視覚復号型秘密分散暗号の復号に要求される重ね合わせ精度
Required Overlay Accuracy for Decryption in Secret Sharing Visual Cryptography

大槻　正伸[†]，小泉 康一[†]
Masanobu Ohtsuki，　Koichi Koizumi

[†]福島工業高等専門学校
National Institute of Technology, Fukushima College
ohtsuki@fukushima-nct.ac.jp

概要

視覚復号型秘密分散暗号は，文字などが描かれた元情報の画像を数枚の画像に分けて暗号化し，そのうち何枚か（または全部）を集めて重ね合わせることにより元の情報が復元できるものである．重ね合わせにより復号化された元情報の文字などの認識は人間の視覚的な認知能力によりなされる．

本研究では，復号に要求される画像の重ね合わせ精度を定量的に測定し明らかにするものである．

キーワード：秘密分散，　視覚暗号，(K,N)しきい値法

1.　はじめに

視覚復号型秘密分散法の（K,N）しきい値法とは，文字や絵などの視覚情報を N 枚の画像情報に分け，そのうちどの K 枚でも集めて画像を重ね合わせると元の情報が視覚的に復元できるが，どの(K-1)枚以下集めても元の情報を復元できないという暗号方式であり，Naor と Shamir により提案された[1].

以下本研究では(K,N)= (2,2)しきい値法を扱う．

(2,2)しきい値法の簡単な例を図 1 に示す．図 1 では，「×」が描かれた元画像があるが，この画像情報を，画像 A と画像 B の N(=2)枚に分割する（分割方式については後述）．画像 A，B は例えば，透明シート等に印刷する．K-1=1 枚の画像 A，あるいは画像 B だけを見ても「×」の情報は得られないが，K(=2)枚を重ね合わせると，元の「×」の情報が視覚的に得られる．図 1 では画像 A，B のドットの重ね合わせを「＋」で表している．この「＋」は，各点の 0（白），1（黒）の論理和（OR）と解釈することもできる．

さて，実際に本論文のこのページを OHP シート等の透明なシートにコピーし，透明シートの画像 B（A）を元のページの画像 A（B）に正確に重ねると，「×」が浮かび上がることが確認される.しかし，この 2 枚の画像 A，B を，「×」が認知できる程度に正確に重ね合わせるのには，慣れないと少々苦労すること，また完全に重ね合わせれば「×」が認知されるのは当然であるが，重ね合わせが不完全でも，ある程度正確に重ね合わせ

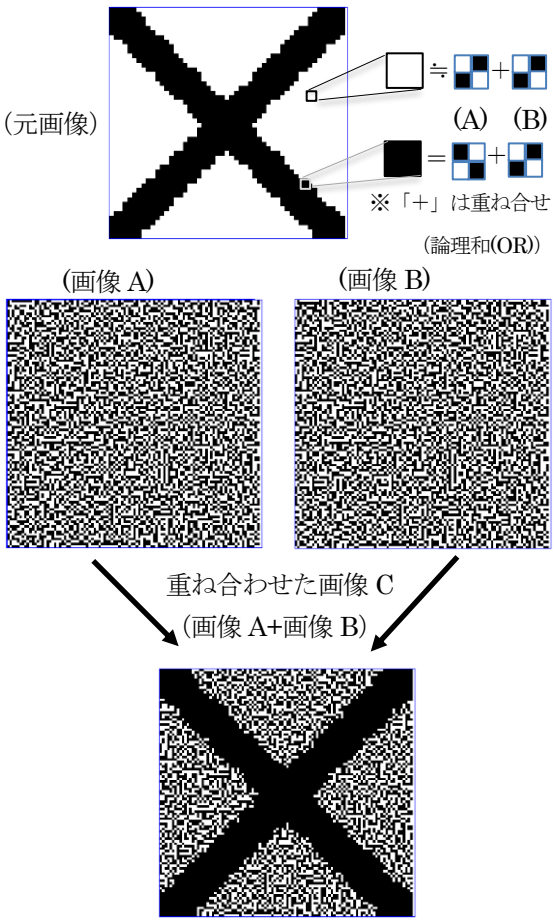


図 1　(2,2)しきい値法視覚暗号の例
($(rw_C,rb_C)=(0.5,1.0)$)

