視覚復号型秘密分散暗号の新しい2つの復号方法

New Two Decryption Methods for Secret Sharing Visual Cryptography

大槻 正伸・小泉 康一
福島工業高等専門学校 電気電子システム工学科
OHTSUKI Masanobu, KOIZUMI Koichi
National Institute of Technology, Fukushima College, Department of Electrical and Electronic System Engineering

（2021年9月1日受理）

Secret sharing visual cryptography is a kind of cryptography using the ability of human's visual sense. Usually decryption is done by overlaying two or more images printed to clear sheets.

It is found that decryption can be done with 2 other methods, that is, with the ability of RDS(Random Dots Stereogram)recognition and with the ability of RDK(Random Dots Kinematogram) recognition.

We introduce these new methods of decryption. And for the method with RDK, we have measured the relation between the clarity of decryption image and gap of displayed two images.

Key words: Secret sharing visual cryptography, RDS, RDK, Apparent movement

1. はじめに

視覚復号型秘密分散暗号[1)3)8)]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、従来の正規の復号方法ではなく、新しく第2の方法（RDS[4) 7)]（ランダムドットステレオグラム）による方法)、第3の方法（RDK[2) 4) 6) 7)]（ランダムドットキネマトグラム）による方法）の2つの復号方法を提案し、2つの方法で復号が可能な理由について考察する。そして第3の復号方法については心理物理学的実験により、どの程度の 2 枚の画像の空間的ずれまで復号可能であるかを調べる。

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 Fig.1 に示す。Fig.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 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等に印刷する。K-1(=1)枚の画像 A、あるいは B だけを見て

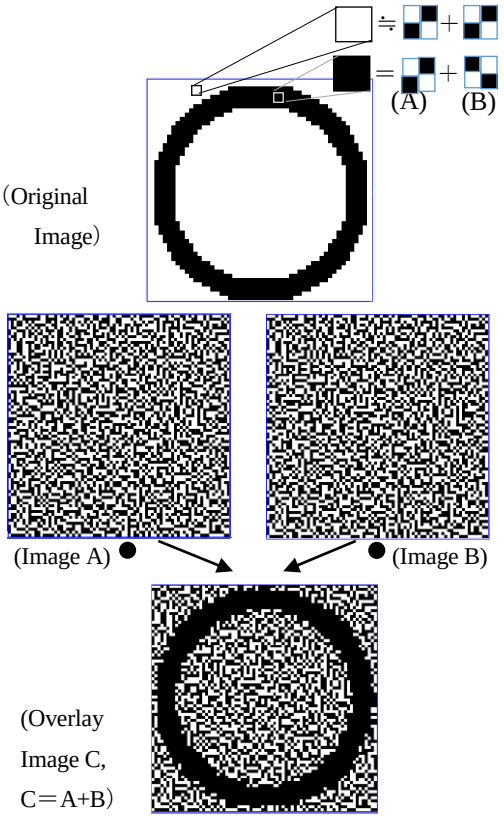


Fig.1 An Example of (2,2)Threshold Cryptography
（(rw_C、rb_C)=(0.5,1.0)）

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 Fig.1 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 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。

視覚復号型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 [3)8)]、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。

Fig.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。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（Fig.1 右上(A)(B)）。

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。

一方、黒のドット（■）の場合、その 2×2 の分割で、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（Fig.1 右上(A)(B)）。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 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。

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、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 を同様に「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。

以上のように、視覚復号型秘密分散暗号は、復号するのに、K 枚（今回の例では 2 枚）の画像の重ね合わせにより、人間の視覚認知能力を用いるところが大きな特徴となっている暗号方式である。

(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復号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文献 5)である。

今回の研究は、「画像 A、画像 B の透明シートへの印刷物の重ね合わせ（正統な復号法）」以外の、視覚認知能力を用いた復号方法について調べるものである。

以下では、そのような復号方法を 2 つ示す。

（1）RDS 認知能力による復号

（立体視の能力を用いての復号：透明シートでなく、白い紙に印刷された画像 A、B から復号できる）

（2）RDK 認知能力による復号

（仮現運動認知能力を用いての復号：ファイル（例えばビットマップ形式、png 形式等）で与えられた、背景が白い画像 A、B から復号ができる）

立体視 [4)7)]や、仮現運動 [2)4)7)]については膨大な研究がなされているが、「これらの視覚認知能力を視覚復号型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皆無である。そもそも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 $n\times n$ 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。

