視覚復号型秘密分散暗号の立体視能力を用いた復号
Decryption of Secret Sharing Visual Cryptography with the Ability of Stereoscopic View

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．元情報の認識は人間の視覚的な認知能力によりなされる．

今回新たに，正統的なシートの重ね合わせ復号法の他に，立体視能力により復号が可能であることが分かった．

本研究では，この新たな復号法についてその脳内計算を推定し，実験により，観察者（両眼）－画像間距離と復号像の明確さについて測定した．

キーワード：秘密分散，視覚暗号, (K,N)しきい値法, RDS（ランダムドットステレオグラム），立体視

1.　はじめに

視覚復号型秘密分散暗号（以下では簡単に「視覚暗号」ともよぶこととする[1][2][4][5][7]）は，復号において人間の視覚認知能力を用いる暗号方式の一種である．本論文では，従来の正規の画像の重ね合わせによる復号方法ではなく，新たな第 2 の方法である，立体視能力を用いた復号法（いわば RDS（ランダムドットステレオグラム [3][6][8] ）を見る立体視能力による復号法）について論じる．

以下本論文では，本節で視覚暗号の概略について述べ，第 2 節で「第 2 の立体視能力を用いた復号法」について説明し，そしてこの方法で復号が可能な理由について考察する．第 3 節では，この方法の復号がどの程度明確なものかの実験について報告する．

さて，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，「○」が描かれた元画像に対し，この画像情報をもとに，A と B の

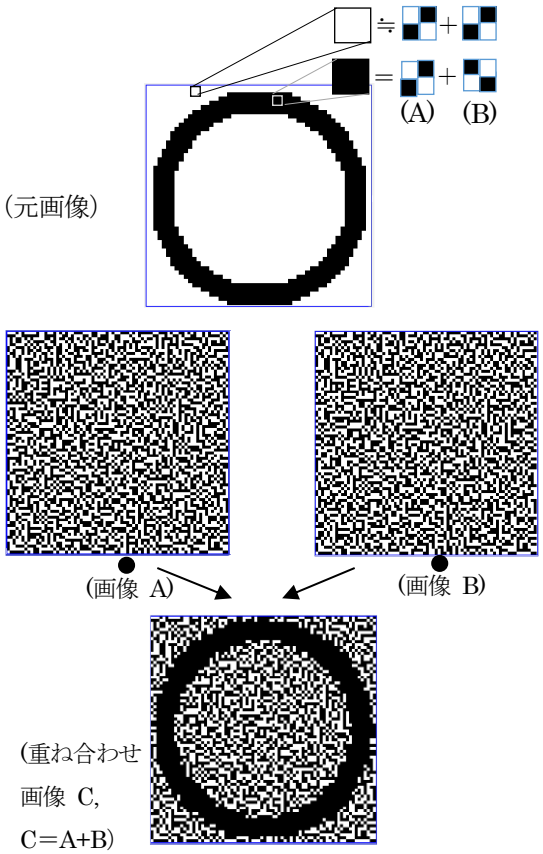


図 1　(2,2)しきい値法の例

N(=2)枚の画像を作成する（作成方式については後述）．画像 A，B は例えば，OHP シート等の透明シートに印刷する．K-1(=1)枚の画像 A，あるいは B だけを見ても何の情報も得られないが，K(=2)枚を重ね合わせると，「○」の情報が視覚的に得られる．

実際に図 1 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．

視覚暗号が提案されてから，この種の暗号方式について様々な数学的研究が行われているが[2][7]，復号に人間の視覚認知能力を使うにもかかわらず，認知科学的な研究はほとんどなされていない．

ここで，(2,2)しきい値法における，画像 A，B への情

報の分割方法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 4 個＝田）への分割を考える. 元画像の 1 ドットが白（□）であれば，2×2 分割領域のうち 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（図 1 右上(A)(B)（上)).

そうすると，画像 C=画像 A＋画像 B（A,B の重ね合わせ : 白＝0，黒=1 としたときの論理和（OR)）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.

一方，黒のドット（■）の場合，その 2×2 の分割領域を，画像 A では，ランダムに 2 つ黒とし，画像 B では，画像 A での白黒を反転したものとする（図 1 右上(A)(B)（下)). 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，ともに元画像で白ドット（□）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 では「○」が視覚的に認知される.

人間の視覚においては，50%黒のドットの領域と 100%黒の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復号されることになる.

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，この方式は，元画像情報を，画像 A，B に暗号化し，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なっている. 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].