れば黒色の文字でなく，やや光ったような感じの「×」の文字が認知されることも体験できる．それでは，元画像の文字情報「×」を認知できるためには，どの程度正確に画像 A,B を重ね合わせなくてはならないかを定量的に調べるのが本論文の目的である．

以下で，(2,2)しきい値法について，および本論文の背景について簡単に説明する．

図 1 に示す通り，画像の 1 画素（（小さな□の領域 1 つ，これを以下「1 ドット」とよぶこととする）に対し，その 2×2 領域（小正方形）への分割（田）を考える．

1 ドットが白（□）であれば，2×2 分割のうち 2 つを（通常ランダムに）黒として，このドットの画像 A における情報＝このドットの画像 B における情報とする．

そうすると，画像 C=画像 A＋画像 B（A,B の重ね合わせ）とすると，画像 C におけるこのドットは 1 ドット領域の 50%が白，50%が黒となる．

同様に，黒のドット（■）の場合，その 2×2 の分割（田）で，画像 A における場合，ランダムに 2 つ黒とし，画像 B における場合，画像 A での白黒を反転したものにする．そうすると，重ね合わせた画像 C では，このドットは 1 ドット領域の 100%が黒となる．

このようにすると，画像 A，B では，ともに白ドット（□）の部分も，黒ドット（■）の部分も，ランダムに 50%（2 個／4 小正方形）が黒であり，画像 A のみあるいは B のみでは元の「×」の情報は得られない.しかし，画像 C＝画像 A＋画像 B の重ね合わせとすると，画像 C では「×」が視覚的に認知される（以下「画像 A」，「画像 B」，「画像 C」は上の意味で用いる（分割暗号化した画像を A，B，重ね合わせた画像を C とする）．

人間の視覚においては，50%黒のドットが集まった領域と 100%黒のドットが集まった領域は明瞭に区別でき，重ね合わせにより「×」の情報が復元されることになる．ただし，元画像で白い領域の部分は，画像 C では完全に白ではなく，全体として画像 C は元画像とは異なるが，人間の視覚認知能力により元の文字等の情報が認識されることになる．

このように，この程度の文字や大雑把な絵などに限定すれば，情報はこの方式により，画像 A，B に暗号化され，1 つの画像のみでは意味をなさず，重ね合わせにより復号ができる暗号システムとして成立している．実際には相当細かい絵のカラー画像に関する暗号システムも構築されている[3].

さて，ここで一般的に M を画像（A，B，または C）とするとき，rw_M を「元画像の白の 1 ドット（□）を表現する際の画像 M におけるドットの黒の割合」，rb_M を「黒の 1 ドット（■）を表現する際の画像 M における黒の割合」とする．上の例では$(rw_C,rb_C)=(0.5, 1.0)$である．そして$(rw_C,rb_C)=(0.5, 1.0)$であれば，ある程度大きな描画平面に描かれた「×」「○」「＋」「◎」程度の文字は十分認知，識別可能である.そして，$(rw_A,rb_A)= (rw_B,rb_B)= (0.5, 0.5)$であるから，画像 A，または B のみでは，何の情報も得られず，暗号システムとして成立する．

この視覚復号型暗号について，

（1） 暗号システムとして成立するための(rw_C,rb_C), (rw_A,rb_A), (rw_B,rb_B)の条件

（画像の黒部分の密度の条件：どの程度の白黒の割合で，文字が認識できるか，また認識できなくなるか，ひいては暗号システムとして成り立つか，成り立たないか）

（2）復号化に必要な空間的精度の条件

（復号する際の重ね合わせの精度の条件）

（3）復号するのに必要な時間的精度の条件

（画像 A を固定し，画像 B を例えば真横右におき，左にスライドしていくとある時間文字が認識できる．スライドする速度と認識可能性，認識時間の関係等）

等については認知科学的にはほとんど調べられていないのが現状である．従来の視覚復号型暗号の研究は，基本的に，「元画像の各ドットを，一般的に n×n 分割し，どのように白黒を組み合わせれば暗号システムとして成立するか」等の組み合わせ数学的研究が主であり，暗号システムとして成立するための条件についての認知科学的研究はほとんどなされていない．

