多層式光学的情報媒体による二次元コードの情報ハイディング

寺浦信之† 櫻井幸一‡
†テララコード研究所
477-0032 愛知県東海市加木屋町郷中53－26
TerraNob@terrara.jp
‡九州大学 システム情報科学府
819-0395 福岡県西区元岡744番地
Sakurai@itslab.csce.kyushu-u.ac.jp

あらまし 通常の光学的情報媒体は可視光を吸収する印材を用いて紙などに印刷し、可視光を投光して、その反射を受光し、解析することで情報を識別している。情報を暗号化することができる二次元コードも開発されているが、可視光を用いた媒体では、コピーが可能であり、セキュリティも高くない。そこで、セキュリティが高く、コピーが不可能な情報媒体を構想している。表層は通常の可視光を用いた二次元コードを印刷するが、その内層に互いに異なる特定の波長を吸収する複数の印材を用いて二次元コードを印刷し、多層の二次元コードを形成する。これら複数の内層に形成された二次元コードに情報分散をさせることにより、高いセキュリティ性を実現する。

Information hiding of two-dimensional code by multi-layer optical

Nobuyuki Teraura† Kouichi Sakurai‡
†Terrara Code Research Institute
53-26 Gochu Kagiya-cho Tokai-city, 477-0032, JAPAN
TerraNob@terrara.jp
‡Information Science and Electrical Engineering, Kyushu University
744 Motooka Nishi-ku Fukuoka,819-0395, JAPAN
Sakurai @itslab.csce.kyushu-u.ac.jp

Abstract The optical information medium printed on paper is used printing materials to absorb visible light. There is the two-dimensional code which can be encrypting. But it is possible to copy. So, we envisage the information medium which is not possible to copy and has high security .In the surface, the normal two-dimensional code is printed. The inner layer is two-dimensional codes printed using a plurality of printing materials absorb certain wavelengths different from each other to form a multi-layered two-dimensional code. Information can be distributed to the two-dimensional codes formed on the inner layer of the multiple.

†寺浦 信之：九州大学システム情報科学府 社会人博士後期課程

1. はじめに

この論文では、紙媒体を用いた光学的情報媒体の情報ハイディングによるセキュリティの高度化について論ずる。

光学的情報媒体では、情報符号として一次元シンボル（バーコード）や二次元シンボル（二次元コード）が用いられている。これらは、POSでの利用のように誰でもが簡単に読めることを目指して開発されたものであり、クレジットカードのようなセキュリティが必要な用途には適していない。特に、コピーが容易である点は、そのような用途では大きな欠点となっている。

そこで、本論文では、現状の光学的情報媒体の二つの課題であるセキュリティの向上とコピー防止について検討し、その後提案する基本構成について提示し、さらにハードウェアおよびソフトウェアによる情報ハイディングによるセキュリティの確保とコピー防止について論じる。また、暗号化二次元コード（SQRC）との比較を行う。

2. 光学的情報の情報ハイディング

2. 1 光学的情報媒体

光学的情報媒体は、当初文字の認識として構想されたが、当時の処理能力では困難であった。そこで構想されたのが、コンピュータ用の文字としてのシンボルである。人には判別が困難であっても、コンピュータにとって判別が容易なシンボルが考えられたのである。当初はまだMPUが発明されていない時代であり、それに対応してブルーアイコードが考案された。その後、MPUの出現や一次元リニアセンサーの出現によってバーコードが発明された。バーコードには、収容するデータの種別（数字、文字、記号など）によって各種のバーコードが考案され、実用に供されている。また、これらの一部はISO／IECによる国際標準として定められている。

バーコードは、横方向にのみ情報を有し、縦方向には情報を有しない。そこで、縦方向のシンボルは冗長度として機能し、一部が汚れなどで読めなくても、その上下を読む事で読取ることが可能である半面、印刷などに大きな面積が必要となり、また含まれるデータ量が少ないという課題があった。バーコードは当初は、IDのみを有することで実用化されてきたが、次第にデータも記憶するニーズが生まれてきたからである。