以下、本論文では、

- 上記（1）RDS による方法については、復号方法および、その推定される復号可能な理由を示し、
- 上記（2）RDK による方法については、復号可能な理由以外にも、やや詳しく心理物理学的実験により復号の明瞭さと 2 枚の画像の配置位置のずれとの関係について調べる。

2. 視覚認知能力の視覚復号型暗号の復号への応用

2.1 RDS 認知能力の復号への応用

RDS（ランダムドットステレオグラム）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 では一部のドットの位置が一致せず左右に少しずれている。

A、B をそれぞれ①右眼、左眼（あるいは②左眼、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（Fig.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。Fig.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。

浮かび上がって認知される中央やや左の四角形を構成するドットは、B では A よりも 1 ドット分ほど右にずらしてあり、ずらした後の空白はランダムに白、黒のドットを埋め込んで構成している。Fig.2 は、2.2 節の RDK にも用いられるため、RDK の確認が容易にできるように付録 2 として Fig.2 を拡大したものを用意した。

以下、①交差法または②平行法で RDS の立体像を認識する能力をここでは「RDS 認知能力」ということにする。

さて、視覚復号型暗号の復号は、前述のように、透明シートに印刷した画像 A、B を重ね合わせて、人間の視覚能力により暗号化した文字等を認識することにより行われる。これを正規の第 1 の復号法とする。

しかし、①（交差法）または、②（平行法）の眼球操作で RDS と同じように両眼視すると復号できてしまうことが今回新たに分かった（文献 8）ではこの復号法は否定されている）。実際に Fig.1 や付録 1 を RDS の要領で両眼視すると暗号化された文字が知覚されることが確認できる。被験者 A と O が通常のステレオグラム [10] を見る要領で､交差法により付録 1 で同じ文字｢×｣ が認知できることを確認した。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。

このようにして復号できてしまう理由は次のように考えられる（Fig.3）。元画像の白ドット（□）の場合（Fig.1）このドット上半分（2 個の小正方形）は Fig.3 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

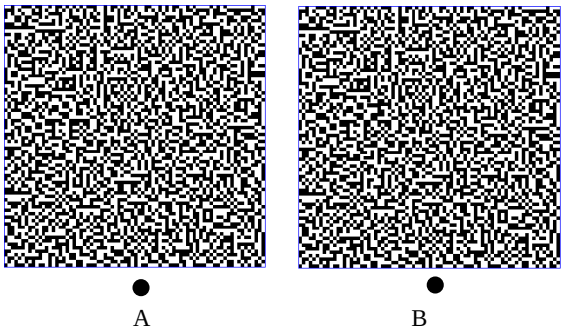


Fig.2 An Example of RDS

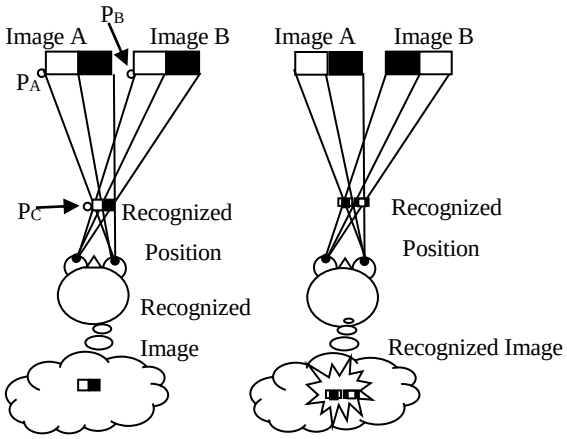


Fig.3 Identification of Dots and Recognized Images

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 Fig.3 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、なんとなく光った領域が認識される。

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、文字等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。

この違いにより、視覚復号型暗号は、人間の RDS 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が知られている。

Fig.4 An Example of Searching Errors Problem
(This example has 3 errors)