そこで，上記（1）の条件すなわち，(rw_C,rb_C), (rw_A,rb_A), (rw_B,rb_B)が上記の値以外のところで，どのような値であれば視覚複合型暗号として成立するかを認知科学的実験により調べたのが[4]である．

今回の研究は，上記（2）の復号のための画像 A，B の重ね合わせに要求される空間的精度を認知科学的に調べるものである.これは，この種の視覚復号型暗号を紙や透明シートに印刷し，カードゲームなどに使用する際，プレーヤーが 2 枚のカードを合わせて文字等カードの種類を認識する場合の復号しやすさ，復号しやすくするための指針も与えることになる．

２．実験プログラムの設計

まず，図 2 の実験用プログラムを作成した．図 2 では，画像 A，B が正確に重ね合わされ「○」が現われているところである（画面の一部が示されている）．

この実験用のプログラムでは，

（1） n：1 ドット（□）の一辺の分割数（i.e. 1 ドットは n×n の小領域に分割する．

n=2 の場合 □→**田と分割する**）

（2）L[cm]：1 ドット（□）の一辺の長さ

（3）rw_C, と rb_C （前節参照）

（4）画像 A（固定）に対して画像 B をどの程度ず

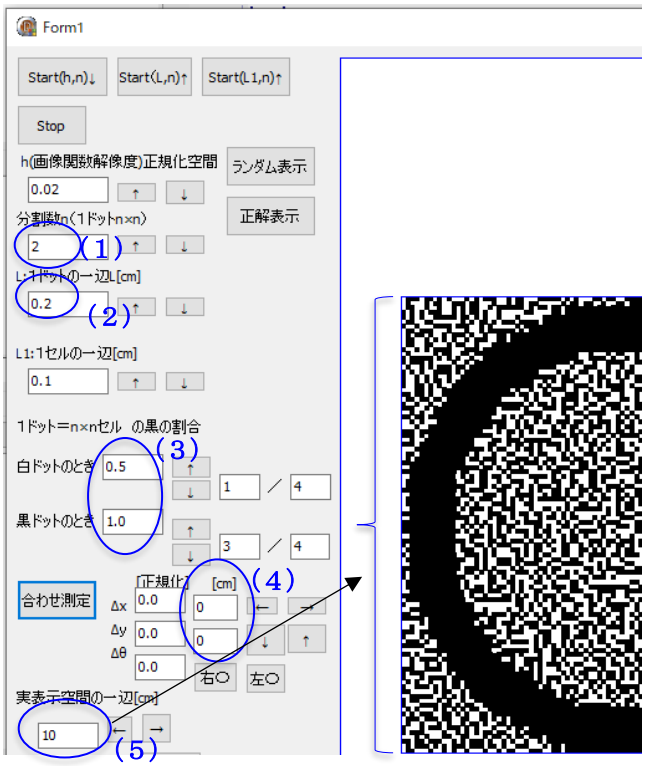
らすか.

Δx,Δy：x 軸,y 軸方向にずらす量[cm]

（５）画像全体を表示する画面の一辺の長さ[cm])

等が設定できるようになっている.

そしてプログラムでは，今回は表示画面に「○」「×」「＋」「■」「◎」のうちの一つが表示できるようになっている.



（１）１ドット１辺の分割数

（２）１ドットの１辺の長さ L[cm]

（３）rwc，rbc

（４）画像Ａに対する画像Ｂのずらし量　（Δx[cm],Δy[cm]）

（５）画像全体の表示画面の一辺の長さ[cm]

図２　実験用プログラム画面

３．実験方法

次のような条件で実験１，実験２を行った.

【実験１】（図３（上））

①n=2　（1 ドットを 2×2 の小領域に分割

②L=0.2[cm]　（1 ドットの一辺）

したがって 1 小正方形は一辺 0.1[cm]

③rw_C=0.5，　rb_C=1.0

④Δx,Δy を　-0.2[cm]～+0.2[cm]の間で，0.02[cm]間隔で動かして「○」の見え方を評価した.

