Research 私の研究

視覚復号型秘密分散法
～人間の“目”を使って計算する暗号～

渡邊 曜大（わたなべ　ようだい）
公立大学法人会津大学
コンピュータサイエンス部門情報基礎論講座
上級准教授

1．はじめに

近年、計算機やネットワークの普及・発展に伴い、さまざまな情報も電子化され、各種電子機器を介して手軽に利用できるようになっています。一方でこうした情報には、国家・企業の機密情報からいわゆる個人情報まで安全に保管されるべき秘密情報も含まれます。ここで漠然と「安全に」という言葉を使いましたが、想定される典型的なリスクとして紛失と漏洩の２つが挙げられます。電子情報は通常、ハードディスクや光学ディスク等の記憶装置・媒体に保管されますが、それら装置・媒体の故障や破損等が原因で情報にアクセスできなくなるのが紛失のリスクです。このリスクを減少させるための単純かつ有効な方法は、秘密情報のコピーを複数用意し、それらを別々にできるだけ相関のない記憶装置・媒体に記録することです。しかしもちろん、情報のコピーが複数存在することは、意図せず情報が流出したり盗まれたりしてしまう漏洩のリスクを増大させることになります。つまるところ、紛失のリスクを減少させるためにはコピーの数は多いほど良く、漏洩のリスクを減少させるためにはコピーの数は少ないほど良いということになります。この相反する２つの要求を同時にみたす安全な情報の保管法を提供するのが、秘密分散法とよばれる暗号技術です。本稿では、これまで学生と共に取り組んできたこの秘密分散法の一風変わった例である視覚復号型秘密分散法の研究について説明したいと思います。

2．秘密分散法

秘密分散法とは、以下の２つの条件をみたすように秘密情報を暗号化して複数の参加者に分配する暗号技術のことです。

(1)　資格を有する参加者集合（有資格集合）は秘密情報を完全に復元できるが、

(2)　資格のない参加者集合（禁止集合）は秘密情報に関するいかなる部分情報も得ることができない。

秘密情報が暗号化され、各参加者に分配される情報のことを分散情報と呼びます。

秘密分散法の典型的な例として、(k,n)-しきい値型の秘密分散法が挙げられます。ここで、k,n は条件 $k \leq n$ をみたす自然数です。この秘密分散法では、n 人の参加者を想定しています。そして、この参加者 n 人のうち k 人以上からなる集合

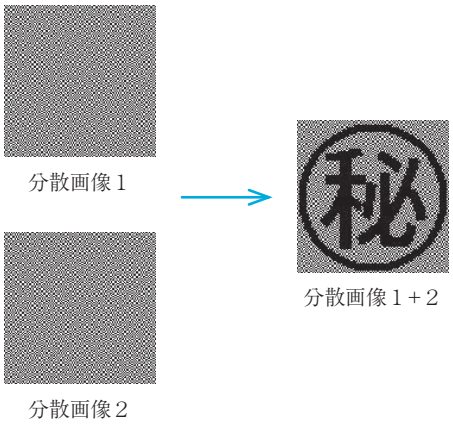

図１　(2,2)−しきい値型視覚復号型秘密分散法

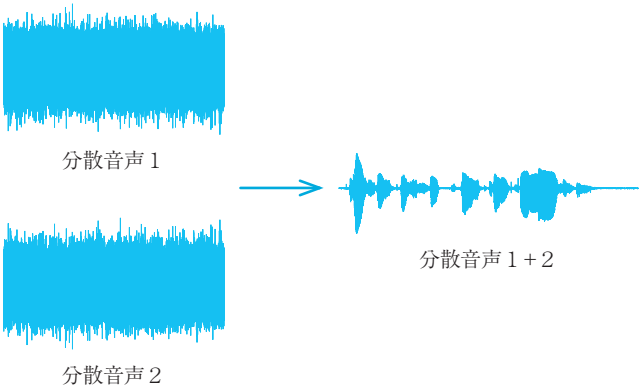

図２　(2,2)−しきい値型聴覚復号型秘密分散法

が有資格集合となり、$k-1$ 人以下からなる集合が禁止集合となります。すなわち、集まった参加者が k 人以上のときは秘密情報を復元できますが、$k-1$ 人以下のときは秘密情報に関するいかなる部分情報も漏れません。したがって、n 人の参加者のうち $n-k$ 人までの分散情報が紛失しても秘密情報の復元が可能であり、また、$k-1$ 人までの分散情報が漏洩しても秘密情報に関するいかなる部分情報も漏れません。(k,n)−しきい値型秘密分散法の具体的な構成法としては、RSA 暗号の発明者の一人でもあるアディ・シャミアによる有限体上の $k-1$ 次多項式を用いる方式が有名です。以上、安全な情報の保管法という観点から秘密分散法について説明してきましたが、この情報の保管というのはいわば副産物で、その直接の目的は、重要な情報に対して誰がアクセスできるのかを定めるアクセス制御の実現にあることを述べておきます。

