

## 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成25年 5月 1日現在

機関番号：12101

研究種目：基盤研究（C）

研究期間：2010～2012

課題番号：22500003

研究課題名（和文）カラー化された視覚型暗号とカードゲーム

研究課題名（英文）Colored visual cryptography schemes and card games

## 研究代表者

加納 幹雄 (KANO Mikio)

茨城大学・工学部・教授

研究者番号：20099823

研究成果の概要（和文）：視覚型暗号は白と黒の2色のピクセルで構成される秘密画像を暗号化することから始まり、その後カラー化の研究もされているが、コントラストが非常に小さくなっており、実用上は使えない。本研究では赤、緑、黒、白の4色に限定し、さらに赤と緑のサブピクセルが重なると黒くなることを利用して、高コントラストで実現することを目指している。具体的な成果として $(n,2)$ -VCSのカラー化の実現とそのコントラストの最適性を証明した。また、上記の暗号化でもコントラストが低くなることが多い。コントラストを高くするため、セキュリティ条件を弱くした視覚カードゲームについても同様の研究を行った。特に、男のカードと女のカードがあり、男のカードと女のカードを合わせると、秘密画像が出現し、同性のカードを重ねてもランダム模様しかでないカードゲームについて、高いコントラストをもつ構成法を提案した。

研究成果の概要（英文）：A visual cryptography scheme (VCS) was started to encode a secret image comprised of black and white pixels into some shares, and a colored VCS, in which the secret image is comprised of colored pixels, also has been studied. But known constructions of colored VCS lose a lot of contrast in reconstructed images. Therefore we cannot use it practically. In this research, we introduce a new colored VCS, which uses only four colors, black, white, red and green, and propose its construction with high contrast by using the property that a stacking of a red subpixel and a green subpixel results a black subpixel. We provide a construction of such a colored  $(2, n)$ -VCS with highest contrast. Moreover, we propose a new visual 4-colored card games for two parties of boys and girls, respectively, such that each boy and each girl receives a card and when a boy and a girl stack their card together, a secret image is recovered. We propose a construction of this colored game with high contrast.

## 交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2010年度	1,300,000	390,000	1,690,000
2011年度	1,000,000	300,000	1,300,000
2012年度	800,000	240,000	1,040,000
年度			
年度			
総計	3,100,000	930,000	4,030,000

研究分野：総合領域

科研費の分科・細目：情報学・情報学基礎

キーワード：カラー視覚暗号、カラー視覚カードゲーム、離散構造

### 1. 研究開始当初の背景

カラー化された視覚暗号も数多く研究されていたが、コントラストの大きな低下があり、実用的には使えない状況があった。

### 2. 研究の目的

カラー視覚暗号の色を4色、赤、緑、黒、白に限定し、さらに赤と緑の透明紙を重ねると黒になることを利用して、コントラストの高い視覚暗号を構成する。さらに、セキュリティ条件を弱めたカードゲームにおいて、同じ手法を用いて、さらに高いコントラストカラー視覚カードゲームを構成する。また、それらのコントラスト等に理論的証明を与える。