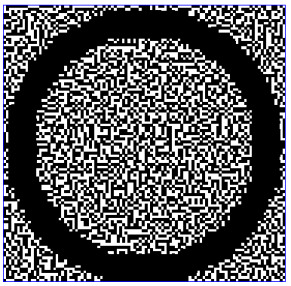
⑤表示画面の一辺＝10.0[cm]

⑥ディスプレイと被験者の顔（両眼（瞳の中心）の乗る平面）との距離=70[cm]，ディスプレイと両眼の乗る平面は平行とした.

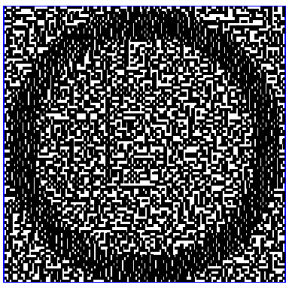
⑦　表示文字は「○」とした.

実際の表示画像の例は図３（上）のとおりである.

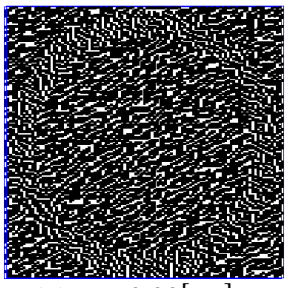
（いくつかの Δx,Δy について，表示画面のみを縮



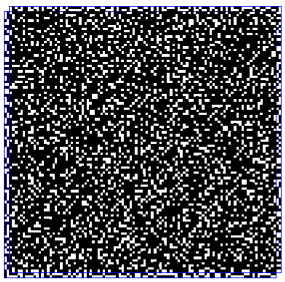
(A) Δx=0.00[cm]
Δy=0.00[cm]



(B) Δx=0.04[cm]
Δy=0.00[cm]

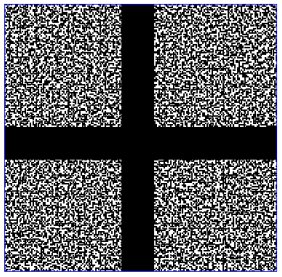


(C) Δx=0.09[cm]
Δy=0.04[cm]

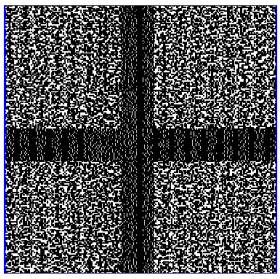


(D) Δx=0.2[cm]
Δy=0.2[cm]

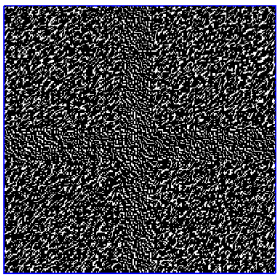
【実験１】



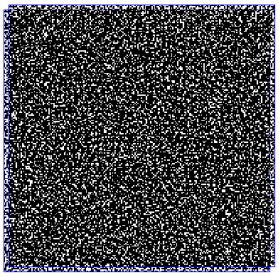
(A) Δx=0.00[cm]
Δy=0.00[cm]



(B) Δx=0.02[cm]
Δy=0.00[cm]



(C)Δx=0.04[cm]
Δy=0.04[cm]



(D) Δx=0.2[cm]
Δy=0.2[cm]

【実験２】

図３　実験用プログラムの実行画面例

小して示してある）.

【実験２】（図３（下））　実験１と同様であるが，
①　n=4,　⑦表示文字は「＋」とした
（したがって，１小正方形は１辺 0.05[cm]）
それ以外の条件は実験１と同じとした.

なお，予備実験で⑦の条件を「○」としてもほぼ同様の結果が得られることをいくつかの(Δx,Δy)で確認してある.