秘密分散法には、人間の目あるいは耳を使って復号（秘密情報の復元）が可能な一風変わったものも在します。前者を視覚復号型秘密分散法、後者を聴覚復号型秘密分散法とよびます。視覚復号型秘密分散法では、秘密情報（白黒画像）を暗号化して生成された分散情報（分散画像）が透明なシートに印刷され、各参加者に分配されます。復号は参加者が持ち寄った透明なシートに印刷された分散画像を重ね合わせ、現れた画像を人間の目で判別することにより行われます（図１）。一方、聴覚復号型秘密分散法では、分散情報は音声になります。復号は参加者が持ち寄った分散音声を同時再生し、合成された音声を人間の耳で判別することにより行われます（図２）。

３．複数画像を暗号化する視覚復号型秘密分散法

複数の秘密画像を暗号化することのできる視覚復号型秘密分散法について紹介する前に、まず視覚復号型秘密分散法の暗号化の仕組みについて説明します。そのために、最も簡単な例として、$(2,2)$−しきい値型の視覚復号型秘密分散法について考えましょう。この秘密分散法では、秘密画像は２つの分散画像に暗号化されます（図１左）。各分散画像は秘密画像とは相関のない“ノイズ画像”と統計的に区別がつかず、したがって秘密画像に関する一切の情報を漏らしません。一方、透明なシートに印刷されたこれらの分散画像を重ね合わせることによって、秘密画像が復元されます（図１右）。この２つの分散画像の生成法として、秘密画像の１画素を分散画像の２画素に暗号化する最も単純な方法を取り上げることにします。こ

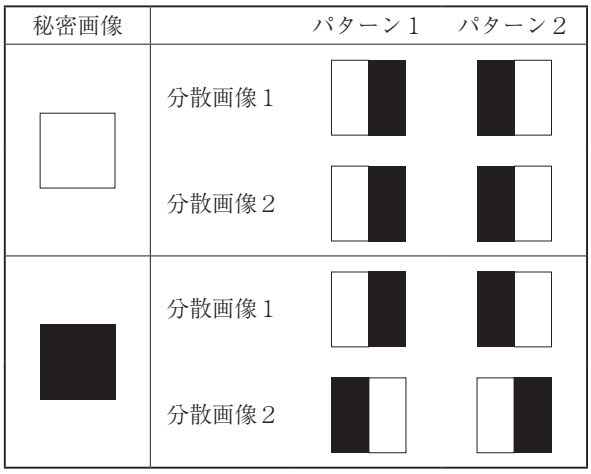

図３　視覚復号型秘密分散法の暗号化

の方法では、秘密画素が白の場合は図３上段のパターン１もしくはパターン２が、黒の場合は同図下段のパターン１もしくはパターン２がランダムに選ばれ、該当する分散画素が分散画像の対応する位置に配置されます。図から分かるように、秘密画素が白の場合（上段）、分散画素を重ね合わせるとパターン1、２のどちらの場合でも白と黒がそれぞれ１つずつで黒の割合が0.5となりますが、秘密画素が黒の場合（下段）、重ね合わせると黒が２つで黒の割合が１となります。この黒の割合の差によって、分散画像を重ね合わせたときに秘密画像が復元されて見えることになります。

これまで扱ってきたしきい値型の秘密分散法では、参加者は皆対等でした。参加者が必ずしも対等とは限らない秘密分散法を扱うためには、アクセス構造という概念を導入すると便利です。ここでアクセス構造とは、(1) 秘密情報を復元できる参加者の組み合わせの集合、および、(2) 秘密情報に関するいかなる情報も得ることができない参加者の組み合わせの集合、により定められます。前者の集合を有資格集合、後者を禁止集合と呼びます。例えば、$(2,3)$-しきい値型の秘密分散法の場合、３人の参加者を a、b、c とあらわせば、その有資格集合は参加者２人以上の組み合わせ

