

自然画像を用いた視覚復号型秘密分散によるテキストハイディング

宮木 孝^{†1} 塩田 和也^{†2} 吉田 英樹^{†3} 小澤 雅治^{†4} 西垣 正勝^{†5}^{†1} 静岡大学大学院情報学研究科 〒432-8011 浜松市城北 3-5-1^{†2} 静岡大学大学院理工学研究科 〒432-8011 浜松市城北 3-5-1^{†3} 株式会社 NTT データ 〒104-0045 中央区築地 1-4-5 第 37 興和ビル 6 階^{†4} チャンスラボ株式会社 〒104-0061 中央区銀座 7-13-10 日本興亜銀座ビル 8 階^{†5} 静岡大学情報学部 〒432-8011 浜松市城北 3-5-1E-mail: ^{†1} cs1088@s.cs.inf.shizuoka.ac.jp, ^{†2} cs6042@cs.inf.shizuoka.ac.jp, ^{†3} yoshidahdk@nttdata.co.jp
^{†4} ozm@chancelab.jp, ^{†5} nisigaki@inf.shizuoka.ac.jp

あらまし デジタル文書にはコピー&ペーストやプリントアウトなどにより、保護すべき情報が容易に流出してしまうという問題がある。この問題に対する一手法として、著者らは「視覚復号型秘密分散を用いたテキスト型秘密分散方式」を提案している。本方式では、複数のランダムドット画像を高速に切り替えて表示することにより、人間の視覚に秘密のテキスト画像を直接、知覚させることができる。各ランダムドット画像には、テキスト画像に関する情報は一切存在しない。本稿では、この方式を改良し、複数枚の「自然画像」を高速に切替表示することによって、秘密のテキスト画像を復元する方法を示す。さらに、提案方式を実現するためのプロトタイプを実装し、基礎実験から得られた結果について検討する。

キーワード テキストハイディング, 視覚復号型秘密分散, 画像変調, 自然画像

A Text hiding by Visual Secret Sharing with Natural Images

Takashi Miyaki^{†1} Kazuya Shioda^{†2} Hideki Yoshida^{†3}Masaharu Ozawa^{†4} Masakatsu Nishigaki^{†5}^{†1} Graduate School of Informatics, Shizuoka University 3-5-1 Johoku, Hamamatsu-shi, Shizuoka, 432-8011 Japan^{†2} Graduate School of Science and Engineering, Shizuoka University
3-5-1 Johoku, Hamamatsu-shi, Shizuoka, 432-8011 Japan^{†3} NTT Data Corp., Dai-37-koa-biru-6F, 1-4-5 Tsukizi, , Chuo-ku, Tokyo, 104-0045 Japan^{†4} ChanceLab. Corp., Nihon-koa-Ginza-biru-8F, 7-13-10 Ginza, Chuo-ku, Tokyo, 104-0061 Japan^{†5} Faculty of Informatics, Shizuoka University 3-5-1 Johoku, Hamamatsu-shi, Shizuoka, 432-8011 JapanE-mail: ^{†1} cs1088@s.cs.inf.shizuoka.ac.jp, ^{†2} cs6042@cs.inf.shizuoka.ac.jp, ^{†3} yoshidahdk@nttdata.co.jp
^{†4} ozm@chancelab.jp, ^{†5} nisigaki@inf.shizuoka.ac.jp

Abstract The information in a digital document can flow out easily by copy & paste, print out, etc. "Text Secret Sharing Scheme Using Visual Secret Sharing" which have proposed by the authors is a solution to the problem. In this scheme, the secret text image can be perceived by displaying two or more random dot images in rapid succession. In each random dot image, information on the text image doesn't exist at all. This paper improves the scheme so that the secret text image can be perceived with "Natural images" instead of random dot images. In this paper, the prototype system is implemented and a basic experiment is carried out.

Keyword Text hiding, Visual Secret Sharing, Image Modulation, Natural Image

1. はじめに

デジタル文書にはコピーが容易であるという利点がある一方、コピーによるデータの情報価値の希薄化や個人情報のような取り扱いに注意を要するデータの流出などが近年問題になっている。例えば、広告収入により運営されている無料ネットニュースサイトは、アクセス数により収入が決まるため、その記事を読むにはそのサイトにアクセスしなければならないという

仕組みを堅持したい。この場合、記事そのものは無料で公開しているものであるのだが、その記事が複製されて、他のサイトに掲載されることは好ましいことではない。人間が記事を読み上げて人手で文字を再入力することによる複製は防ぎようがないにしても、長文の記事がコピー&ペーストによりとても簡単に複製されてしまうことは大きな問題である。また、デジタルデータそのものの不正コピーによる情報漏えいに匹