図３の例を見ると，(A) (Δx,Δy)=(0.00,0.00),i.e.ずらしなしの場合は，明瞭に「○」「＋」が認知されるが，(B) (Δx,Δy)が少し増加すると元画像が薄れ始め，もう少し増加すると，(C)白黒反転したような文字（「○」や「＋」）が現われ，(D)さらに増加し x,y 方向に１ドット分ずらすと，当然ながら元画像の情報が全く認知できなくなる.なお，この(A)(B)(C)(D)の現象は他の文字「×」「＋」等でも同様に起こることが確認されている.

さて，被験者 O が，前記の条件で実験を行った.いろいろな(Δx,Δy)（前述の通り Δx,Δy ともに-0.2[cm]～+0.2[cm],　0.02[cm]間隔で動かして）「○」「＋」に対し，表示画面に(Δx,Δy)だけずらして重ね合わせた画像を表示し，全く文字等が認識できない場合を０として，認識できた場合その明瞭さを５段階評価した

（1：ほんの少し認識できる←→5：明瞭に認識できる）．また，文字が図 3(C)のように白黒逆転してなんとか認識できる場合を-1 として記録することとした.白黒反転して認識できる場合は，いずれの場合も微妙であり，明瞭には認識できなかったため，見え方に差をつけず記録としては-1 のみとした.

４．実験結果

図４に実験結果を示す.図では，濃い青色(5)ほど明瞭に元の画像を認知できること，濃い青→青→深緑となるほど認知できにくくなることとして示してある.赤色は全く認知できなかったこと(0)を，灰色は白黒反転したような元画像が認知できたこと(-1)を示す.図 4 を見ると，以下のことが示唆される.

（１）　明瞭に（レベル３以上程度に）元画像情報を認知するには，小正方形の１辺の半分（L/2n）以下程度の正確さで，画像 A.B を重ね合わせる必要がある.

（２）　白黒反転して，ぼんやり元画像が認知できる領域がある.そしてそれは(Δx,Δy)=(0,0)を中心に，半径 L/2 程度の範囲のずれまで広がっている.