間違い探し問題とは、Fig.4 のように、2 枚の画像があり、2 枚はほとんど同じであるが、数か所だけ異なったところがあり、それを探す問題である。この問題の解を素早く見つけ出すのに RDS の場合と同じ眼球操作を利用する方法が知られている。①交差法または②平行法で、左右に並べた 2 つの画像を両眼視すると、異なった個所が光ったような感じで見えるためすぐに異なる個所が認知できるのである。実際に、視覚復号型暗号の RDS 認知能力による復号と、間違い探しの上記方法とではほとんど同じ感覚で一部が光って認識される。

結論として、RDS 認知能力により、間違い探しの場合と同様に、視覚復号型暗号で暗号化した画像 A と画像 B で異なる個所が光っているように、しかもその位置も曖昧に浮かび上がっているように認識されるために復号が可能となるものと考えられる。

前述のように文献 8)では視覚複合型暗号の画像 A,B を RDS の要領で見ても復号されないと述べられているが、文献 8)の例ではドットが小さいため RDS 能力では認知されず、Fig1、付録 1 ではドットがある程度大きいため RDS 能力で復号されると考えられる。ドットの大きさと復号可能性については研究の余地が残っている。

2.2 RDK 認知能力の復号への応用

本節では、第 3 の視覚復号型暗号の復号方法である RDK 認知能力を応用した復号法について述べる。これは仮現運動認知能力による復号法と考えられる。

仮現運動 [2)6)]とは、実際に運動していなくとも、脳内でのみ認知される錯覚された物体の運動のことである。

仮現運動は、例えば、鉄道踏切の左右（上下）交互に点灯する警報機を見ていると赤色光が左右（上下）運動しているように認識される現象や、「パラパラ漫画」[9)]での運動認識等でも体験できることが知られている。RDK は仮現運動認知による錯視の一種である。これは Fig.2 またはそれを拡大した付録 2 を（コンピュータディスプレイ上の）次のように操作で確認される。

（1）画像 B を切り取り画像 A に重ね合わせる。
（2）重ね合わせた画像を自然に見ている状態（この時点では画像 B のみ見える）で画像 B を選択し、
（3）画像 B を（del キーで）削除する（画像 A が見える状態になる）

こうすると、画像 A が提示された状態になるが、実際には RDS で認識される「浮かび上がった四角形領域」が、短時間のみ認識される。この操作は例えば、

・「Windows アクセサリ」の画像処理ソフト Paint を用いて、画像 B を切り取り、A に重ねることでもできるし（Paint による方法）、
・A、B を画像ファイル（例えば　png 形式等）として保存しておき、Word の文書に貼り付けることによってもすぐにできる（Word による方法）

これによって容易に RDK の錯視現象を確認することができる。

RDK で、Fig.2、付録 2 の中央やや左の四角形の領域が短時間認識される理由は以下のとおりと考えられる。

まず、RDS で浮かび上がる図形は画像 A、B で少し位置がずれているため画像 B を見ていて、短時間で画像 A に変わったとき、不動のドット群（四角形の領域以外）と、仮現運動として動くドット群（四角形の領域）を認識した結果と考えられる。

人間には（他の多くの動物も持っていると考えられるが）このように、時間的な離散情報を連続な運動の情報と認識できる能力（錯覚する能力）がある。これを以下では「RDK認知能力」とよぶことにする。

さて、今回新たに、RDK 認知能力が視覚復号型暗号における復号に用いることができることが新たに分かった。実際に、Fig.1 や、付録 1 の 2 つの画像を上記の方法（Paint または Word を用いる方法等）で、短時間ではあるが確実に復号像が得られることが確認できる。

実際約 40 人の集団にスクリーン上でこの操作をして見せたところほぼ全員が同じ文字を認知できた。3 章での実験は Word による方法で行っている。

なおこの現象は両眼視でも単眼視でも生起する。

これは、白の領域のドット群は画像 A、B で位置、色が同一であり、黒の領域（文字等の領域）では、ドットの色が（画像 A では（□■）、画像 B では（■□）と）異なるため、この「色が異なる部分」で黒の物体が動いたように（すなわち仮現運動が）認識されるためと推定される。ここはあくまでも推定であり、正しいかどうかについては今後の研究の余地が残されている。例えば、