### 3. 研究の方法

いくつかの実装と、離散数学の手法、特にグラフ理論を活用する。また、本研究のカラー化は離散幾何など関連分野にも当てはめて新しい研究問題ができる。

### 4. 研究成果

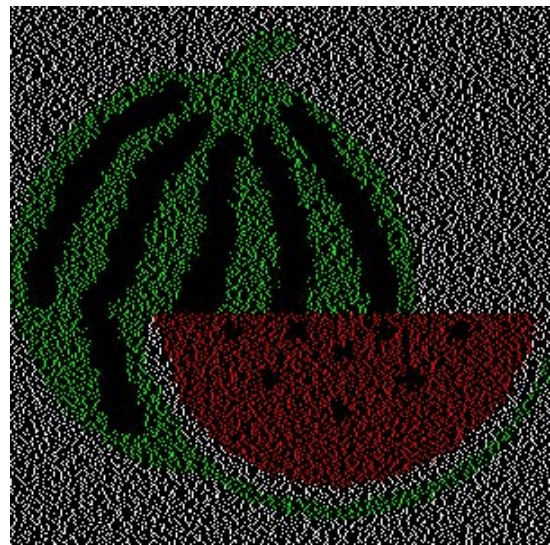
(k, n)-VCS(視覚暗号, Visual Cryptography Scheme)においては、秘密の画像を n 枚のカード(透明な固めのフィルムに印刷したもの)に分散暗号化してランダム模様印刷する。そして、この n 枚のカードの中の k 枚を重ねると元の秘密画像が復元できる。秘密画像は白黒の2色の場合から研究が始まり、その後カラー秘密画像に対しても同様のことができることが理論的に示されている。しかし、コントラストが極端に低下し実用的には使えない。

上で述べたような赤、緑、白、黒の4色に制限した(k, n)-VCSにおいて、コントラストが  $1/(2n-1)$  となる(2, n)-VCSを構成し、このコントラストが最適であることを証明した。また、ピクセル分割数は  $2n-1$  以上となり、これも本構成で最適になっていることを示した。この構成法を実際に実装して、コンピュータ上でカードをつくり、かなりの複雑な秘密画像でも復元できること、さらに4色に色数を制限してもかなりのカラー化になることを確認した。

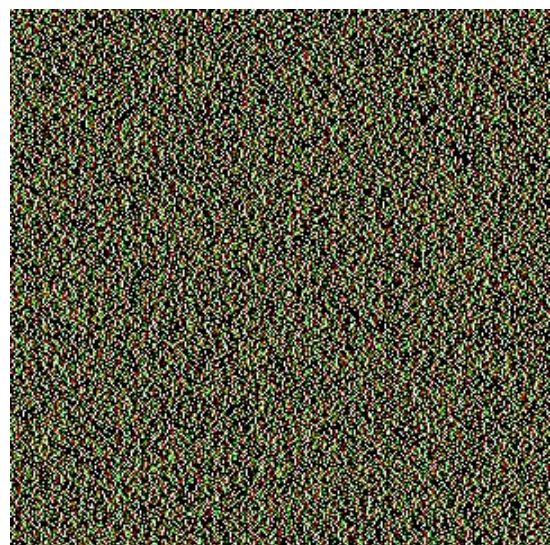
さらにコントラストをあげるために、セキュリティ条件を弱くした視覚カードゲームについても同様の研究を行った。そして次のような結果を得た。任意のグラフに対して、これをアクセス構造とする視覚カードゲームを考えることができるが、ここでは r 人の男と s 人の女がそれぞれカードを1枚ずつもち、男のカードと女のカードを重ねると秘密画像が出現し、同性のカードを重ねてもランダム模様のみである完全2部グラフ  $K(r, s)$  をアクセス構造にする4色視覚カードゲームを主に考えた。そして、 $2 \leq r \leq s$  のとき、コ

ントラスト  $1/(2r)$  でピクセル分割数  $2r$  の構成法を提案した。同時に、ピクセル分割数  $2r$  は最適であることを示した。コントラストについてはいくつかの場合に最適であることを示した。この構成法も実装して、適当な人数であれば使えることを確認した。

本研究を進めるにはグラフ理論とか離散幾何的な手法も必要であり、これらの分野も合わせて研究を行った。特に、グラフ理論の手法、方法、結果には重要なものがいくつかあり、離散幾何にはここでのアイデアを適用できる新しい問題を研究した。



