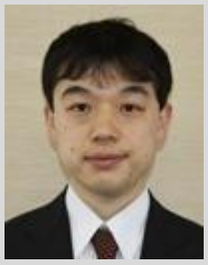
会津大学

複数画像を暗号化できる視覚復号型秘密分散法



上級准教授　渡邊　曜大

概要

秘密分散法とは、「秘密情報」から複数の「分散情報」を生成し、あらかじめ定まった分散情報の集合のみから元の秘密情報が復元できるようにするための暗号技術のことです。例えば、(k,n)閾値型秘密分散法では、秘密情報からn個の分散情報が生成され、k-1個以下の分散情報からは秘密情報に関するいかなる部分情報も漏れない一方、分散情報をk個以上集めると秘密情報が復元できることが保証されています。

秘密分散法には、秘密情報を復元するのに計算機を必要とせず、これを人間自身が行うことができるものが存在します。視覚復号型秘密分散法はこのような秘密分散法の例です。視覚復号型秘密分散法では、秘密情報および分散情報はどちらも画像であり、分散情報は透明なシートに印刷されます。そして、あらかじめ定まったいくつかの分散情報を重ね合わせることによって、人間が自身の目を用いて秘密情報を復元することができます。

従来の複数画像を暗号化できる視覚復号型秘密分散法では、秘密情報を復元できる分散情報の集合（アクセス構造）に制限がありました。本技術ではこの制限を排除し、あらゆるアクセス構造に対応した視覚復号型秘密分散法の構成法を与えます。

実用化の可能性

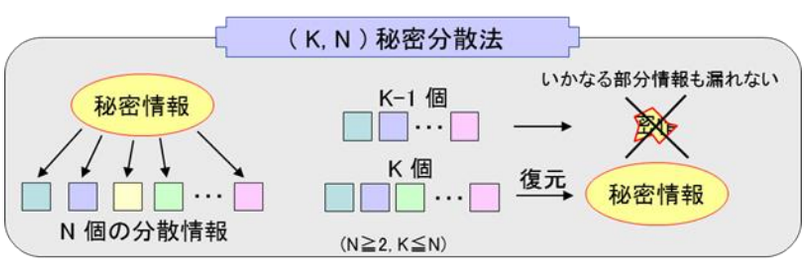
秘密分散法は、秘密情報に対する安全なアクセス制御を実現するための要となる重要な暗号技術です。本技術は、情報量的に安全な秘密分散法であるという本来の特性に基づいて、個人認証における実用化を期待しています。また、利用者の興味を喚起しやすいという特徴に基づいて、娯楽や教育の分野での実用化も期待しています。

UBICからのメッセージ

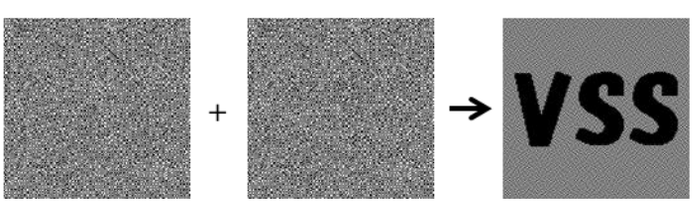
近年、情報処理分野における暗号化に対する要求レベルが高まり、暗号化された情報の解読にも計算機処理が必須となっています。視覚復号型秘密分散法では、情報を物理的に分散させると同時に、人間の目さえあれば解読できる点に特徴があります。そのため、ネットワークやデータベースシステムの脆弱性に起因した情報漏えいなどとは、無縁の世界であるとも言えます。また視覚的にも興味深い振る舞いを見せることから、ゲームやデザインなど、情報セキュリティとは全く異なる世界での利用にも、今後広がっていく可能性があると考えられます。

研究概要図

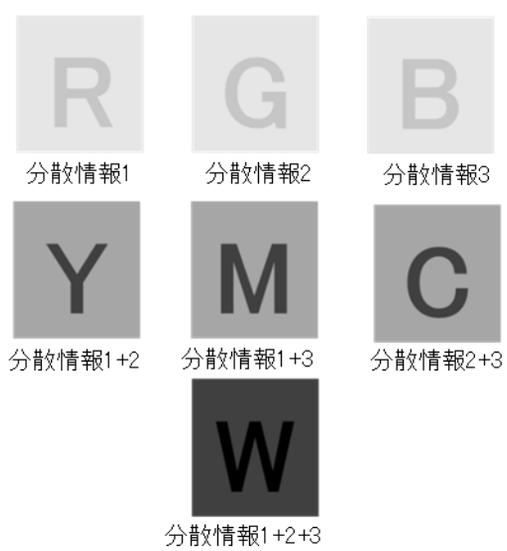
・(k,n)閾値型秘密分散法



・視覚復号型秘密分散法の例



・本技術による視覚復号型秘密分散法の構成例（イメージ）



人の目で解読できる暗号技術の新手法

関連発明：視覚復号型秘密画像分散法、及びこれを実行するプログラム（特願2014－087842）