敵する問題として認識されているのがプリントアウトによる持ち出しである。紙媒体で出回る情報の管理は、往々にしてデジタルデータ以上に難しい。このように、然るべき場所にて公表されることは問題ないが、許可されていない場所に持ち出されることは禁止したい情報が存在する。

データ量の増加を許容できる場合には、デジタル文書を画像データとして提示すれば、デジタル文書のコピー＆ペーストに対しては対抗することができる。しかし、単に文書を画像化するのみでは、OCRを用いた画像からのテキストデータの抽出や、画像データのプリントアウトによる情報の持ち出しに対する問題が残る。

この要件を満たす方式として、我々は画像変調方式[2][3]と視覚復号型秘密分散法[1]を利用した「視覚型秘密分散を用いたテキスト型秘密分散方式[4](以下、VTSS)」を提案した。

画像変調は画像データの不正コピー防止を目的として開発された技術であり、オリジナル画像から画質の劣化した複数枚の変調画像を生成し、これらの変調画像を高速に切り替えて表示することにより、人間の視覚上でオリジナル画像を動的に知覚させている。画像変調技術によれば PC 内にはオリジナルデータが一切存在せず、文書のコピー＆ペーストおよび画像のプリントアウトの両者にある程度の耐性を持つことが可能である。

視覚復号型秘密分散法(Visual Cryptography または Visual Secret Sharing, 以下 VSS)は、秘密情報を複数枚のトランスペアレントシートに分散して印刷する技術である。トランスペアレントシートのそれぞれには、秘密情報とは全く関係ない画像が印刷されており、 $k-1$ 枚のトランスペアレントシートを使っても秘密情報に関する情報は何も得られないが、 k 枚のトランスペアレントシートを重ね合わせることで秘密情報が浮かび上がる。VSS によればそれぞれの画像から秘密情報が全く漏れないため、テキスト情報を隠すことに適している。

VTSS は、画像の変調に VSS の技術を利用し、画像の復元に画像変調の高速切替表示を利用した方式である。VTSS では、テキスト画像から 2 枚の変調画像を作る。それぞれの変調画像はランダムドット画像になっており、1 枚の変調画像からは元のテキストに関する情報は全く得られない。さらに、それらの変調画像を高速切替表示により、人間の頭の中でテキスト画像を知覚させるため、PC 内のいかなる記憶装置にもテキストの情報が残ることはない。

本稿では、この VTSS の変調画像作成方法を拡張し、変調画像としてランダムドット画像ではなく、自然画

像(に近い画像)を高速に切替表示することによって秘密のテキストを知覚させる方式を提案する。

2. 各既存方式の画像分割方法

2.1. 画像変調方式における画像分割

画像変調方式(文献[2]の輝度変更型変調方式)では、オリジナル画像の各ピクセルに対し以下の作業を行い、1 枚のオリジナル画像から 2 枚の変調画像を作成する。

- (1) オリジナル画像に対し、各ピクセルの階調レベル

(l_0)から輝度レベル(L_0)を計算する。 r は CRT デイスプレイのガンマ値を示す。ここで、「階調レベル」とは PC 内で R, G, B それぞれが 0~255 の整数により指定される色、「輝度レベル」とは現実の色座標における色である。

$$L_0 = l_0^r$$

- (2) 画像の変調を行う。 L_1 , L_2 はそれぞれ変調画像 1 および 2 を構成するピクセルの輝度レベルを示し、 α は変調量を表す。

$$L_1 = L_0 + \alpha, \quad L_2 = L_0 - \alpha$$

- (3) 輝度レベルを階調レベル l_1 , l_2 に戻すことにより変調画像 1 および 2 を得る。

$$l_1 = \sqrt[r]{L_1}, \quad l_2 = \sqrt[r]{L_2}$$

この方法で作られた 2 枚の変調画像をおよそ 100Hz 以上のリフレッシュレートで高速に切り替え表示することにより、人間の知覚的に継時加法混色が起こり、

視覚上でオリジナル画像(L_0)が認識される。画像閲覧時に PC が行うべき処理は変調画像の高速切替表示だけであるため、メモリや VRAM などの記憶装置上にオリジナル画像のデータが復元されることはない。