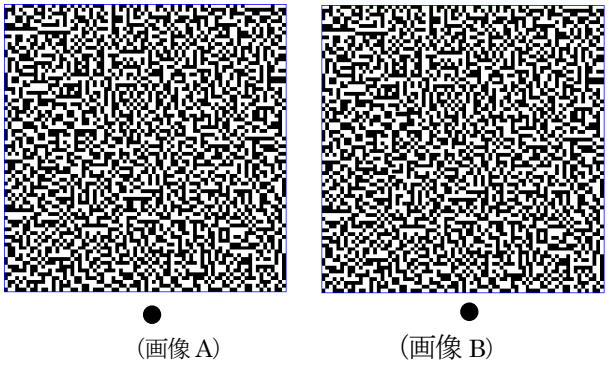


図 2　RDS の例
（視覚暗号ではなく純粋に RDS の例である）

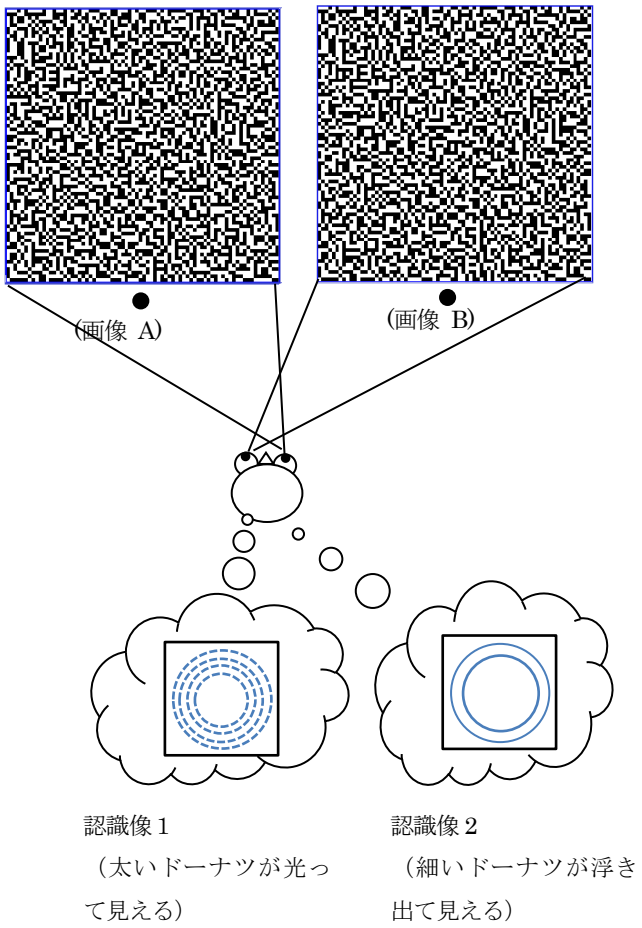


図 3　視覚分散型暗号画像を交差法で見て復号する例（画像は図 1 を拡大したもの）

2.　立体視能力による復号

前節で述べた通り, 視覚暗号の復号は 2 枚の画像（少なくとも片方は透明シートに印刷されたもの）を物理的に重ね合わせることによって行われる.

しかし今回は新たに, 人間の立体視能力, すなわち, RDS（ランダムドットステレオグラム[6][8]）において立体錯視像を認知する能力を用いて，簡単に復号されてしまうことが分かった. これはいわば物理的な重ね合わせでなく, 脳内の重ね合わせによる復号法である. 脳内の重ね合わせでは，白(0)，黒（1）の論理和をとっているわけではない（実際に「○」等の文字の部分は黒色ではない)が，明確に復号される.

まず RDS であるが，RDS では，2 枚の画像 A，B を

用意し，A を左側に B を右側に配置する．A，B をそれぞれ①A を右眼，B を左眼（あるいは②A を左眼，B を右眼）に入力すると，描画されたドットのずれにより奥行き知覚が生じる（図 2）．①は交差法，②は平行法とよばれ，①で手前に浮かび上がって知覚された図形などは，②では逆に奥に知覚される．図 2 を①交差法で両眼視すると中央付近やや左の四角形の領域が浮かび上がって見える．基準（●）が 3 つに見えるよう眼球操作をすると①（②）の状態になり立体錯視現象が生起する．

