画像割符技術におけるシェア画像の圧縮

熊谷 美津子　　福岡 久雄
松江工業高等専門学校専攻科

1. はじめに

画像割符（VC：Visual Cryptography）は，1994年 Naor 氏と Shamir 氏によって提案された[1]．一般に（k, n）-VSS (Visual Secret Sharing) は，秘密画像を n 枚のシェア画像に分散することでランダムな画像を生成して秘密情報を秘匿する．そして，任意の k（≦n）枚以上のシェア画像を，コンピュータを用いることなく視覚的に重ね合わせ元の秘密画像を復元する．また，n 枚のシェア画像のうちどの k−1 枚を集めても個々のシェア画像から元の秘密画像を類推することはできない．任意の枚数のシェア画像を透明なシートに印刷し，それぞれをユーザに分配して情報を共有することで秘密画像を秘匿する．また，それぞれのシートを重ね合わせることで秘密画像を復元する．

地理的に離れたところに存在するユーザ同士でVC を実施するためには，シェア画像の伝送が必要となる．そのためには，一般的に莫大なサイズとなるシェア画像を圧縮することが重要である．しかし，シェア画像は一見したところランダムに近い画像であることから，従来の圧縮方式での有効性に疑問があり，新たな圧縮方式を検討する余地があると考える．

本稿では，このような新たな圧縮方式を検討するための予備段階として，既存の圧縮方式をシェア画像に適用した実験結果を報告する．

2. 研究目標

本研究では，Rastislav Lukac 氏と konstanions 氏よって提案された（2, 2）-VSS-GS（gray-scale）-8[2]の実装に基づいて，遠隔地間でのシェア画像の伝送方法を検討する．まず，既存の画像圧縮方式をシェア画像に適用することによって，問題点の抽出等を行う．また，シェア画像の性質について詳細な調査を行う．

その結果に基づいて，シェア画像に対して効果を発揮する画像圧縮方式を検討する．

Compression of Shared Images in Visual Cryptography
Mitsuko Kumagai・Matsue College of Technology
Hisao Fukuoka・Matsue College of Technology

3. （2, 2）-VSS-GS-8

（2, 2）-VSS-GS（gray-scale）-8 は 1 枚の秘密画像を 2 枚のシェア画像に分散し秘密情報を秘匿する．そしてその 2 枚のシェア画像を重ね合せることで秘密情報を復元する．（2, 2）-VSS-GS-8 の原理を述べる．本項では，8 bit/pixel 256×256 秘密画像（図 1）を用いる．

3.1. 分散符号化

8 bit/pixel の $K_1 \times K_2$ 秘密画像の各画素 P(i, j)は(1)式で表される．

$$P(i, j)=(p_1(i, j), p_2(i, j), \cdots, p_8(i, j)) \quad (1)$$
但し，$i=1, 2, \cdots, K_1$，$j=1, 2, \cdots, K_2$

p_1 は最上位ビット（MSB），p_8 は最下位ビット(LSB)である．これを，ビットごとに切り出すことで秘密画像を 2 値画像へ分解する．それぞれの切り出されたビットは 2 値の $K_1 \times K_2$ ビットプレーン画像 1～8 を生成する．

図 1. 8bit/pixel 256×256 秘密画像
（65KB：ヘッダ含む）

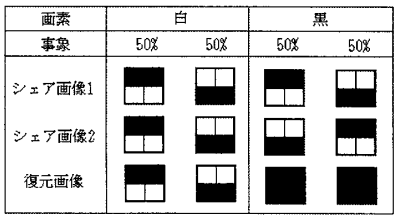


図 2.　2×2 ブロックのパターンと組合せ

ここで，$K_1 \times K_2$ ビットプレーン画像それぞれの各画素 $p_k(i,j)$ (k=1, 2, …, 8) が，白 ($p_k(i,j)=1$)，黒 ($p_k(i,j)=0$) それぞれの場合に，図 2 に示すルールに従って 50%の確率で 2×2 ブロックに置き換える．その結果，（2），（3）式に示す 2 組の $2K_1 \times 2K_2$2 値シェア画像群 s_1^B, s_2^B が生成される．

$$s_1^B=(s_1^1(u, v), s_1^2(u, v), \cdots, s_1^8(u, v)) \quad (2)$$
$$s_2^B=(s_2^1(u, v), s_2^2(u, v), \cdots, s_2^8(u, v)) \quad (3)$$
但し，$u=1, 2, \cdots, 2K_1$，$v=1, 2, \cdots, 2K_2$