変調画像に現れる変調の効果は変調量 α の値に応じて異なる。 α の値はピクセルごとに許容範囲がある

(変調画像の各ピクセルの階調レベル l_1, l_2 が 0~255

の範囲に納まらなければならない)が、その範囲内であれば α の値はピクセルごとに独立に選ぶことが可能である。例えば α を(許容範囲内の)乱数にした場合、変調画像はオリジナル画像にノイズが付加された画像として生成される。

2.2. VSS における画像分割

白黒の画像を 2 枚に分割する場合を例に採ると、

VSS[1]では、一つのピクセルが二つのサブピクセルから構成されるものとして考え、次の C_0 と C_1 を用いて画像を分割する。

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}, C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

C_0 と C_1 が表す行列の 0 は白を、1 は黒を表す。オリジナル画像の、任意のピクセルの色が白の場合は、 C_0 のどちらかの行列をランダムに選択して、上の行を用いて一方の分割画像のピクセルを構成し、下の行を用いてもう一方の分割画像のピクセルを構成する。オリジナル画像のピクセルの色が黒の場合は、 C_1 を用いて同様の処理を行う。

VSS では分割された 2 枚の画像はトランスペアレントシートに印刷され、画像復元の際には 2 枚の分割画像が物理的に重ね合わされる。オリジナル画像において色が白のピクセル、すなわち、分割画像において C_0

のいずれかの行要素で構成されているピクセル（二つのサブピクセル）は、2 枚の分割画像が重ね合わされた際に (1,0) または (0,1) となるため灰色に見える。オリジナル画像において色が黒のピクセル、すなわち、 C_1 のいずれかの行要素で構成されているピクセル（二つのサブピクセル）は、分割画像が重ね合わされた際に (1,1) となるため黒に見える。 C_0 と C_1 の行の選択

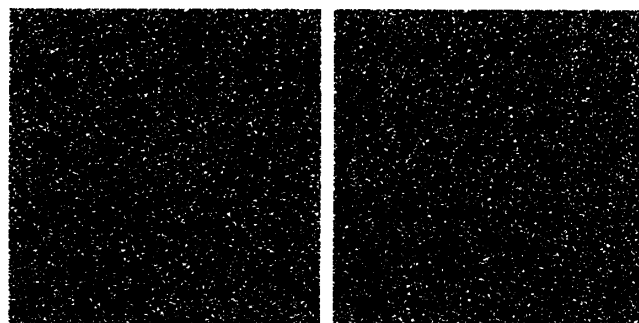
はランダムに行われ、分割画像 1 枚だけでは C_0 と C_1 のどちらを利用しているかわからないため、分割画像からは何の情報も得られない。

2.3. VTSS における画像分割

VTSS[4]では、VSS の考え方を利用して、白地の背景に黒色のテキストが描かれた画像（テキスト画像）から 2 枚の変調画像を生成する。具体的には、テキスト画像の各ピクセルに対し、次の D_0 と D_1 を用いて分割処理を行う。ここで、0 は白を、1 は黒を表す。また、 $\bar{\beta}$ は β の否定（ β が 0 なら $\bar{\beta}$ は 1、 β が 1 なら $\bar{\beta}$ は 0）である。なお、VTSS は VSS のように各ピクセルを二つのサブピクセルで構成する方法を採らないので、 D_0 、 D_1 は 2×1 行例であることに注意されたい。

$$D_0 = \left\{ \begin{bmatrix} \beta \\ \beta \end{bmatrix} \right\}, D_1 = \left\{ \begin{bmatrix} \beta \\ \bar{\beta} \end{bmatrix} \right\}, \beta \in \{0,1\}$$

テキスト画像の背景部分のピクセル（白色）に対しては D_0 の 1 行目を適用して変調画像 1 を作成し、2 行目を適用して変調画像 2 を作成する。テキスト部分のピクセル（黒色）に対しては D_1 を用いて同様の処理を行う。 β の値（0 または 1）はピクセルごとにランダムに選ばれるので、各変調画像はランダムドット画像になる。高速切替表示時には、 D_1 を適用されたピクセルは β と $\bar{\beta}$ の混色によってそのまま β の色（0 ならば白、1 ならば黒）として知覚される。すなわち、全体的にはノイズ画像となる。 D_0 を適用された部分は、 β と $\bar{\beta}$ の混色によってグレー色に知覚される（図 1）。



変調画像 1

変調画像 2

SAMPLE SAMPLE

テキスト画像

高速切替画像(イメージ図)

図 1. VTSS 方式

この方式では、それぞれの変調画像から元のテキストについての情報は全く得られない。しかし、2 枚の変調画像の平均を取るだけでテキスト画像とほぼ同じ画像が復号されてしまうという問題や、すべての変調画像をコピーして、それらを高速切替表示しさえすれば

