論文の要旨

自然画像を対象とした視覚復号型秘密分散の物理的実現法

中嶋 瑞穂

はじめに

人間の視覚特性により，それまで見えなかったものが突然現れる「隠し絵」や「だまし絵」は，古来よりさまざまなものが考案されてきた．一方，昨今ではデジタルカメラや計算機の発達により，写真などの自然画像を入手し，計算機処理することが広く行われるようになった．本論文では，複数の画像を OHP シートなどに印刷して重ね合わせると，隠された自然画像が見えるという隠し絵の作成方法を提案する．

本研究と関連の深い研究として，視覚復号型秘密分散が挙げられる．これは暗号復号のために計算機を用いることなく，人間の視覚システムによってメッセージが復号できる暗号の一形態である．視覚復号型秘密分散の 1 つである，(k, n) しきい値視覚復号型秘密分散の概念図を図 1 に示す．ランダムノイズ状の暗号が印刷された複数の OHP シートがあり，このうち任意の k 枚以上を重ね合わせると暗号化されたメッセージが復元されて見えるが，いかなる $k-1$ 枚以下の組み合わせでもメッセージの情報は漏れないという仕組みである．視覚復号型秘密分散においては通常，各 OHP シートにはランダムな砂の嵐状の模様が印刷されている．これに対して OHP シートにランダムな模様ではなく，何らかの意味ある画像が表示されていれば，OHP シートが暗号情報に関係していること自体も隠蔽できる．このような細工を施した視覚復号型秘密分散を，特に拡張視覚復号型秘密分散という．本論文では，グレースケールやカラーの自然画像を対象とし，OHP シートに印刷された 2 枚の画像を重ね合わせると，隠されていた別の画像が見えるという隠し絵の構築法を議論する．これは暗号分野の用語で言うと，(2, 2) しきい値の視覚復号型秘密分散および拡張復号型秘密分散に相当する．本研究では，2 枚の OHP シートに表示される画像をそれぞれシート 1，シート 2 と呼び，特に両者を区別する必要がない場合には単にシートと言う．またその 2 枚を重ね合わせて見える秘匿画像をターゲットと呼ぶ．

従来の視覚復号型秘密分散の研究は基本的な視覚復号型秘密分散に関するもの，拡張視覚復号型秘密分散に関するもの，グレースケールおよびカラー画像を扱うものの 3 種に大別できる．しかしこれらは皆，暗号研究の一つとして位置づけられており，暗号の安全性が絶対的な前提条件だった．この

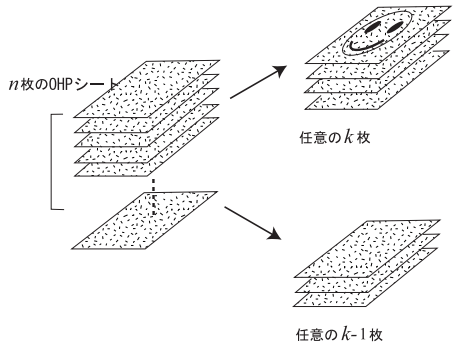

図 1: (k, n) しきい値拡張視覚復号型秘密分散の概念図

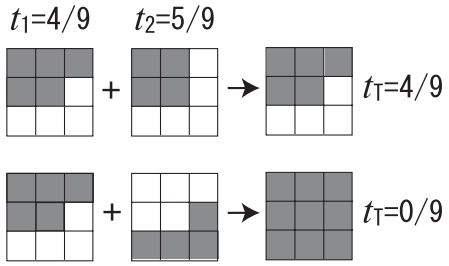

図 2: シート 1，シート 2 のサブピクセルの配置とターゲットの透明度の関係

前提のもとに，秘密分散のためのスキームの提案や，埋め込み可能な画像情報の制約に関する論理的解析を行っていた．これに対して本研究の対象は自然画像の隠し絵であり，自然画像の画質を損なわないよう画像の階調や色の再現性に配慮する必要がある．また隠し絵としての価値を考えると，人間の手で重ね合わせることで容易にターゲットが視認できる点も重要な条件となる．従来の視覚復号型秘密分散の研究では，自然画像を対象として画質の保持に努めたものや，実際に OHP シートに印刷して重ねる際に生じる現実的問題を考慮したものはなかった．一方本研究で扱う隠し絵は，隠し絵として楽しめるものである限り，セキュリティの観点では妥協できる面がある．すなわち，シートからターゲットの画像が予想できなければ，ターゲットの情報が多少シートに現れても特に問題ではないと考えられる．ここでは，本研究で扱う隠し絵を広義の暗号および視覚復号型秘密分散ととらえ，2 枚のシートにターゲットを隠すことを「暗号化」，シートを重ね合わせてターゲットを得ることを「復号」と呼ぶことにする．

視覚復号型秘密分散とハーフトーニング

視覚復号型秘密分散は，印刷分野でよく利用されるハーフトーニングと，シートの重ねあわせに対応するブール代数に基づいたスキームである．ハーフトーニングとはプリンタのトナーやインクのように，オンとオフの 2 値のみを表現できる出力装置で，多階調を疑似表示するための技術である．画像の 1 ピクセルは，ハーフトーニング手法の 1 つである濃度パターン法により，シート上の有限個の透明もしくは不透明のサブピクセルで表現される．画像のピクセルを有限個のサブピクセルで表現可能な透明度として量子化する際には，誤差拡散法などの量子化手法が用いられる．

シートを重ね合わせてターゲットを得る操作は，サブピクセルのブール積に相当する．たとえばシート 1，シート 2 の透明度，t_1, t_2 がそれぞれ $\frac{4}{9}$, $\frac{5}{9}$ であるとき，シートのサブピクセル配置を図 2 上段のようにすれば，重ね合わせた結果のターゲット透明度 t_T は $\frac{4}{9}$ となる．また同じシートの透明度でも図 2 下段のようにサブピクセルを配置すれば，t_T は 0 となる．このようにシートの透明および不透明サブピクセルの配置を調整することにより，ターゲットの透明度を制御できる．