それらのニーズに答えるために考案されたのが二次元コードである。二次元コードには、スタック型とマトリックス型が考案されており、それぞれニーズ対応する特徴を有した二次元コードとなっている。これらの中で、日本などアジア地域では日本で考案されたQRコードが広く用いられている。

2. 2 セキュリティの向上

QRコードなどの二次元コードはその仕様が公開されており、その読取装置は多くのメーカから発売されており、最近では携帯電話でも読取が可能となっている。そこで、人が目で見て理解できないという、文字と比較してのセキュリティは存在するが、読取装置を有する者にとっては、その内容は簡単に読取ることができる。

そこで、セキュリティ確保のために実際になされているのは、

①アプリケーションレベルの暗号化

②システムレベルの暗号化

である。

2. 2. 1 アプリケーションレベルの暗号化

アプリケーションレベルの暗号化とは、アプリケーションによってデータの暗号化を行い、二次元コードに記憶させ、読取時に読み取ったデータの復号化を行わせることである。これにより、復号化キイを有しない第三者のデータ識別が不可能となるので、セキュリティの確保は実現できる。しかし、個別のアプリケーション毎に暗号化と復号化の処理機能が必要となり、煩雑であるという欠点があった。

2. 2. 2 システムレベルの暗号化

システムレベルの暗号化とは、二次元コードの暗号化方式を予め定め、読取装置が復号化したのちにアプリケーションプログラムにデータを受け渡すものであり、全ての記憶領域が暗号化データ領域である場合と通常の非暗号化領域と暗号化領域の両方を含む場合がある。

この方式では、アプリケーションでの暗号化は必要であるが、復号化については対応する必要がな

いという利点がある。

後者では、非暗号化領域については通常の二次元コードとしての読取が可能であるという利点もある。

システムレベルの暗号化によって、容易に第三者へデータを秘匿することが可能となったと言える。しかし、光学的情報媒体は複製が非常に容易であり、例えばクレジットカードに応用する場合では、クレジット番号が他者に容易に読み取られることはないが、コピーされることで、その行使を防止することはできない。

2．3　コピー品の利用防止

一般の光学的情報媒体では、コピーを防止することは不可能である。それは、光学的情報媒体では、反射波を読取装置に受信させる方式であり、その同じ方式でコピー機などが動作しているからである。そこで、コピー防止を図るためには、原理的に異なる方式が必要である。

3．本提案の原理

光学的情報媒体のセキュリティでは、読取防止とコピー防止が主要な目的となるが、その両方を同時に実現する情報ハイディング手法を開発したので、以下に説明する。

3．1　システムの構成

通常の光学的情報媒体では、読取りに可視光領域の波長を用いる。一方、多層式光学的情報媒体では、読取りに不可視光を用いるところに特徴がある。不可視光を反射する素材（紙など）の上に、不可視光を吸収する印刷材料を用いて二次元コードを印刷する。これにより、不可視光を照射して読取るときに、印刷部分と非印刷部分で可視光を用いたときのように白と黒を表現することが可能になる。このとき、印刷に用いる印刷材料の不可視光吸収の波長をそれぞれ異なった波長にピークを有する印刷材料を用いて印刷し、読取時にそれぞれの層の波長に一致する光源で照射することにより、多層に重ね合わされていても、二次元コードの映像を読取ることが可能になる。

また、情報媒体の表層には、不可視光を透過するが可視光を反射または吸収する印刷材料で二次元コードが印刷されている。この構成により、表面から見た場合には、表面の二次元コードのみが見えるので、コピーをすることが不可能となる。

3．2　ハードウェアによるセキュリティ

多層式光学的情報媒体では、3．1で述べた構造を有しているので、秘匿性の要因として、層数とその印刷材料の吸収波長を用いる。そして、複数の層に分散された情報を記憶する。

3．3　ソフトウェアによるセキュリティ

ソフトウェアによるセキュリティについては、種々の手法を適用可能である。ここでは、視覚復号秘密分散方式の考え方を適用した手法について検討する。

視覚復号秘密分散は、画像データを複数のチャートに分解し、それらの分解された画像片を重ね合わせることで、人の視覚で元の画像を識別する手法である。

二次元コードの復号では、画像センサーによる画像（符号）識別であり、人の画像編集、識別能力を用いることができないが、逆にセンシング能力は人よりも高いと考えられるので、それらを活かした識別手法と言える。