・黒ドットのみの移動と認識しているのか、白ドットの移動としても認識しているのか

・左右の移動のみを認識しているのか、上下の移動や斜め方向の移動としては認識していないのか

等々、不明なことが多々あるのが現状である。

そもそも、本当に仮現運動認識によるものかについてもより精密に確認する必要があるが、ここではその仮定のもとで「RDK 認知能力による復号」という言葉を用いる。例えば、透明シートによる本来の第 1 の復号法と同じように「画像 B の消去後はその脳内に一定時間残る B の残像と新たに提示された画像 A を用いて、人間は脳内で第 1 の方法で復号している」という解釈も成り立ちそうではある。しかし、実際に短時間認知される像の文字の部分は、完全に黒一色でなく、半分程度の白もあることから、現在のところ我々は、この復号は RDK 認知能力によるものと推定している。

次章では、本節の「RDK 認知能力によるものと推定される復号」について、その復号像の明瞭さと画像 A、B の提示位置のずれの関係について調べることとする。

3. RDK認知能力による復号の明瞭さと2枚の画像のずれ

RDK認知能力による復号については、今後次のことを調べる必要があると考えられる。

（1）復号に必要な画像Bの消去時間の程度について調べること（紙ベースで、画像Bを抜き取っても復号は難しいことが確認されている。すなわち、どの程度短時間に画像Bを消去する必要があるのか）

（2）復号像は1[s]以内程度で脳内から消え去ることが確認されるが、この復号像の残る時間を精密に測定すること。

（3）教室等でプロジェクタにパソコンの画面を映して、この復号法を試してみたところ、復号像が消えるまでの時間がパソコン画面での復号像よりも明らかに短いことが確認された。この原因を調べること。

すなわち、画像Bが消去される時間や、表示画面の大きさ等と復号像が脳内に残る時間の関係を調べること。

（4）どの程度のドットの大きさの画像までこの復号法が使えるのか調べること、

（5）2枚の画像の重ね合わせに必要とされる精度について調べること。（重ね合わせの精度が甘いと復号像が得られないことが確認されている）

（6）どの程度の(rw_A,rb_A), (rw_A,rb_B),(rw_C,rb_C)において、暗号方式が成り立ち、かつこのRDKによる方法で復号像が得られるのかについて調べること、

等々、不明のことが多々ある。

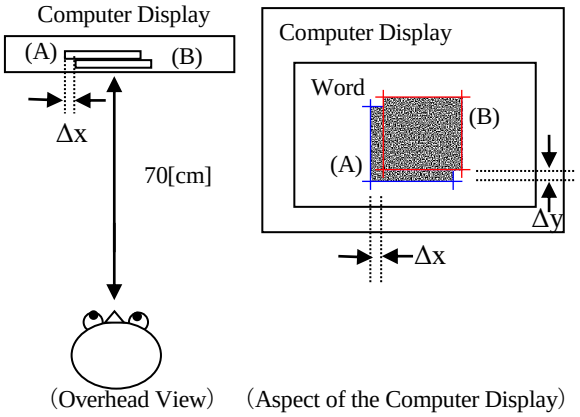


Fig.5　Environment of　the Experiment

上記（1）～（3）はいわば時間的条件について調べることであり、（4）（5）は空間的条件について、（4）（6）は人間の光学的認知能力について調べることといえる。

今回は（5）の、2枚の画像の提示位置のずれと、復号像の明瞭さについて計測した。

ここでは、画像Aに対し、画像Bをずらし、Bを削除した後に復号像がどの程度明瞭に認知できるかを心理物理学的実験により計測した。

実験方法は以下の通りである（Fig.5）。

（＊1）パソコンのディスプレイ（表示部：縦29.9[cm]、横53.8[cm]）上の中央にWordの文書（背景白色の縦20.85[cm]、横32.70[cm]）に付録1の画像A、Bを貼り付ける。

なお、付録1の2枚の画像は縮小してあり、実際はA、Bともディスプレイ上は1辺が10.20[cm]の正方形である。

この実験においては、1ドットはディスプレイ上一辺0.22[㎝]の正方形であり、それを4分割（2×2）して暗号化した画像となっている。

（＊2）画像Aを実験中は固定しておき、固定位置の画像A)対し、画像Bをx軸方向にΔx[cm]、y軸方向にΔy[cm]だけx軸、y軸に平行にずらして配置する。なお、ディスプレイの解像度により、ずらす位置、Δx、 Δyの解像度（一回の↑→↓←キーによる画像Bの移動量）は0.0275[cm]であることが実測から推定された（100回移動の平均値）。

