視覚復号型秘密分散暗号と視覚認知能力
Secret Sharing Visual Cryptography and Visual Cognitive Capability

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，復元画像に対する認知可能性の条件を定量的に測定し，視覚暗号システムが可能であるための条件について考察した．

キーワード：秘密分散，視覚暗号

1. はじめに

視覚復号型秘密分散法[1][2]とは，文字や絵などの視覚情報をいくつかの画像情報に分け，分けた情報をいくつか集めると元の文字や絵の情報が復元できるというものである．より正確にいうと，(K,N) しきい値法とよばれる視覚復号型秘密分散法は，文字や絵などの画像情報を N 枚の画像に分け，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ものである．

簡単のため，(K,N)=(2,2)のしきい値法の視覚復号型秘密分散法での例を図 1 に示す．図 1 では，「○」が描かれたモノクロの元画像があった場合，この画像情報を，画像 A と画像 B の N(=2)枚に分割する．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「○」の情報が得られる．

この際，画像 A,B への情報の分け方であるが，図 1 に示す通り，画像の 1 画素（(小さな□の領域 1 つ，これを 1 ドットとよぶこととする）に対し，その 2×2 領域への分割（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 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 100%黒となる．

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）．

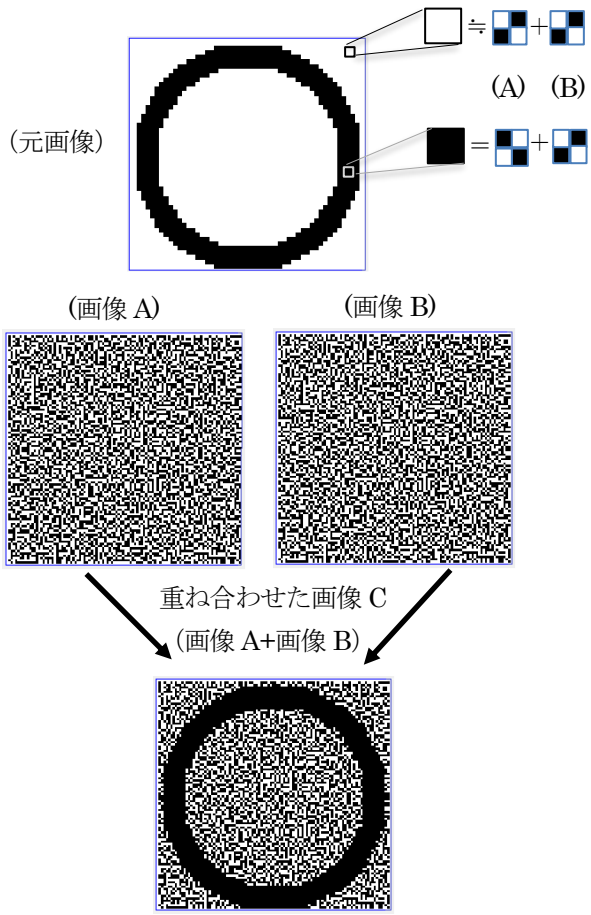


図 1　(2,2)しきい値法視覚暗号の例
$((rw_C,rb_C)=(0.5,1.0))$

人間の視覚においては，50%黒のドットと100%黒のドットは明瞭に区別でき，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 では全くの白ではなく，すなわち全体として画像 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[2].

さて，ここで一般的に X を画像（A,B,または C）とするとき，rw_X を「元画像の白の 1 ドット（□）を表現する際の画像 X におけるドットの黒の割合」, rb_X を「黒の 1 ドット（■）を表現する際の画像 X 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，識別可能であり，暗号システムとして成立することが確認されるが，$(rw_C,rb_C)=(0.5, 1.0)$の組み合わせ以外ではどうなっているのか，視覚暗号システムとして成り立つのかどうか等についての詳しい認知科学的議論はほとんどなされていない．