$$\{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}$$

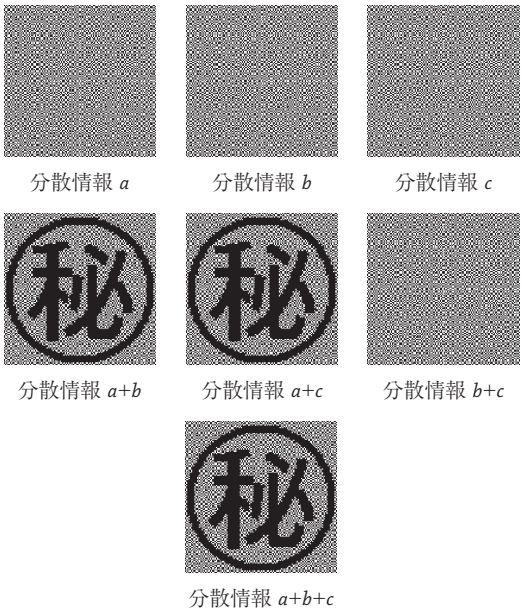

図４　参加者が対等でないアクセス構造を実現する視覚復号型秘密分散法

から成る集合であり、その禁止集合は参加者１人以下の組み合わせ

$$\emptyset,\ \{a\},\ \{b\},\ \{c\}$$

から成る集合（ただし、$\emptyset$ は要素を何も持たない空集合）となります。一方、参加者が対等でない簡単な例として、有資格集合が

$$\{a, b\},\ \{a, c\},\ \{a, b, c\}$$

から成り、禁止集合が

$$\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{b, c\}$$

から成るアクセス構造を考えることができます。実際この場合、参加者 a は他の参加者と組むことによって秘密情報を復元できますが、参加者 b,c のみでは秘密情報を復元できず、参加者 a が参加者 b,c に比べて“偉い”アクセス構造になっていることが分かります。このアクセス構造を実現する視覚復号型秘密分散法は、$(2,2)$-しきい値型の分散情報１を参加者 a に分配し、分散情報２を２つ用意してそれぞれを参加者 b,c に分配することによって簡単に構成することができます（図４）。

最後に、最も一般的なアクセス構造、すなわち、複数の秘密情報をもつアクセス構造を実現する視

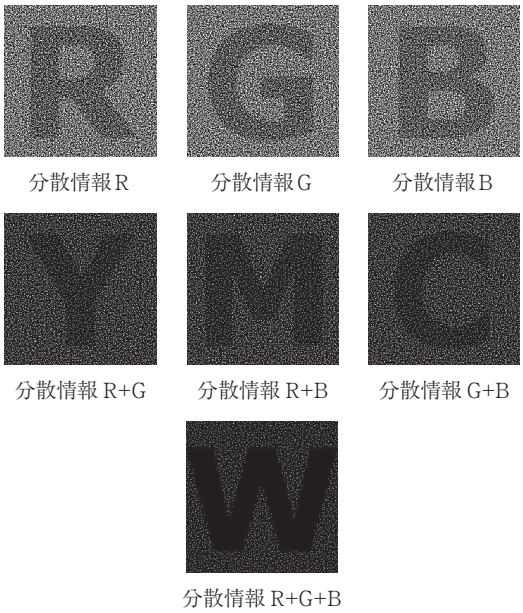

図５　複数の秘密画像を暗号化する視覚復号型秘密分散法

覚復号型秘密分散法について考えましょう。ただし、秘密画像の数だけ各参加者の分散画像を用意すればこれを実現できるのは自明なので、各参加者に配布される分散画像は１つのみという制限を課すことにします。つまり同じ分散画像の組み合わせを変えて重ね合わせるだけで異なる秘密画像が復元されるようにしたいわけです。実は、このような最も一般的なアクセス構造を実現する視覚復号型秘密分散法を構成することは可能で、実際私たちは暗号化関数のみたすべき十分条件を導出することができました。具体的には、各秘密画像に対してそれに対応する暗号化関数が存在して、その各暗号化関数が、(i)対応する秘密画像のアクセス構造を実現する視覚復号型秘密分散法を与え、(ii)他の秘密画像に対応する分散情報の復号に干渉しない、という２つの条件をみたすとき、各暗号化関数により出力された分散画素を連結し、それをランダム置換することによって暗号化関数が構成できることを示しました。

図５は、３人から成る参加者集合の空集合を除くすべての部分集合に秘密画像が付与されている

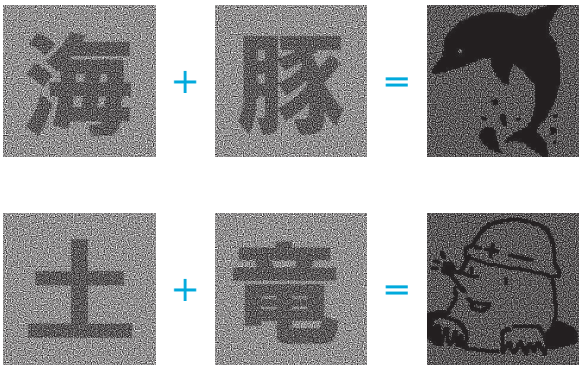

図６　セキュリティ分野以外への応用例：楽しく漢字を学ぶ

視覚復号型秘密分散法の例です。上段は、光の三原色である赤（Red）、緑（Green）、青（Blue）の頭文字を表し、中段・下段は、それらの加法混色

Red ＋ Green ＝ Yellow,
Red ＋ Blue ＝ Magenta,
Green ＋ Blue ＝ Cyan,
Red ＋ Green ＋ Blue ＝ White,

により生成された色の頭文字を表しています。

４．おわりに

これまで強調しませんでしたが、視覚復号型秘密分散法は、あくまで、数学的にその安全性が証明された暗号技術です。しかし同時に、大学のオープンキャンパスや展示会等で年代を問わず来場者の方に興味を持っていただけることも多く、図６のように、セキュリティ分野以外への“意外な”応用も考えられるのではないかと期待しています。

＜プロフィール＞
東京大学大学院理学系研究科修了、博士（理学）。理化学研究所基礎科学特別研究員、会津大学准教授などを経て2016年４月より現職。計算機科学の基礎に関わる分野の研究に従事。日本応用数理学会第３回若手優秀講演賞受賞。