ハーフトーニングによって 2 値化された画像の重ね合わせはブール積となるが，この際，2 枚のシートとターゲットのピクセルの間には次のような制約条件が存在する．

$$t_T \in [\max(0, t_1 + t_2 - 1),\ \min(t_1, t_2)]. \tag{1}$$

ここで，t_1, t_2, t_T はそれぞれ，シート 1，シート 2，ターゲットのピクセルの透明度を表す．シートの画像のダイナミックレンジを $t_1, t_2 \in [L, U]$ とするとき，(1) 式を常に満たすターゲット画像のダイナ

ミックレンジは，

$$t_T \in [\max(0,\ 2U-1),\ L] \tag{2}$$

となる．(1) 式は暗号化のための必要十分条件，(2) 式は十分条件である．

ブール代数に基づくアプローチによる自然画像の扱い

まず従来から用いられているブール代数に基づくアプローチで，自然画像の暗号化を試みた．従来手法で前提とされていた十分条件が満たされるダイナミックレンジは非常に狭いため，暗号化によって自然画像の画質が著しく低下する．そこでダイナミックレンジの制約を緩和する方法を考察した．本研究では画像のダイナミックレンジを (2) 式よりも広く取ることを許すとともに，誤差拡散法を拡張し，量子化誤差に加えて必要十分条件の違反量を近隣のピクセルに分配することで (1) 式の制約違反を解決した．この制約の緩和法はセキュリティ上の脆弱性につながるものであるが，この点についても検討し，セキュリティ低下を最小限にするためのダイナミックレンジ決定法の提案も行った．さらに 2 枚の OHP シートだけでなく，3 枚以上の OHP シートに複数の画像を暗号化することも可能であることを示した．

連続量的アプローチによる自然画像の扱い

自然画像の画質を向上させるためには，ダイナミックレンジ幅だけでなく階調数も重要な要素である．従来型のブール代数に基づくアプローチでも原理的には階調数を無限に増やせるが，階調数の増加にともなってサブピクセルが小さくなるため，2 枚のシートを重ね合わせるのが困難になる．そこで中間階調が増えても人間の手で重ね合わせやすい暗号化手法として，ドット分散型ではなくドット集中型のハーフトーニング手法を利用することを考える．しかし単なるドット集中型では，シートの透明度のみでサブピクセルの配置が決まってしまい，ターゲットの透明度を制御できなくなってしまう．本研究では透明・不透明の 2 値ではなく，中間的なグレーを導入することによってこの問題の解決を図る．さらに，位置誤差を含んだ重ね合わせ画像を計算機でシミュレートし，画質評価の指標である PSNR 値を求めることによって，この連続量的な手法が位置誤差に関して頑健であることを検証した．

カラー自然画像のための視覚復号型秘密分散

より一般的な自然画像としてカラー画像を扱う手法を検討する．自然画像の隠し絵では，色の再現性は欠くことのできない条件である．そこで，視覚復号型秘密分散において適切に色を再現する手法について考察した．具体的には，一見一様な中間色に見える 2 枚のシートを重ねると，隠された自然画像のターゲットが見えるというスキームである．このスキームの実現方法として，シート 1 は透明および不透明サブピクセルからなる市松模様，シート 2 は表示色およびその補色のサブピクセルからなる市松模様として，両シートを重ねるとシート 2 の補色部分がシート 1 の不透明部分にマスクされる，という方法を考案した．ただし，シート 1 の市松模様には入力された自然画像の情報が全く含まれておらず，本手法は暗号の「秘密分散」としては機能していない．画像を安全に隠蔽するスキームの構築は重要な課題ではあるが，本研究ではカラー自然画像の扱いが主眼であり，自然画像の色を忠実に再現できる方法を検討した．ここで重要となるのは，シート 2 の表示色と補色の決定法である．シート 2 全体として一様な中間色を実現しつつ，ターゲットが元の画像の色を適切に再現できるものでなくてはならない．この問題を解決するため，計算機でよく用いられる RGB 色信号空間ではなく，知覚色を表現できる CIE-XYZ 色空間において，表示色と補色の計算を行う．表示色および補色の決

定方法としては，出力機器で表示可能な色範囲から平行六面体を切り出す方法と，必要に応じて各色の彩度情報を変更する方法の 2 つを提案した．プリンタでは出力機器の特質に由来する技術的困難があるものの，ディスプレイやプロジェクタなどの加法混色に基づく出力機器では好ましい結果が得られ，手法の基本的な有効性が確認できた．

おわりに

本論文では，自然画像を対象とした隠し絵の構築法について研究した．まず本研究と関連の深い視覚復号型秘密分散の研究を概観し，暗号化の制約条件である画像ダイナミックレンジの制約を提示した．この制約は非常に厳しく，暗号化された自然画像の画質が大幅に低下してしまうことから，制約を緩めて画質を維持する手法を提案した．また従来手法では画像の階調数を増やすと，サブピクセルが細かくなるため人間の手でシートを重ね合わせにくくなるという問題点があったが，本論文では連続量的アプローチを導入し，復号時の位置誤差に頑健で，多階調表現が可能な暗号化手法を考案した．カラー自然画像の視覚復号型秘密分散においては，適切に色を再現する手法について考察した．具体的には，一見一様な中間色に見える 2 枚のシートを重ねると，自然画像のターゲットが復号されるスキームを提案した．このスキームを実装し，複数の出力機器を用いて実験を行い，手法の基本的な有効性を確認した．