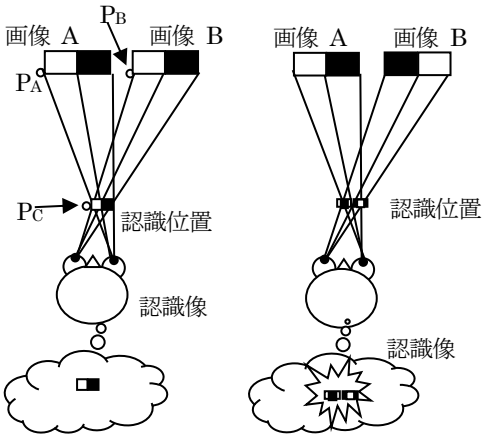
次に立体視能力による視覚暗号の復号であるが，実際に図 1，図 3 の画像 A,B を RDS の要領で立体視すると，RDS の認知像ほど明瞭にではないが，確実に「○」を認知できる．図 1,図 3 は小さいので眼球操作がやや難しいため，付録として，より大きな視覚復号型暗号の画像（今回第 3 節の実験で使用した画像 A,B の縮小版）を示す．RDS の眼球操作にある程度慣れている観察者でなくては復号像が得にくいようではある．

図 1，図 3 を RDS の要領で両眼視（特に交差法の方が見やすいようである）すると暗号化された文字が，RDS ほど明瞭ではないが第 2 の復号法とできる程度に十分文字等が認知されることが確認できる．実際図 3 を交差法で見ると「ちかちかと光ったような○」が観察できることが O,K,A らの複数人の観察者によって確認されている．

このようにして復号が可能になる理由は次のように考えられる（図 4）．元画像の白ドット（□）の場合（図 1）このドット上半分（2 個の小正方形）は図 4 左のような状況になっている（①交差法の状況を想定）．
まず白の領域の左端点について考える．人間の脳内では，この 2 つの白の領域が同一のものであると認識（同一視）され，P_A（画像 A の左端点）と右眼を結ぶ直線と，P_B（画像 B の左端点）と左眼を結ぶ直線の交点にこの左端点がないと「同一」に矛盾するから，白の領域の左端点は P_C の位置に認識される．このような位置認識が各部分で行われ，それを統合し図 4 左のように，白と黒の領域（□■）は実際よりも手前に認識される．

一方，元画像の黒ドット（■）の上半分は暗号化により，画像 A では（□■），画像 B では（■□）となっているため，この範囲の領域の同一視を行うと，白の領域と黒の領域が同一視され，白か黒か曖昧であり全体では「目がちかちかするような感覚」を覚え，少し光ったような領域が認識される．

元画像の白のドットと黒のドットの認識には以上のような違いがあり，全体として，白い領域は明瞭に位置が定まり，文字（「○」）である黒の領域は光った感じに，しかも位置も曖昧に認識される．



（1）元白色ドット　　（2）元黒色ドット
（上から見たところ）

図 4 ドットの同一視と認識像

この違いにより，視覚復号型暗号は，人間の立体視能力により復号されてしまうと考えられる．

なお，RDS 認知能力は，「間違い探し問題」にも応用することができること，間違い探しにおいても「光った感じ」により間違いが見つかるものであることが知られている．これは，この視覚暗号の復号と同種類の現象と思われる．

以上の考察はあくまでも推論であり，より詳しい実験等により確認されるものである．というのも次の現象も今回分かったからである．

視覚復号型暗号の画像 A,B を実際に交差法で見ると，まず前述のように図 3 左のように光った「○」が認識されるが，さらに眼球をそのまま固定していると，○の部分が，少し細（ほそ）くなり浮き出て見えることも観察できる（図 3 右）．このように，2 つの認識像があることは，図 3 左（認識像 1）の状態では距離計算がほとんどなされずにいるのに対し，図 3 右（認識像 2）では，白のドットと黒のドット（あるいは，白と白のドット，黒と黒のドット）を，ある意味無理やり同一視し距離計算を行った結果とも考えられる．認識像 2 の「細くなった文字等が浮き出て認知される現象」についての考察は今後の課題となっている．

3.　立体視能力による復号の明瞭さ

立体視能力を用いた視覚暗号の復号は，どのような条件で可能となるのかについては全く調べられていない．実際に複数の観察者 O, K, A がいくつかの実例で試した感じであるが，各ドット（あるいはドットを分割した白色または黒色の領域）の大きさが小さくなると認知しにくくなるようである．[7]で紹介されている視覚復号型暗号の例は，ドット（白黒の領域）が小さいせいかと思われるが，立体視能力での復号がほとんどできない．

そこで，立体視能力による復号可能な条件を調べる第一歩として，画像と観察者間距離と復号像の明瞭さを計測する実験を行った．同じ大きさのドットであっても，観察する距離が大きくなれば，その網膜像は小さくなるから，この実験によりドットの大きさと復号可能性の関係がある程度明らかになるものと思われる．

今回は実験環境を図 5 のように設計した．まず，コンピュータディスプレイ（または壁）に視覚暗号の画像 A,B を表示（下記 d≧3[m]では、壁に同サイズの印刷物を表示）する．画像 A,B は，ともに一辺 10.0[cm]の正方形とし，画像 A,B は 2.0[cm]の間隔をあけて表示する．