例えば，$(rw_C,rb_C)=(0.25,0.5)$の場合の例を図 2 に示す．

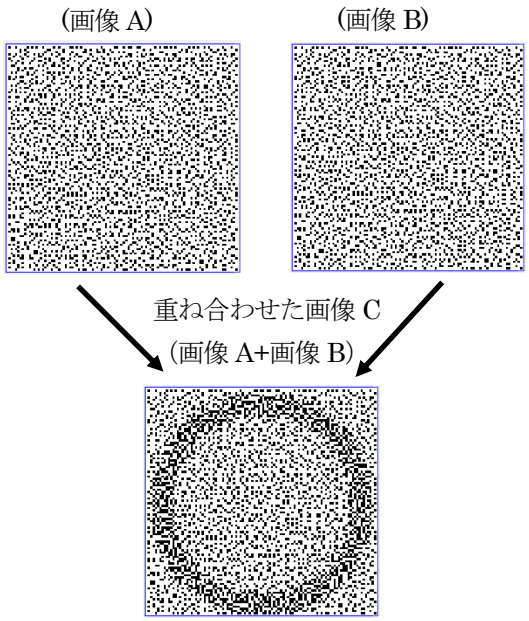


図 2　(2,2)しきい値法視覚暗号の例
（元画像は図 1 と同じで，$(rw_C,rb_C)=(0.25, 0.5)$）

この場合，簡単な文字程度を扱う暗号システムとしては成立しそうであるが，$(rw_C,rb_C)=(0.5, 1.0)$の場合に比べ明瞭さに欠けることが分かる．

また，$(rw_C,rb_C)=(0.25, 0.75)$の場合は，図 3 のようになる．$(rw_C,rb_C)=(0.25,0.5)$の場合（図 2）に比べ，復元した画像 C は，白黒の差が明瞭ではあるが，画像 A,B に「○」

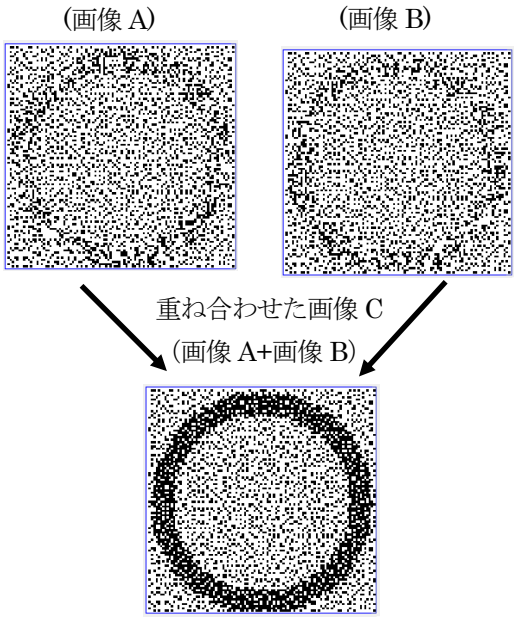


図 3　(2,2)しきい値法視覚暗号の例
（元画像は図 1 と同じ$(rw_C,rb_C)=(0.25,0.75)$）

の情報が入り込んでいて，暗号システムとしては成り立たない．

これは，1 ドットを 2×2=4 個の領域に分け，そのうち$(rw_C,rb_C)=(0.25, 0.75)$とするためには，$(rw_A,rb_A)=(rw_B,rb_B)=(0.25,0.375)$とするのが自然であるから，結果，0.25 と 0.375 の差のために，画像 A,B のみでも「○」が認識されてしまうのである．

一方，$(rw_C,rb_C)=(0.25,0.5)$の場合（図 2）は$(rw_A,rb_A)=(rw_B,rb_B)=(0.25,0.25)$となり，画像 A,B のみでは「○」が認識されず，暗号システムとして成立する．

以上のことから，このような視覚復号型秘密分散暗号のシステムが構成できるための条件を調べる問題が提示される．以下ではより一般的に「1 ドットを 2×2 の 4 領域に分割」でなく「n×n 領域に分割する」ものとして考える．

暗号システムとして成立するためには，

（1）画像 A,B において，すなわち(rw_A,rb_A)と(rw_B,rb_B)に関して，rw_A と rb_A（rw_B と rb_B）が十分近く，人間の視覚では「○」等の情報が全く復元でき