データ分散方法として、セルレベルの分散とビットレベルの分散を検討する。

3．3．1　セルレベルの暗号化と復号化

セルレベルのデータ分散または情報ハイディングは、二次元コードの一つの白黒データについて、各層間にデータを分散することで実現する。

表1　セルレベルの分散の復号化表

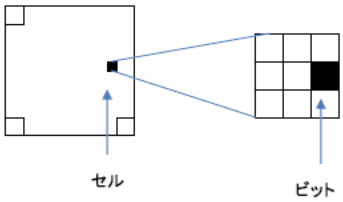
分散色	復号色
白白白	黒
白白黒	白
白黒白	白
白黒黒	黒
黒白白	白
黒白黒	黒
黒黒白	黒
黒黒黒	白

例えば、内層が3層である場合について、検討する。データ分散は、表1のような論理表に従うことができる。論理表は、秘匿されているので、第三者が例え内層の3層すべてについて読取が行えたとしても、論理表がない限り解読は不可能である。また、表に依らずに、排他的論理和などの論理式を用いることも可能である。

3．3．2　ビットレベルの暗号化と復号化

ビットレベルのデータ分散または情報ハイディングは、セルを幾つかの正方形に分割し、分割したドットを各層に分散させる手法である。

図1　セルとビットの単位



ここでは、内層が3層であり、またセルを3X3のビットに分解する例で説明する。

データ分散の過程は、次の3つのステップから構成される。

①セルの分割

②ビットの計算

③ビットの割当

また、ビットレベルへの分散に際しては、表1同様の予め定められた符号化ルールに従って、分散する。

4．提案するセキュリティ方式

ここでは、考え方を具体的に説明するために、表2に示す三つの事例について説明したのち、N層の場合の一般化について論じる。

表2　セキュリティ方式

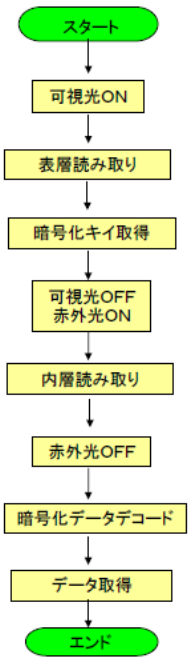
番号	セキュリティ方式	表層	内層
1	暗号化方式	暗号化キイ	暗号化データ
2	セルレベル分散方式	暗号化キイ 復号化ルール	セル分散データ
3	ビットレベル分散方式	暗号化キイ 復号化ルール	ビット分散データ

4．1　暗号キイ方式

ここでは、一番単純化構造を持つ内層1層の場合について、取り上げる。暗号化キイ方式と呼ぶこの方式は、暗号化されたデータを内層に有し、その暗号化キイを表層に保持する方式である。表層と内層は分離されており、読取る場合にのみ合体され、読取り装置によって同時に読取られる。

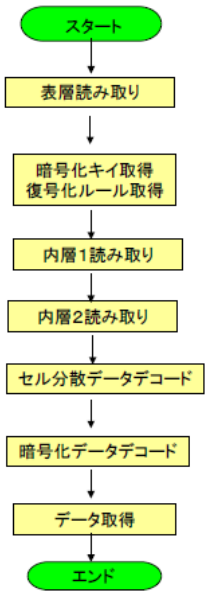
この場合の読取りフローを図2に示す。

図2　暗号化方式



（照明制御を含む）

図3　セルレベル分散方式



4．2　セルレベル分散方式

セルレベル分散方式は、内層に一つの仮想的な光学的情報媒体を設定し、その仮想的な媒体をセルレベルで複数の実在する内層の光学的情報媒体にデータ分散させるものである。すなわち、光学的情報媒体のデータは、セルが白であるか黒であるかによって表現させるが、その個々のセルデータをあるルールに基づいて複数のセルに分解させる。その分散ルールは、表層のデータに保持する。仮想的な情報媒体が暗号化データを保持している場合には、その暗号化キイも表層に保持される。