観察者(O：矯正視力 左 1.2 右 1,0 で実験)は，ディスプレイに両眼を平行にして，交差法により復号する．復号できた場合，その復号像（認知像 1,2（図 3 参照））の明瞭さを 5 段階評価し(認識できない場合を 0 とし，見える場合を 1～5 の 5 段階評価)，そのときの両眼の乗る平面からディスプレイの表面までの距離 d[m]をレーザー距離計（精度：1[mm]）により測定する．

表示画像 A,B は，ドットの一辺を 0.27[cm]とし，

（1）　各ドットを 2×2 の 4 分割(ドット内の黒領域，白領域は一辺 0.135[cm]の正方形)

（2）　各ドットを 5×5 の 25 分割（ドット内の黒領域，白領域は一辺 0.054[cm]の正方形)

の 2 つの場合について実験を行った（付録）．

実験結果を図 6 に示す．この結果から次が示唆される．

1．認識像 1 より認識像 2 の方が明瞭に認識される．

2．立体視能力による復号は，画像に比較し，相当の距離があっても可能であるが，距離が遠くなればまたは極端に近くなると復号しにくくなる．
（10[cm]×10[cm]の画像(1 ドット一辺 0.27[cm]）を 5[m]以上離れて見ても復号可能）

3．1 ドットの中の黒領域，白領域が小さくなると復号可能な限界距離は短くなる．

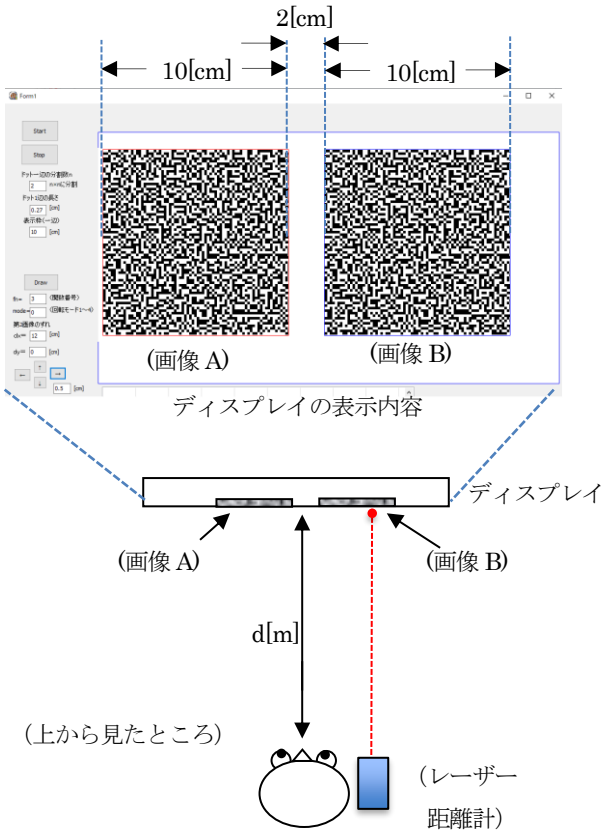
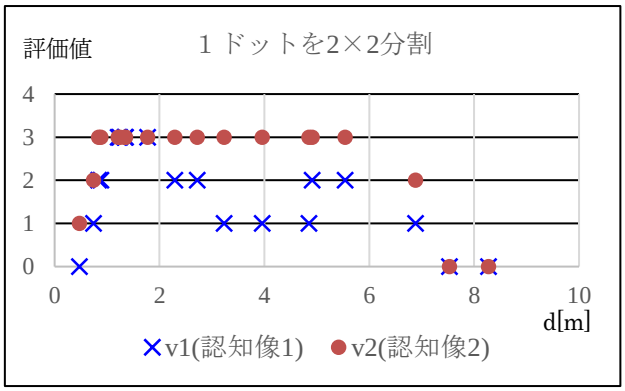