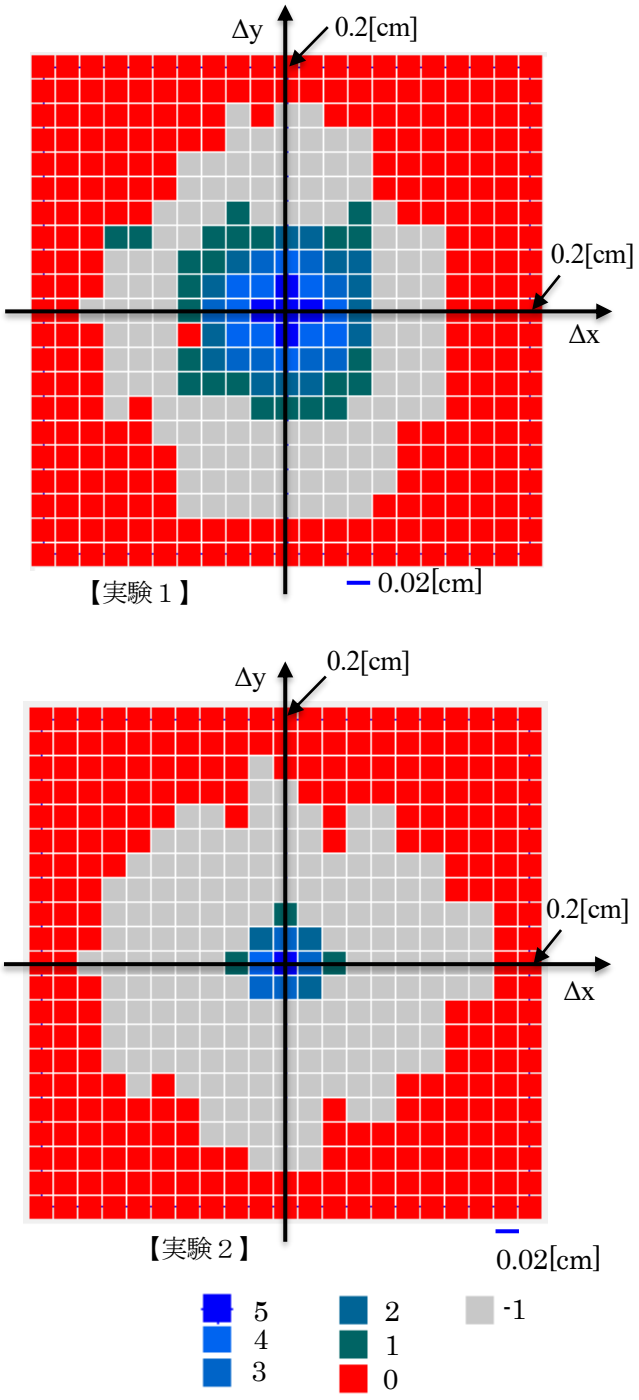


図４　実験結果（(上）実験１，（下）実験２

したがって，明瞭に元画像を知覚できなくとも，ぼんやりながら認知できる領域（レベル 2，1，-1）がある程度の大きさで存在する.

ただし，これらはこの２つの実験結果により示唆される推論であり，これを明確に主張するにはさらに詳しい実験が必要となると考えられる.

従来の視覚復号型暗号の研究においては，正確に画像を重ね合わせれば元画像の情報が得られること等を数学的に議論していたため，上記（2）についてのようなことは考慮されていなかった.（2）は今回見つかった新しい知見と考えられる.実際に，図 1 の「×」の画像についても（透明シートコピー等で重ね合わせることにより）実際に（2）の現象を確認することができる.

さて図 1 の「×」の場合，元の画像は 1 辺 10.0[cm]（正確には x 軸方向は 10.0 の点からもう 1 ドット描いているから 10.2[cm]）それを，縮小して，画像を論文に貼りつけてあり，A4 用紙に印刷すると，3.35[cm]となるから，3.35/10.2≒0.33 倍に縮小されている.

したがって，1 ドットの 1 辺は 0.2[cm]×0.33＝0.066[cm]程度となり，画像 A.B を重ね合わせて，明瞭に「×」が認識できるようにするには，x 軸，y 軸方向とも，L/2n＝0.066/4[cm]程度, すなわち, 0.01～0.02[cm]程度の精度で重ね合わせる必要があることが今回の定量的な測定から見積もることができる.

４．結言および今後の課題

視覚復号型暗号で特に（2,2）しきい値法において，元画像の文字等の情報を得るには，画像 A，B をどの程度正確に合わせる必要があるのか（復号化に必要な空間的精度）について, 心理物理学的実験により測定した．おおよそ，縦方向(y 軸方向)，横方向（x 軸方向）ともに，ずれを L/2n 程度以下に抑える必要があることが推定される結果となった.

また,「白黒反転での微妙な元情報再現領域」もあることが分かった.

今後の課題としては次のことがあげられる.

（1） より多くの条件（n，L の条件，元情報の文字の細かさ等の条件で，他の被験者の実験）でも, 同様のことが成り立つことを確認すること.

（2） 画像 A に対して，画像 B を回転してずらした場合についても今回同様の実験を行うこと.

（3） 白黒反転での微妙な元情報再現の現象について数学的に理由を明らかにすること.

（4） ２つの画像を（不完全に）重ね合わせた画像を与え, 人間が知覚する文字等を計算するアルゴリズムを設計し, 視覚復号型暗号における人間の認知過程と同様の機能をコンピュータに組み込むこと.

（5） 復号するのに必要な時間的精度の条件（1 節参照）について調べること

等があげられる.

文献

[1] M.Naor,A.Shamir(1990),“Visual Cryptography”, (Advance in Cryptography-EUROCRYPT’94), Lecture Notes in Computer Science Vol.950, Elsevier,pp.1-12,

[2] 視覚復号型秘密分散法 http://ohta-lab.jp/users/mitsugu/research/VSSS/main.html （2021 年 4 月 8 日現在）

[3] 石原 武 (2003)，カラー画像に対する効率的な視覚暗号の構成法， 筑波大学大学院 システム情報工学研究科修士論文, 2003

[4] 大槻 正伸， 小泉 康一(2020)”視覚復号型秘密分散暗号と視覚認知能力”, 日本認知科学会第 37 回大会論文集 pp. 294-299