ここで、分散のルールは、EX－ORなどがある。EX－ORを用いると、内層データの白黒比率をほぼ同じにできる利点がある。

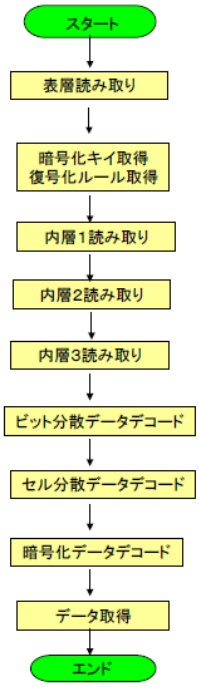
内層が二層である場合について、その読取りフローを図3に示す。

4．3　ビットレベル分散方式

ビットレベル分散方式は、内層に一つの仮想的な光学的情報媒体を設定するところは、上記のセルレベル分散と同じであるが、そのデータ分散の方法が異なる。ビットレベル分散では、書き込む場合にはプリンターなどの印刷手段の分解能で定まるドッ

トレベルで分散する。理想的には、例えば、黒のセルを表現するのにプリンターのドットで60X60ドットで表現される場合には、そこで分解される3600のドットそれぞれで黒を分解するのである。そして、読取る場合には、読取り装置が分解能で定まるドットについて、それぞれの層のデータについて、復号化させる。しかし、現実的には、読取り側のドットの分解能がプリンターのそれと異なり、またドットの各層でのズレが発生し、ドットレベルでは必ずしも、的確な対応とならない可能性がある。そこで、ここでは、セルを複数の仮想的なビットに分解し、そのビットについてデータ分散させる。例えば、一つのセルを3X3の9つのビットに分解し、それぞれのビットデータを各層の実在するデータに分散させる。ここでの分散方式でもEX－ORを用いることが有効である。白ビットと黒ビットの比率を同じにできる利点がある。

図4　ビットレベル分散方式



内層が2層である場合について、その読取りフローを図4に示す。

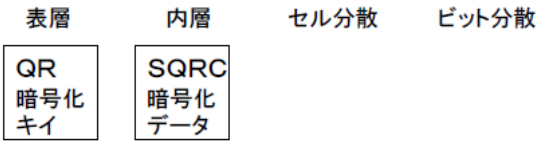
4．4　N層の場合の一般化

前節に示した三つの事例では、内層が二層の場合について述べたが、ここではN層の場合について検討する。N＝1～4について、具体的に提示する。N＝5以上の場合も同様にデータ分散可能である。

4．4．1　N＝1

内層が1層の場合には、データ分散をすることができないので、4．1で示した暗号化キイ方式となる。この場合の構成図を図5に示す。

図5　N＝1の場合（暗号化方式）



4．4．2　N＝2

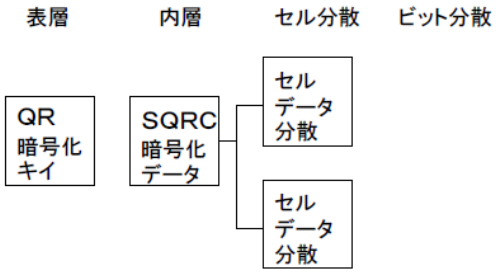
内層が2層の場合には、データ分散をすることが可能であり、データ分散方式としては、セルレベル分散方式とビットレベル分散方式の二つの方式が可能である。これらの場合の構成図を図6に示す。

4．4．3　N＝3

内層が3層の場合には、データ分散の方法としてセルレベル分散方式とビットレベル分散方式に加えて、その一部の併用方式が可能となり、三つの分散方式が可能である。これらの場合の構成図を図7に示す。