ないこと

（2）画像 C において，すなわち(rw_C,rb_C)に関して
rw_C と rb_C が十分離れていて，人間の視覚で十分「○」等の情報が復元できること

の２つがあげられる．

(rw_X,rb_X)に関して，人間の視覚的に「十分近い」「離れている」とはどの程度なのか，それを心理物理学的実験により定量的に測定し，結果を示すのがこの論文の目的である．

今回は，「コンピュータを用いて統計的に暗号を破ろう」というようなことは想定していない．すなわち，例えば n×n＝10×10 で，(rw_A,rb_A)＝(rw_B,rb_B)＝(0.25,0.28)では，人間の視覚的には区別がつかず視覚暗号として成立するが，統計的に調べられると画像 A(orB)のみでも情報が読み取られてしまう，という可能性はある．今回は，このような統計処理を用いた悪意の第三者は想定せず，純粋に人間の視覚認知的に「「○」「×」等の大雑把な図形が区別できる，できない」ための(rw_X,rb_X)について実験的に調べようとするものである．

２．実験方法と結果

まず，図 4 の実験用プログラムを作成した．図 4 では「×」が表示画面に表示されているところであるが，全体画面の一部のみが示されている．

この実験用のプログラムでは，

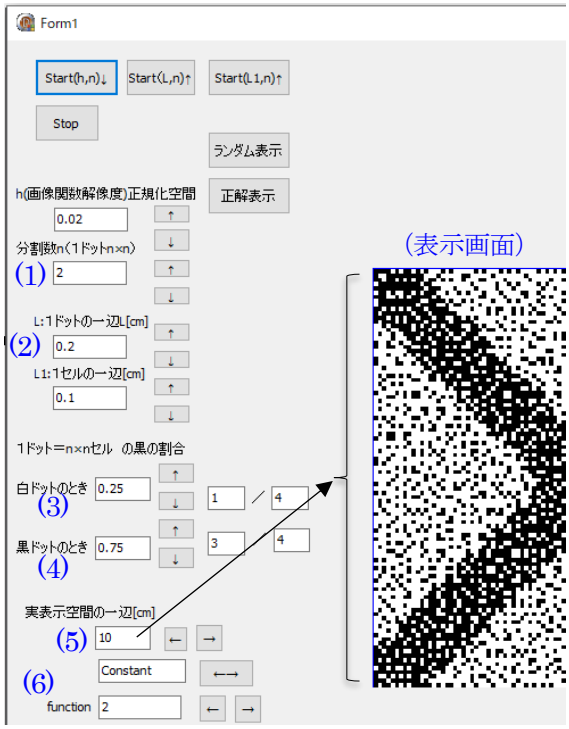
・n：１ドットの一辺の分割数（i.e. １ドットは n×n の小領域に分割する） (1)
・L[cm]：１ドット（□）の一辺の長さ (2)
・白のドットを表現する場合の黒の小領域の割合 =rw (3)
・黒のドットを表現する場合の黒の小領域の割合 =rb (4)
・表示画面の大きさ（表示画面の一辺の長さ[cm]）(5)
・表示する文字の選択 (6)

等が設定できるようになっている．

今回は表示画面には「○」「×」「＋」「■」「◎」のうちの一つが表示されるようにした．

この実験用プログラムを用いて，実験条件を次のように設定して実験を行った．

① 使用した液晶ディスプレイの１ピクセルの１辺＝0.027[cm]



（1） 1 ドットを n×n 分割数に分割する際の n
n=2 の場合（□→田）
（2） 1 ドット（□）の一辺の長さ
（3）rw （4）rb （5）表示画面の一辺の長さ[cm]
（6）表示する文字選択（1⇒「＋」 2→「×」等）

図 4 実験用プログラム画面

② 1 ドットの一辺 L=0.54[cm]
（一辺 20 ピクセルの正方形で 1 ドットを表現）

③ n=10 （1 ドットを 10×10 の小領域に分割，1 小領域は一辺 0.054[cm]＝2 ピクセル）

④ 表示画面の一辺＝12[cm]

