SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

プログレッシブ型視覚暗号に対する安全性評価に関する考察
A study of security analysis of Progressive Visual Cryptography

レ タン タイ ビン * 田中 秀磨 *
Le Thanh Thai Binh Hidema Tanaka

キーワード 視覚暗号、情報理論的評価手法、安全性評価

あらまし

視覚暗号 (Visual Cryptography - VC) は Naor らによって提案された秘密分散 (Secret Sharing-SS) の一種である [3]。VC では秘密情報がデジタル画像に特化されている特徴があり、1 枚の秘密画像から信頼できる第三者であるディーラーにより複数枚のシェア画像に分散される。様々な VC 手法が提案されており、それらに共通の利点は秘密情報を復元するには PC などデジタルデバイスや電力を必要としないことである。VC は現在幅広い範囲で応用が検討され、新しい用途として特に対フィッシング攻撃技術等が注目されている [1]。

プログレッシブ型視覚暗号 (Progressive VC-PVC) は VC の一種であり、復元画像の画質が使用するシェア画像の枚数に依存する特徴がある。PVC は様々な VC 手法の中で、VC の基本的機能を強化させた手法であり、ユーザの利便性を向上しているという点で非常に実用的である。本研究では PVC に焦点を当て、文献 [2] で提案されたアルゴリズムを評価対象とする。これまでの VC に対する評価は主観的な被験者の視覚評価あるいは、一般的には公開されない符号化行列から算出される "*relative difference*" による評価であった。以上のことは、VC の利用においていくつかの問題を生じさせる。

- 客観性のない評価のため、手法同士の効果の比較が公平に実行できない。
- シェア画像の有効性はディーラーの処理を信頼するのみである。
- シェア画像間の公平性の検証をユーザが実行できない。

PVC 対しても同様の評価手法が適用され評価されている。従って、画質向上に関する主観的な視覚評価のみであり、シェア画像のランダム性や復元プロセスにおける情報量の増加など客観性を持つ評価は実施されていない。

本論文では PVC に対する新たな評価手法を提案する。提案手法はシャノン・ハートレーの定理を応用した定量的な手法であり、シェア画像のみを使用するため、ユーザ側から簡単に実行できる特徴がある。また、VC が情報理論的安全性を有すると文献 [3] で示唆されているが、解析手法が明確に示されていなかった。特に random shuffle が理想的と暗に仮定されており、符号化行列における行のハミング重みの偏りや差が与える影響に関する言及がない。本論文では、PVC を対象として具体的な攻撃シナリオに基づいてこれを示すと共に符号化行列の行のハミング重みの偏りが、復元画像の排他的論理和差分において、特徴的な偏りを生じさせる可能性があることを示す。本研究では具体的な PVC の符号化行列に対して、計算機実験により提案手法の評価結果を示すと共に、PVC が計算量的安全性を持つことを考察した。

参考文献

[1] D.James, M.Philip,"A Novel Anti Phishing framework based on Visual Cryptography," 2012 International Conference on Power, Signals, Controls and Computation, pp.1-5.

[2] H.Koga,"A General Formula of the (t, n)-Threshold Visual Secret Sharing Scheme," Advances in Cryptology - ASIACRYPT 2002, pp.328-345.

[3] M.Naor, A.Shamir,"Visual Cryptography," Advances in Cryptology - EUROCRYPT 1994, pp.1-12.

* 神奈川県横須賀市走水 1-10-20 防衛大学校情報工学科 Department of C.S, National Defense Academy, 1-10-20 Hashirimizu, Yokosuka, Kanagawa