図6　N＝2の場合

（1）暗号化＋セルデータ分散方式



（2）暗号化＋ビットデータ分散方式

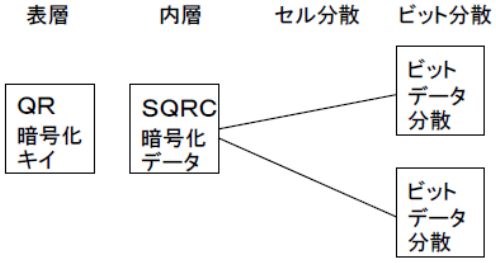
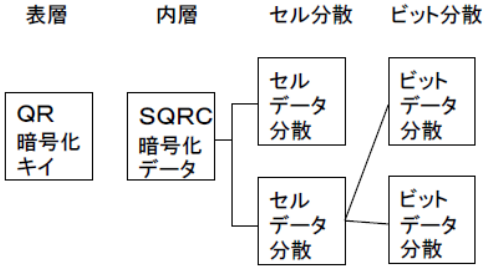


図7　N＝3の場合

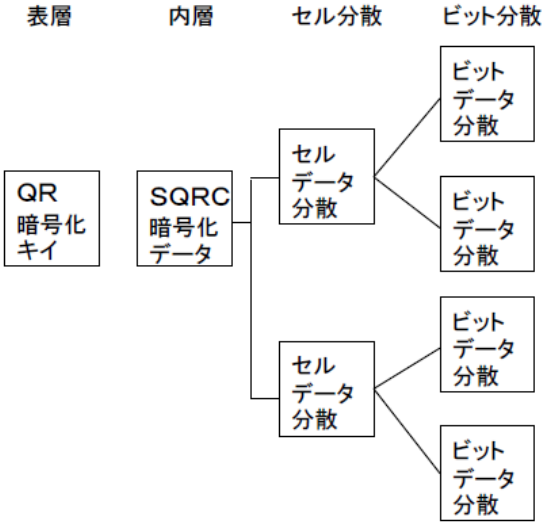
（3）暗号化＋セルデータ分散方式
＋ビットデータ分散方式



4．4．4　N＝4

内層が4層の場合には、データ分散の方法としてセルレベル分散方式とビットレベル分散方式に加えて、その併用方式が二つが可能となり、全部で四つの分散方式が可能である。これらの内、新たに可能になる場合の構成図を図8に示す。この構成の特徴は、全ての内層データがビット分散されており、仮想セル分散データを経て、仮想内層データに統合される。

図8　N＝4の場合



5．SQRCとの比較と補完性

SQRCは、暗号化領域と非暗号化領域を有し、暗号化領域は暗号化キイを有する読取り装置しか読み取ることができない。そこで、閉じた利用領域で用いられる。

一方、多層式光学的情報媒体では、内層に隠された複数の層に仮想的な二次元コードが分散されており、分散ルールを知る者しか読取り結果を復元することができない。

ここで、SQRCは暗号化という手段を用いたコードであり、多層式光学的情報媒体はデータ分散という手段を用いたコードであるので、両者は異なる層の手法であり、両立することが可能である。また、同時に用いることが可能であり、補完関係にあると言え、同時に用いることでセキュリティ性を強化することができる。

6．セキュリティ性のまとめ

本論文で提案した多層式光学的情報媒体によるセキュリティ性について、その要因を表3に示す。

表3　セキュリティの源泉

番号	セキュリティ方式
1	データ存在の秘匿
2	データ読取装置の特殊性
3	データの暗号化
4	データの分散化
5	データと復号化キイの分離

7．終りに

本論文では、非可視光を用いた多層の情報媒体について、それらにデータ分散することによって、情報ハイディングを行い、セキュリティ性の向上を実現し、且つコピーができない情報媒体について、提案した。

参考文献

[1]　寺浦　信之：RFタグ入門、食品包装　2009年1月号　p18−p23、　2009年2月号　p42−p46、2009年3月号　p56−p61

[2]　平本純也：『知っておきたいバーコード・二次元コードの知識』日本工業出版、2006．4

[3]　松井甲子雄：情報ハイディングの基礎、森北出版

[4]　小林哲二：二次元コードのセキュリティ向上と応用、FIT（情報科学フォーラム）2002、M－96

[5]　竹口　佑斗：公立はこだて未来大学卒業論文概要