図 5　実験環境



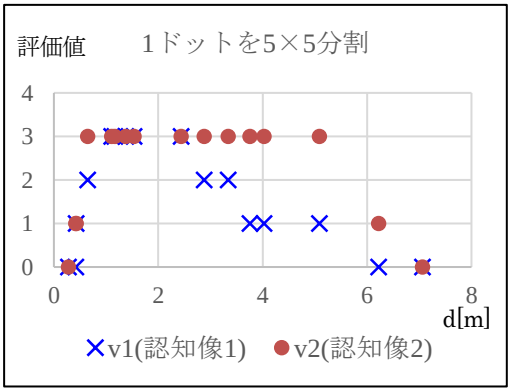


図 6　実験結果

４．結言および今後の課題

視覚復号型暗号（(2,2)しきい値法）の画像を立体視能力（RDS を認知する能力）を用いて復号が可能であることが分かった．これは新たな復号法と考えられる．

復号可能な理由を推定し，心理物理学的実験により，提示画像，観察者間距離と復号像の明瞭さを計測した．

立体視，RDS については膨大な研究がなされているが[3][6]，これらの視覚認知能力を視覚暗号の復号に用いる，という考え方は今のところほとんどない．

一方，視覚暗号の研究は，基本的に，元画像の各ドットを，一般的に $n \times n$ 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，前述のように認知科学的研究はほとんどなされていない．

従来の物理的重ね合わせでなく，脳内の重ね合わせと立体視能力により視覚暗号が復号されることが分かったことで，視覚暗号を認知科学的に研究することの重要性が増したものと思われる．

今後の課題としては

１．復号可能な理由については簡単な推定の域を出ていない．理由をより明確にすること．

２．この復号による認識像には，前述の通り 2 種類あるが，その理由も明らかにすること．

３．より多くの観察者により，よりきめ細かい条件による実験を行い，この復号法の明瞭さを明らかにすること．

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] 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

[3] 内川 恵二，塩川 論：視覚Ⅱ(2007），pp67−157，朝
倉書店

[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

[5] 大槻 正伸， 小泉 康一(2021) “視覚復号型秘密分散山号の新しい２つの復号方法”, 福島高専研究紀要 No. 62 pp1−7

[6] 下条 信輔(1995)：視覚の冒険，pp1−59，産業図書

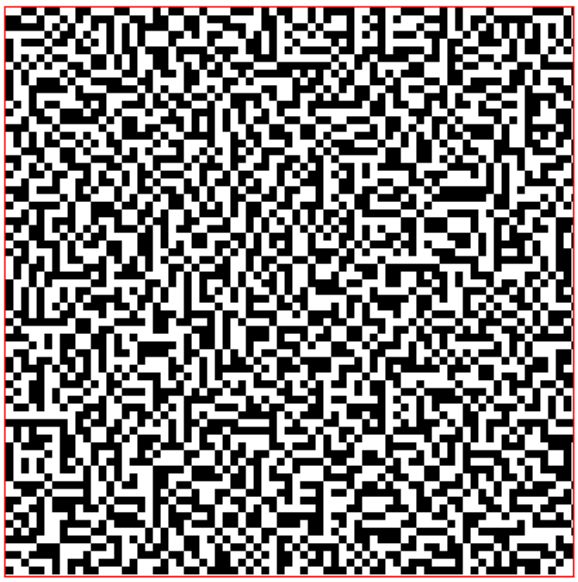
[7] 視覚復号型秘密分散法
http://ohta-lab.jp/users/mitsugu/research/VSSS/main.html
（2022 年 6 月 27 日現在）

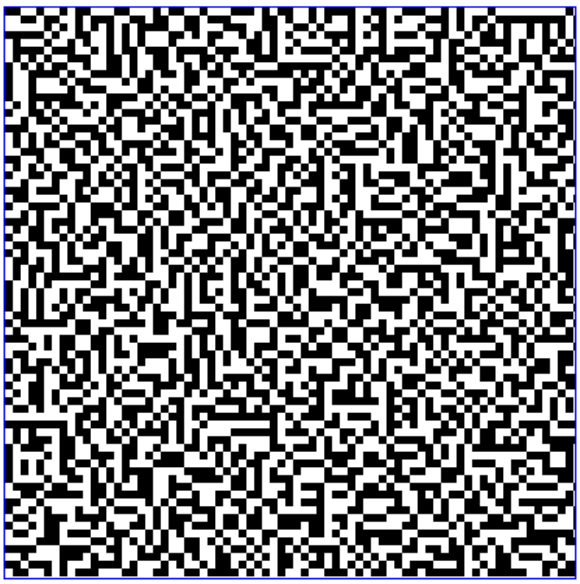
[8]ステレオグラム，－Wikipedia
https://ja.wikipedia.org/wiki/%E3%82%B9%E3%83%86%E3%83%AC%E3%82%AA%E3%82%B0%E3%83%A9%E3%83%A0
（2022 年 6 月 27 日現在）

付録

第 3 節の実験で使用したものと同等の画像.
実験では，これらの画像を 1 辺 10[cm]の大きさとし，
画像 A（左），B（右）の間隔を 2[cm]とした.

【各ドットの分割数＝2×2】





【各ドットの分割数＝5×5】