4色の(2, 3)-VCSの3枚のカードの2枚を重ねて復元された秘密画像



4色の(2, 3)-VCSの3枚のカードの内の1枚

## 5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文] (計 12 件)

- ① M. Kano and A. Kyaw, A note on leaf constrained spanning trees in a graph, *Ars Combinatoria*, Vol.108 (2013) 321--326. 査読あり  
<http://www.combinatorialmath.ca/arscombinatoria/>
- ② M. Kano and K. Suzuki, Discrete Geometry on Red and Blue Points in the Plane Lattice, *Thirty Essays on Geometric Graph Theory*, Ed by J. Pach, Springer, (2012) 355-369 査読あり  
DOI 10.1007/978-1-4614-0110-0\_18
- ③ M. Kano and K. Suzuki, Geometric graphs in the plane lattice, XIV Spanish meeting on computational geometry, LNCS 7579 (Springer) (2012) 274-281 査読あり  
<http://www.springer.com/computer/theoretical+computer+science/book/978-3-642-34190-8>
- ④ M. Kano and A. Saito, Star-factors with large components, *Discrete Math.* 312 (2012), 2005-2008. 査読あり  
DOI:10.1016/j.disc.2012.03.017
- ⑤ S. Akbari, M. Ghanbari, M. Kano, M. J. Nikmehr, The Chromatic Index of a Graph Whose Core has Maximum Degree 2, *The Electronic Journal of Combinatorics*, Vol. 19 (2012) P.58 15-pages 査読あり  
<http://www.combinatorics.org/>
- ⑥ M. Kano, A. Kyaw, H. Matsuda, K. Ozeki, A. Saito and T. Yamashita, Spanning trees with a bounded number of leaves in a claw-free graph, *Ars Combinatoria*, Vol. CIII=34, (2012) 137-154 査読あり  
<http://www.combinatorialmath.ca/arscombinatoria/>
- ⑦ S. Bereg and M. Kano, Balanced line for a 3-colored point set in the plane, *The Electronic Journal of Combinatorics*, Vol. 19 (2012) P.33 4-page 査読あり  
<http://www.combinatorics.org/>
- ⑧ M. Uno, Y. Ishibashi and M. Kano, 4-Colored visual cryptography schemes with high contrast, *International Journal of Information Science and Computere Mathematics*, Vol. 4 (2011) 61--77. 査読あり

<http://www.pphmj.com/journals/ijiscm.htm>

- ⑨ M. Kano and H. Kishimoto, Spanning  $k$ -trees of  $n$ -connected graphs, *Graphs and Combinatorics*, Vol. 27 (2011) 413--418. 査読あり  
DOI 10.1007/s00373-011-1021-6
- ⑩ M. Kano and M. Uno, Balanced subdivisions with boundary condition of two sets of points in the plane, *International Journal of Computational Geometry & Applications* Vol. 20 (2010) 527--541. 査読あり  
DOI: 10.1142/S0218195910003426
- ⑪ M. Kano, Y. Wu and Q. Yu, Star-uniform graphs, *Graphs and Combinatorics*, Vol. 26 (2010) 383-394. 査読あり  
DOI 10.1007/s00373-010-0917-x
- ⑫ M. Kano, H. Lu and Q. Yu, Components factors with large components in graphs, *Applied Mathematics Letters*, Vol. 23 (2010), no.4 385-389. 査読あり  
doi:10.1016/j.aml.2009.11.003

[学会発表] (計 18 件)

- ① 加納幹雄, 津垣正男, Yan Guiying, Spanning trees whose stems have bounded degree, 応用数学合同研究集会 2012, 龍谷大学, 2012年 12月 20日~23日
- ② M. Kano, (Invited talk)  $\{a, b\}$ -factors of regular graphs, Thailand-Japan Joint Conference on Computational Geometry and Graphs 2012, 2012/12/ 6-8 Srinakharinwirot University (Bangkok)
- ③ 加納幹雄, グラフの 0 なし一定総和流れ問題, 第24回位相幾何学グラフ理論研究集会, 横浜国立大学 2012年 11月 17日~18日
- ④ 宇野美由紀, 加納幹雄, 4-colored visual card games played on graphs, 離散数学とその応用研究集 2012, 茨城大学, 2012年 8月 9日~8月 11日
- ⑤ Z. Yan and M. Kano, Star-cycle factors of graphs, 離散数学とその応用研究集会 2012, 茨城大学, 2012年 8月 9日~11日
- ⑥ 齊藤明, 加納幹雄, Star-factors with large components, 離散数学とその応用研究集 2012, 茨城大学, 2012年 8月 9日~11日
- ⑦ 加納幹雄, 平面上の 3 色点集合の平衡分割, 第8回組合せ論若手研究集会, 2012年 2月 22日~ 2月 24日 慶應義塾大学 矢上キャンパス
- ⑧ 加納幹雄, (特別講演) グラフの次数因子の新しい問題とグラフの流への応用, 2011年度応用数学合同研究集会, 龍谷