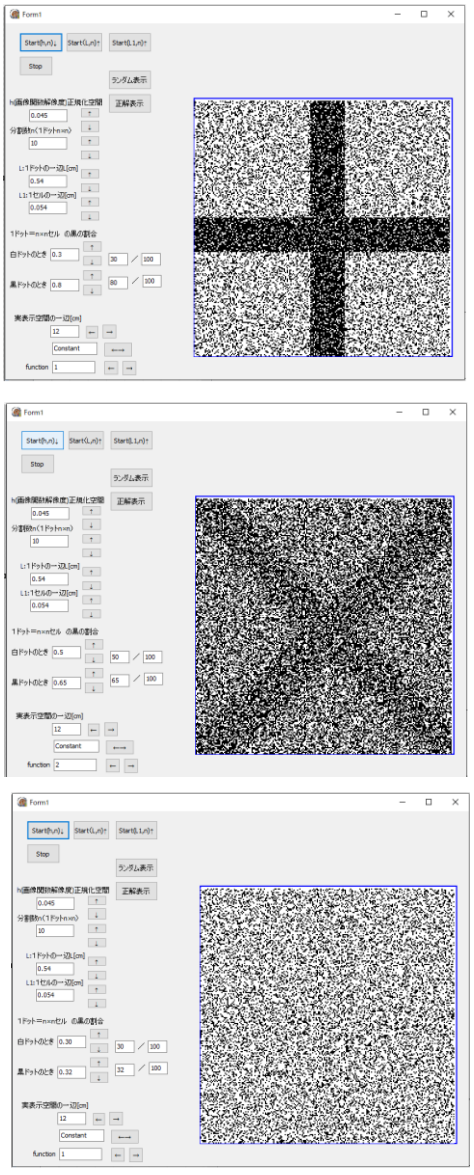
⑤ ディスプレイと被験者の顔（両眼（瞳の中心）の乗る平面）との距離=70[cm]
ディスプレイと両眼の乗る平面は平行とした．

被験者 O が，この条件で，いろいろな(rw,rb)に対し，表示画面に文字をランダムに表示し，それぞれの(rw,rb)で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，rw を大きく，rb を小さくすると，文字が白黒逆転して認識できるようになる．この場合は−5：白黒逆転して明瞭に認識できる←→−1（白黒逆転してほんの少し認識できる）で評価した．

(rw,rb)の値の動かし方は，rw を固定し，rb を 0.01 間

隔で増やしていき，一組の(rw,rb)について上記の 11 段階評価をしていった．これを rw を 0.0～1.0 まで，0.1 刻みで動かし明瞭さを測定した．ただし，評価 5 がいくつか続いた場合はそれ以降の測定は明らかであるから打ち切る方式とした．評価-5 のところも同様である．

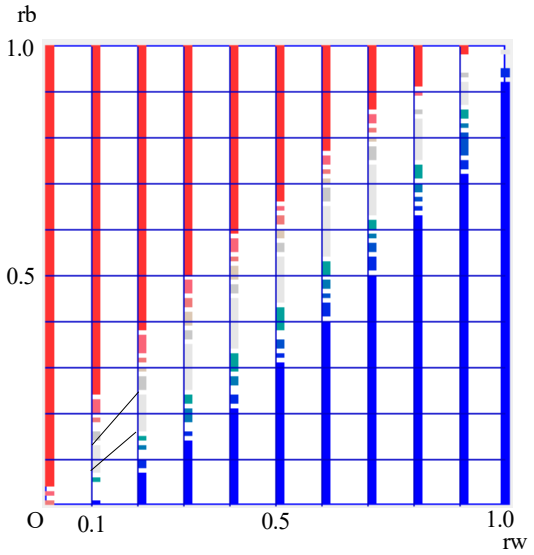
実験画面の例を図 5 に示す．例えば，図 5（上）は評価 5，すなわち明瞭に「＋」が認識できる，図 5（中）で評価 3，すなわち，「×」が十分に認識できる，図 5（下）は評価 0，すなわち全く文字等が認識できない，であった．



