学会，情処研報，Vol.2001, No.53, 2001-CSEC-13，May, 2001.

［3］小林哲二：“二次元コードのセキュリティと応用方法の検討”, コンピュータセキュリティシンポジウム２００２論文集，情報処理学会，pp. 349-354, Nov. 2002.

［4］T. Kobayashi and J. Kim: “Security Considerations on Two-dimensional Symbols”, Proc. of the First International Conference on Information Technology & Applications, Paper No. 223-21, pp. 1-4, IEEE, Australia, Dec. 2002.