- 大学, 2011年12月15日～17日
- ⑨ 加納幹雄, 平面格子上への3-木の埋め込み, 第23回位相幾何学的グラフ理論研究集会, 2011年11月25, 26日, 横浜国立大学
  - ⑩ 加納幹雄,  $\{r-k, k\}$ -factors of  $r$ -regular graphs, 離散数学とその応用研究集会2011, 奈良県文化会館, 2011年7月31日
  - ⑪ M. Kano (Invited talk), Factors of graphs with big components, The 4th International Symposium on Graph Theory and Combinatorial Algorithms (GTCA2011) Beijing (Academy of Science) 2011, July 8 -July 11
  - ⑫ M. Kano and K. Suzuki, Geometric graphs in the plane lattice with L-line segments, XIV Spanish Meeting on Computational Geometry, Alcala de Henares (Spain), June 27 - 30, 2011
  - ⑬ 宇野美由紀・加納幹雄, 2つのグループのための視覚型カードゲーム, 情報セキュリティ研究会 (ISEC), 2011年3月3日～3月4日
  - ⑭ 加納幹雄, S. Akbari, 5-正則グラフにおける5-フロー, 2010年度応用数学合同研究集会, 龍谷大学, 2010年12月18日
  - ⑮ M. Kano, H. Kishimoto and K. Suzuki. Spanning  $k$ -trees of Bipartite Graphs, The China-Japan Joint Conference on Computational Geometry, Graphs and Applications (CGGA 201, Dalian, Dalian Maritime University ) 2010年11月3日～6日
  - ⑯ M. Uno and M. Kano, Visual card games played on graphs, The China-Japan Joint Conference on Computational Geometry, Graphs and Applications (CGGA 201, Dalian, Dalian Maritime University) 2010年11月3日～6日
  - ⑰ 加納幹雄, 2部グラフの全域 $k$ -木, 離散数学とその応用研究集 2010, 2010年7月30日(金)～8月2日(月) 高知大学朝倉キャンパス
  - ⑱ M. Kano, Spanning  $k$ -trees of  $n$ -connected Graphs and Bipartite Graphs, 8th France Combinatorial Conference, 2010年6月28日-7月2日

[図書] (計1件)

Jin Akiyama and Mikio Kano, Springer社, Factors and Factorizations of Graphs, Springer LNM 2031, (2011) 353 pages

[産業財産権]

○出願状況 (計0件)

名称 :  
 発明者 :  
 権利者 :  
 種類 :  
 番号 :  
 出願年月日 :  
 国内外の別 :

○取得状況 (計0件)

名称 :  
 発明者 :  
 権利者 :  
 種類 :  
 番号 :  
 取得年月日 :  
 国内外の別 :

[その他]

ホームページ等

<http://gorogoro.cis.ibaraki.ac.jp>

## 6. 研究組織

### (1) 研究代表者

加納 幹雄 (KANO MIKIO)  
 茨城大学・工学部・教授  
 研究者番号 : 20099823

### (2) 研究分担者

宇野 美由紀 (UNO MIYUKI)  
 茨城大学・大学教育センター・講師  
 研究者番号 : 90567843