（上）文字＝「＋」　rw=0.30,rb=0.80
（中）文字＝「×」　rw=0.50,rb=0.65
（下）文字＝「＋」　rw=0.30,rb=0.32

図 5　実験画面の例

図 6 に測定結果を，図 7 に図 6 の結果を補間したものを示す．補間は，rw を 0.1 間隔で動かしたが測定していない領域を直線近似した．すなわち，例えば rw=0.1 で，評価 0（全く文字等が認識できない）の範囲が rb_0～rb_1 であり，rw=0.2 で評価 0 の範囲が rb_0’～rb_1’である場合，rw=0.12 での見え方 0 の領域を $rb_0+0.02\times\frac{rb_0'-rb_0}{0.1}\sim rb_1+0.02\times\frac{rb_1'-rb_1}{0.1}$ 等としたものである（図 6）．



■ : -5（文字が白文字としてよく認識できる）
■ : 0（文字が全く認識できない）
■ : 5（文字が黒文字としてよく認識できる）
rw : 0.1 刻み　rb : 0.01 刻みで測定した

図 6　測定結果

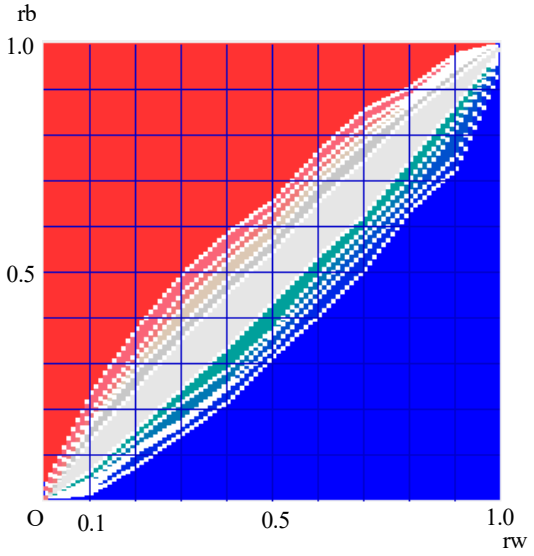


図 7　測定結果（図 6 の結果を補間）

３．測定結果の考察

図 7 を見ると, (rw,rb)=(α,α)　である点は当然ながら, 評価 0（文字等が認識できない）の領域に入っている. この評価 0 の領域はある程度の幅を持っているが，rw, rb が 0 または 1 に近いところでは幅が狭くなっていることがわかる.

以下で，この結果の応用について考えてみる.
この測定では n=10 として，1 ドットを 10×10 に分けるという条件での測定であった.

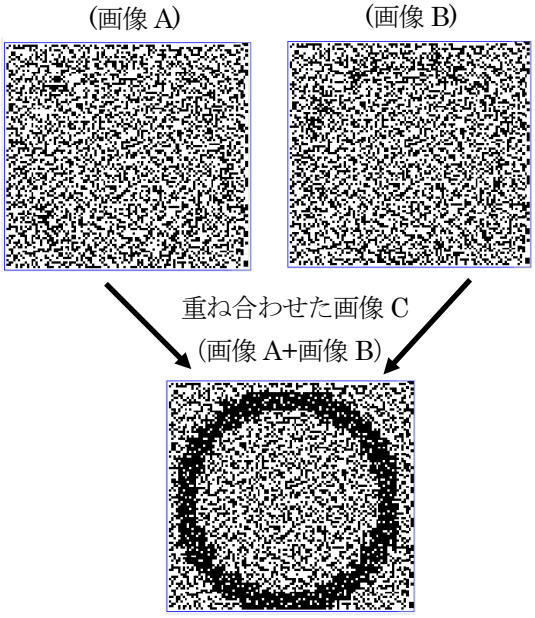
これを n=4，(K,N)＝(2,2)での視覚暗号の設計に利用してみる.

$(rw_C,rb_C)=(\frac{6}{16},\frac{14}{16})=(0.375,0.875)$,

$(rw_A,rb_A)=(rw_B,rb_B)==(0.375,0.4375)$の場合，図 7 で解釈すると,

「重ね合わせた場合十分に文字は認識できるが（点(0.375,0.875)は評価 5 の赤の領域に入っているが)，画像 A,B では，ほんの少し文字が浮かび上がるであろう（点(0.375,0.4375)は，はっきりと評価 0 の領域に入っていない)」, したがって, 暗号システムとしては成り立たないであろう，ということが予測できる.