（＊3）ディスプレイ画面から70[cm]離れた位置に、被験者の両眼をディスプレイに平行に位置させ、ディスプレイの画像Bの中心を自然に両眼視する。

（＊4）画像Bをマウスで選択しDeleteキーで削除する。

（＊５）被験者は復号像の明瞭さを5段階評価する（評価値が大きいほど明瞭に復号像が得られたことを示す）。全く復号像が得られない場合は評価0とする。

この実験を、被験者Oが、

Δxは-7×0.0275[cm]～7×0.0275[cm]まで、

Δyは-10×0.0275[cm]～10×0.0275[cm]まで

ともに0.0275[cm]間隔で、21×15＝315点で評価した。結果をFig.6に示す。なお、｜Δx｜≧8×0.0275[cm]のところは明らかに復号像が得られないため、実験を省略し、評価0としてグラフ化してある。この結果からRDK認知能力による復号は、1ドットが一辺0.22[cm]の正方形の場合、±0.1～0.15[cm]程度に正確に2枚の画像を重ね合わせなくては明瞭な復号像が得られないことが分かる。

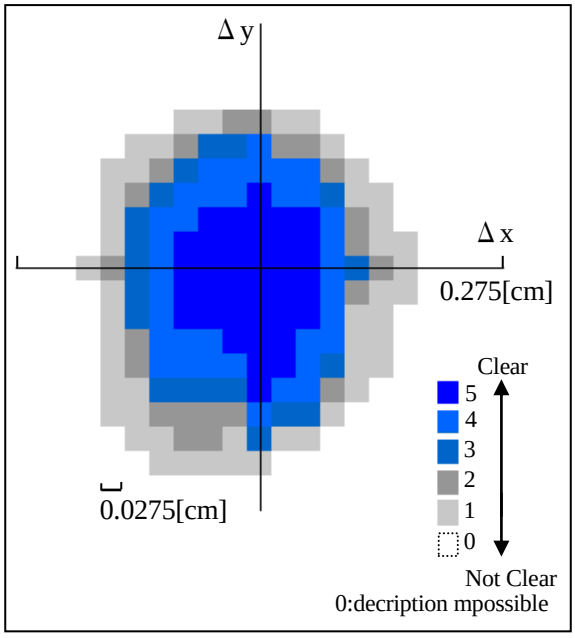


Fig.6　The Result of　the Experiment

4. まとめと今後の課題

視覚復号型暗号において、従来の重ね合わせの復号法以外に、RDS認知能力、RDK認知能力を用いた2つの復号方法を新たに提案した。

今後の課題として、

・3章で述べた（１）～（６）について調べること

・3章（５）の今回の実験をより多くの被験者で行うこと

・RDS、RDK認知能力による復号において、人間が認知する復号像を計算するコンピュータプログラムを設計すること

等があげられる。

参 考 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) 蘆田 宏：動き知覚と動画の認識、映像メディア学会誌Vol.58 pp1151-1156（2004）

3) 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)

4) 内川 恵二、塩川 諭：視覚Ⅱ pp1-20、pp67-157、朝倉書店（2007）

5) 大槻 正伸、小泉 康一：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(2020)

6) 塩入　諭、Patric CavanGh：動きの知覚の二重性、光学第 18 巻第 10 号 pp516-523(1989)