そして，2値シェア画像 s_1^B，s_2^B の各ビットプレーンをそれぞれ重畳することにより（4），（5）式に示す $2K_1 \times 2K_2$ 多値シェア画像 S_1，S_2 が生成される（図3-（a），（b））．

$$S_1(u, v) = s_1^1(u, v) \times 2^7 + \cdots + s_1^8(u, v) \times 2^0 \quad (4)$$
$$S_2(u, v) = s_2^1(u, v) \times 2^7 + \cdots + s_2^8(u, v) \times 2^0 \quad (5)$$

ここで，生成された多値シェア画像 S_1，S_2 をユーザに分配することで 8 bit/pixel 秘密画像を 2 つに分散し秘匿する．

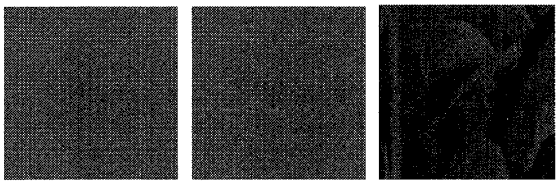
3.2. 秘密画像の復元

多値シェア画像 S_1，S_2 それぞれにビットプレーン分解を適用し 2 値シェア画像群 s_1^B，s_2^B を生成する．ここで，2 値シェア画像群 s_1^B，s_2^B の各画素 $s_1^B(u, v)$，$s_1^B(u, v)$ の互いに対応する画素で論理和を適用し $2K_1 \times 2K_2$ 2 値復元画像 r_B を生成する．（6）式に論理計算を示す．

$$r_B(u, v) = s_1^B(u, v) \vee s_1^B(u, v) \quad (6)$$

そして，復元画像 r_B を重畳することで（7）式に示す $2K_1 \times 2K_2$ 多値復元画像 R を生成して 8 bit/pixel 秘密画像を復元する（図4-(c)）．

$$R(u, v) = r_1(u, v) \times 2^7 + \cdots + r_8(u, v) \times 2^0 \quad (7)$$



(a) (b) (c)

図3．（2，2）-VSS-GS-8

(a) 512×512 多値シェア画像 1（257KB：ヘッダ含む）
(b) 512×512 多値シェア画像 2（257KB：ヘッダ含む）
(c) 512×512 多値復元画像

4. シェア画像の圧縮実験

従来の圧縮方式を用いた，シェア画像の圧縮について述べる．秘密画像の復元にはシェア画像のどの画素情報も欠落してはならない．したがって，非可逆圧縮方式はシェア画像の圧縮には不適切である．そこで，可逆な画像圧縮方式の代表例として PNG を採用し，シェア画像の圧縮実験を行った．

5. PNG 圧縮実験結果

PNG を用いてシェア画像を圧縮した結果について報告する．

画像サイズ（ヘッダ含む）65KB の秘密画像（図1）に（2，2）-VSS-GS-8 を適用し，多値シェア画像 1，2 を生成する．それぞれの画像サイズ（ヘッダ含む）は 257KB である（図3-（a），（b））．

PNG を用いた場合のシェア画像の圧縮率を表 1 に示す．また，実用的ではないが参考までに JPEG をシェア画像に適用した場合の圧縮率も同表に示す．

当然のことながら，非可逆圧縮方式である JPEG の方が優れた圧縮率を示している．しかしここで，シェア画像の PNG と JPEG の圧縮率に着目すれば，PNG と JPEG では，シェア画像の圧縮率は約 50%前後と大差がない．

これは、シェア画像がランダムに近い画像であることに起因すると考えられる．すなわち，ランダムに近い画像はそもそも圧縮に不向きな画像であることから，可逆圧縮方式と非可逆圧縮方式で大きな差が出ないと考えられる．

したがって，PNG 圧縮は，一見するとランダムであるシェア画像に対しても有効な圧縮方式であると推測する．

表 1. 圧縮率比較

	自然画像	多値シェア画像 1	多値シェア画像 2
PNG	86%	58%	58%
(JPEG)	(17%)	(46%)	(46%)

6. おわりに

遠隔地間での VC を実現するためにはネットワークを介したシェア画像の伝送が必要となる。その際に適用するシェア画像の圧縮方式について予備的な検討を行った．

復元画像の劣化を避けるために、シェア画像の圧縮には可逆圧縮方式を用いなければならない．本稿では，可逆圧縮方式の代表例として PNG を用いた場合の実験結果を報告した．その結果、非可逆圧縮方式である JPEG と比べても遜色ない圧縮率が得られることが分かった．

今後，シェア画像の性質を詳細に調査し，シェア画像に適した新たな可逆圧縮方式の検討を進めていく．

参考文献

[1] M.Noar, A.Shamir, "Visual Cryptography," Proc. Eurocrpt1994, Lect.Notes Comput.Sci. vol.950, pp.1-12, (1994).
[2]Rastislav Lukac, konstanions N.Plataniotis "B-bit level based secret sharing for image encryption," PatternRecognition, no.38, pp.767-662, (2005).