実際にこの条件で画像 A,B,C を作成したのが図 8 である．確かにおおよそ予測どおりとなっている.



表示画面の一辺＝8.0[cm]
1 ドットの一辺＝0.32[cm]として画像を作成

図 8　$(rw_A,rb_A)=(rw_B,rb_B)=(0.375,0.4375)$,
$(rw_C,rb_C)=(0.375,0.875)$の例

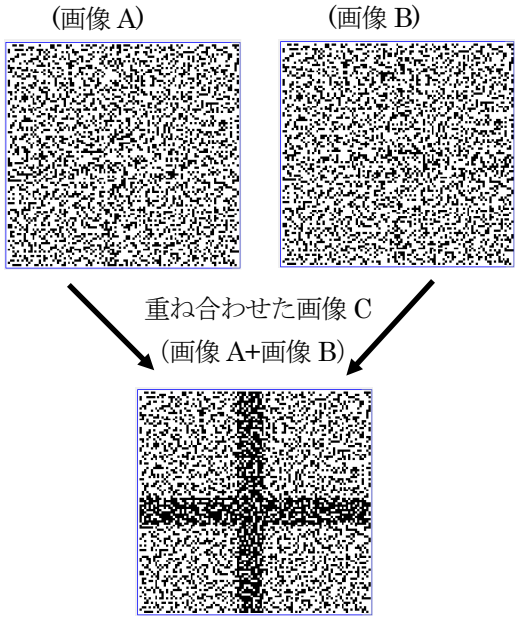
しかし，同様に

$(rw_C,rb_C)=(0.3125,0.6875)=(\frac{5}{16},\frac{11}{16})$,

$(rw_A,rb_A)=(rw_B,rb_B)=(0.3125,0.34375)$

の場合，図 7 で解釈すると,

「重ね合わせた場合十分に文字は認識でき（点(0.3125,0.6875)は評価 5 の赤の領域に入っている)，画像 A,B では文字は認識されない（点(0.3125, 0.34375)は，はっきりと評価 0 の領域に入っている)」, したがって, 暗号システムとして成立する，と予測される.
しかし実際は図 9 のように，画像 A,B に文字「＋」がほんの少し現われている.



表示画面の一辺＝8.0[cm]
1 ドットの一辺＝0.32[cm]として画像を作成

図 9　$(rw_A,rb_A)=(rw_B,rb_B)=(0.3125,0.34375)$,
$(rw_C,rb_C)=(0.3125,0.6875)$の例

これらは，もちろん 2 節で示した①～⑤の測定条件で測定した結果の図 7 を用いての推測であるから，この条件，特に 1 ドットの辺分割数 n や画像～被験者の顔との間の距離等を合わせないことには正確な予想ができないことは当然である.

結論としては，図 7 を用いて，測定条件を合わせれば，かなりの程度暗号システムとしての成立の可否を予測できると考えられる.

４．今後の課題

どのような(rw, rb)で，大雑把な文字「○」「×」「＋」等を区別して認識できるか，認識できないようになるかを，心理物理学的実験により測定した．それは視覚復号型秘密分散暗号システムとして成り立つための条件の推定に使える可能性があることまで考察した．

しかし，精密な推定を行うためにはより多くのデータが必要となる．

今後の課題としては次のことがあげられる．

（１） 様々な条件，特にドット辺分割数 n，画像 - 両眼平面間の距離 d を変化させたときの条件を測定すること

（２） 被験者数を増やし，より多くのデータを求めること

（３） （１）（２）より視覚復号型秘密分散暗号が成り立つ条件をより精密に調べること

文献

[1] 視覚復号型秘密分散法 http://ohta-lab.jp/users/mitsugu/research/VSSS/main.html （2020 年 7 月 6 日現在）

[2] 石原 武，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 http://www.iit.tsukuba.ac.jp/wp-content/uploads/2003/01/Isihara_2002.pdf （2020 年 7 月 6 日現在）