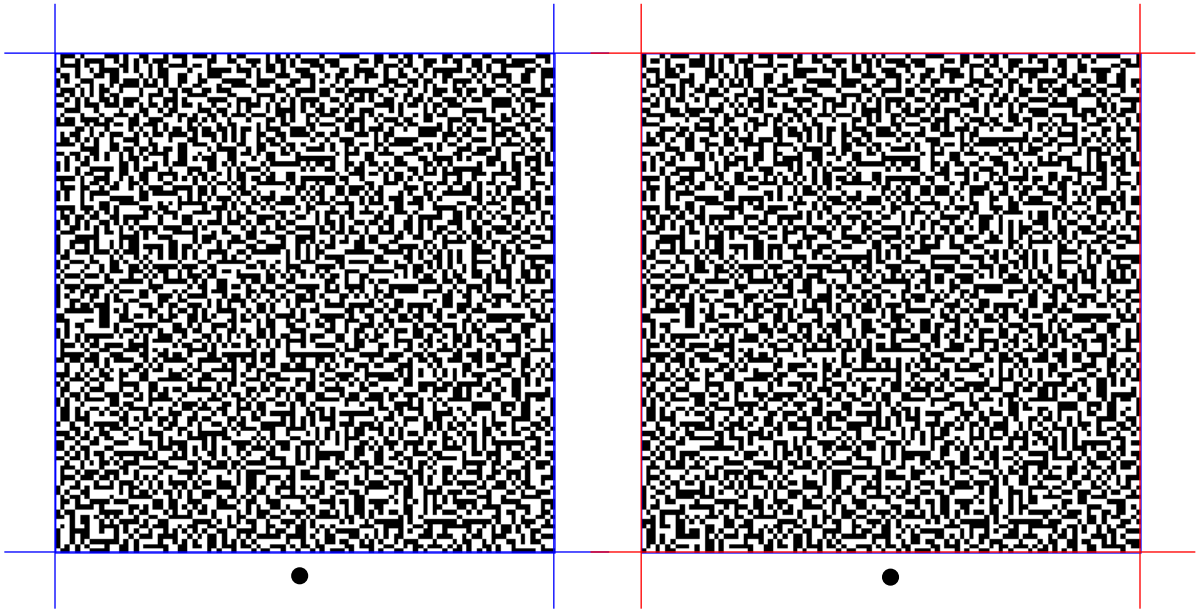
7) 下条　信輔：視覚の冒険、産業図書(1995)

8) 視覚復号型秘密分散法 http://ohta-lab.jp/users/mitsugu/research/VSSS/main.html （2021年9月1日現在）

9) パラパラマンガ - Wikipedia https://ja.wikipedia.org/wiki/%E3%83%91%E3%83%A9%E3%83%91%E3%83%A9%E3%83%9E%E3%83%B3%E3%82%AC （2021年9月1日現在）

10) 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 （2021 年 9 月 1 日現在）

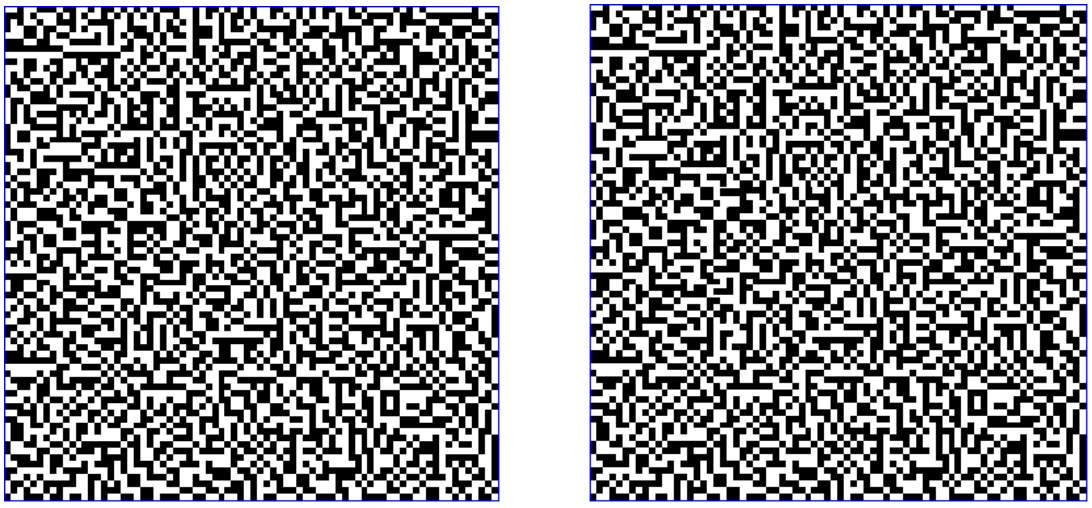
付録１



（A）　　（B）

視覚復号型暗号（「×」の文字を暗号化したもの）
外枠の青色線、赤色線は、ずれΔx、Δyを正確に確認するためのものである。

付録２



（A）　　（B）

RDS、RDK のサンプル（Fig.2 を拡大したもの）