講演番号：4

2 枚の画像を復元する新しい視覚復号型(2,2)秘密分散法

A－7　　(2,2) - Threshold New Visual Secret Sharing Scheme for Two Images

関根 恭平† 野村 亮†
Kyohei Sekine† Ryo Nomura†
†専修大学ネットワーク情報学部
† School of Network and Information , Senshu University

1.はじめに

視覚復号型秘密分散法とは，1994 年に Naor と Shamir によって提案された暗号化技術[1]である．この技術では，秘密とする白黒の画像情報をシェアと呼ばれる暗号化した画像情報に分散して秘密を共有する．このとき作られるシェアの総数を n，秘密情報を復元するために必要なシェアの枚数を k とすると，その視覚復号型秘密分散法は，視覚復号型(k,n)秘密分散法と呼ばれる．これは任意の k 枚以上のシェアによって秘密情報を復元することが可能であるが，k 枚未満のシェアからは秘密画像に関する情報は一切漏れないという性質を持つ暗号技術となる．そのため n-k 枚までのシェアを紛失・破損しても秘密画像を復元することが可能であり，k-1 枚までのシェアが盗まれても情報は漏えいしない．また，この安全性に関する性質は情報理論的にその安全性が証明されている[1]．

視覚復号型(k,n)秘密分散法の原理は，秘密画像の一つのピクセルを複数のピクセルに分割し，それらの分割されたピクセル内の黒の個数が k 枚以上のシェアを重ねると，k 枚未満のシェアを重ねた場合と差が生まれ，そのピクセル全体が相対的に黒く見えるために元の画像が復元されるというものである．復元後に黒ピクセルと白ピクセルを区別するための基準としては相対差が用いられる．

2.複数の画像を復号する視覚復号型秘密分散法

Naor と Shamir に提案された当初の技術では 1 つの視覚復号型秘密分散法が復元できる秘密画像は 1 枚だけであったが，その後の研究で 1 つの視覚復号型秘密分散法から複数の秘密画像を復元することが可能となった．従来研究[2]では同じシェアを m 通りの重ね方をすることで m 枚の秘密画像を保存することができる視覚復号型(2,2)秘密分散法が提案されている．このときの m 通りの重ね方とは，2 枚のシェアが完全一致する重ね方を一通り目，片方のシェアを1ピクセルずらして重ねる方法を二通り目…m ピクセルずらして重ねる方法を m 通り目の重ね方としている．

この技術によって理論上制限なく複数の画像を埋め込むことができる．しかし，2 枚の画像を復元するための相対差は 1/4 となり，実際に作成すると視覚的に認識することが難しい．本研究では，復元する画像を 2 枚に限ることで，相対差が 1/2 となる，従来よりも認識が容易な視覚復号型秘密分散法の作成方法を提案する．

3．提案作成方法

秘密にする 2 枚の秘密画像を SI1，SI2 とし,座標(x,y)の画素の色を SIi(x,y)で表す．作成する 2 枚のシェアを W1,W2 で表し，2 枚の原点を合わせて重ねることで SI1 を復元し，W2 をずらして重ねることで SI2 を復元する．作成するシェアは，復元する秘密画像の 1 つのピクセルを 4 分割したピクセルを 1 画素として割り当てた，図1の 2 つのパターンの組み合わせによって作成する．復元の際には，2 枚のシェアを重ねて 4 分割したサブピクセルのうち 2 マスが黒の場合には白，4 マス全てが黒の場合には黒と判別する．

具体的な作成手順としては，まず W1(1，y)に 2 つのパターンをランダムに並べる．次に SI1(1,y)と W1(1,y)を参照して表 2 の通りに W2(1,y)を決める．その後 SI2(2,y)と W2(1,y)を参照して表 1 の通りに W1(2,y)を決める．この作業を繰り返すことで 2 枚の秘密画像を復元する 2 枚のシェアが完成する．

また，以上によって作成したシェアは，[1]の安全性の基準を満たしていると確認できる．

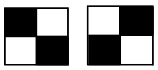

図 1 シェアに用いる 2 つのパターン

表 1 シェア 1 作成の表

W1(x,y)	W2(x-1,y)	W2(x-1,y)
SI2(x,y):白		
SI2(x,y):黒		

表 2 シェア 2 作成の表

W2(x,y)	W1(x,y)	W1(x,y)
SI1(x,y):白		
SI1(x,y):黒		

参考文献

[1] M.Naor and A.Shamir, “Visual Cryptography”, Advance in Cryptography-EUROCRYPT’94, LNCS 950, pp.1-12, Springer-Verlag, 1994.
[2] 坂本 太志,古賀 弘樹, “複数の画像を復元できる視覚復号型(2,2)秘密分散法の提案”, 電子情報通信学会信学技報, IT2007-15, pp.1-6, 2007.