ば、不正者にもテキスト画像が知覚されてしまうという問題がある。

3. 自然画像を用いた視覚復号型秘密分散によるテキストハイディングの提案

一般にランダムドット画像などの無意味な画像コンテンツがホームページなどに掲載されるようなことはないので、VTSS においては逆に、ホームページなどにランダムドット画像があるということが、不正者に「そこに秘密のテキスト画像が隠されているに違いない」という知識を与えてしまうことになる。そこで本章では、既存の VTSS を改良し、ランダムドット画像ではなく、自然画像を高速に切替表示することによって、秘密のテキスト画像を復元する方法を提案する。本提案方式によれば、一見、何の変哲もない画像の中に秘密のテキストが隠されていることになり、VTSS のステガノグラフィ的な性質を強化することが可能となる。

3.1. 自然画像の高速切替によるグレー画像の復元

VTSS (画像変調方式) では、各ピクセルにおいて 2 枚の変調画像の輝度レベルの平均値が知覚されることになる。よって、変調画像 1 として任意の自然画像 A を選び、変調画像 1 の各ピクセルの輝度レベル L_1 に対して、対応するピクセルの輝度レベルが $L_2 = 255' - L_1$ となるように変調画像 2 を用意してやれば、変調画像 1 (自然画像 A) と変調画像 2 (自然画像の相補的な画像 \bar{A}) 高速切替表示することにより、ユーザに輝度レベルが $255'/2$ (階調レベルが $255/\sqrt{2}$) のグレー画像を知覚させることができる。

しかし、このままでは変調画像 2 が自然画像となっていない。そこで、もう 1 枚の自然画像 B (各ピクセルの輝度レベルを L_2' とする) を用意し、これに対する相補的な画像 \bar{B} (各ピクセルの輝度レベルは $L_1' = 255' - L_2'$ となる) を作成する。そして、画像 A と画像 \bar{B} 、および、画像 \bar{A} と画像 B をそれぞれ図 2 のように市松模様状に貼り合わせることによって、変調画像 1 および 2 を生成することにする。変調画像 1 および 2 は、対応するピクセルが (L_1, L_2) のペア、もし

くは、 (L_1', L_2') のペアになっているため、やはり、高速切替表示によって輝度レベルが $255'/2$ (階調レベルが $255/\sqrt{2}$) のグレー画像として知覚される。

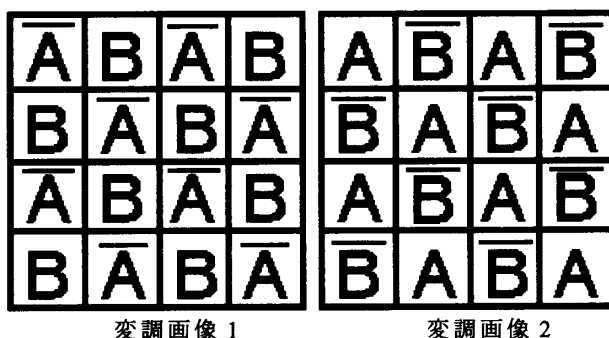


図 2. 市松模様状の張り合せによる変調画像の作成

ただし、それぞれの変調画像における自然画像の領域は半分になる。そこで、本方式を更に発展させ、自然画像を n 枚使って、 n 枚の変調画像を生成することにする。この場合、それぞれの変調画像における各自然画像の領域は $(n-1)/n$ となる。また、理由は後述するが、本方式では、 n 枚の変調画像を高速に切替表示するにあたって、輝度レベルが $255'/n$ (階調レベルが $255/\sqrt{n}$) のグレー画像が知覚されるようにする。

以下に、 $n=3$ の場合を例に、変調画像を生成する方法を説明する。

- (1) 同じサイズ ($M \times N$ ピクセル) の 3 枚の自然画像 A , B , C のそれぞれに対し、各ピクセルの階調レベル (l_0, l_1, l_2) から輝度レベル (L_0, L_1, L_2) を計算する。

$$L_i = l_i' \quad (0 \leq i \leq 2)$$

- (2) 画像のピクセルの座標 (x, y) に対して、

$s = Mx + y$ の変換を行うことによって、ピクセル

に通し番号を与える。 $\text{Mod}(s/3) = 0$ である第 s ピクセルにおいては自然画像 A のピクセルの輝度レベルを L_a 、自然画像 B のピクセルの輝度レベル

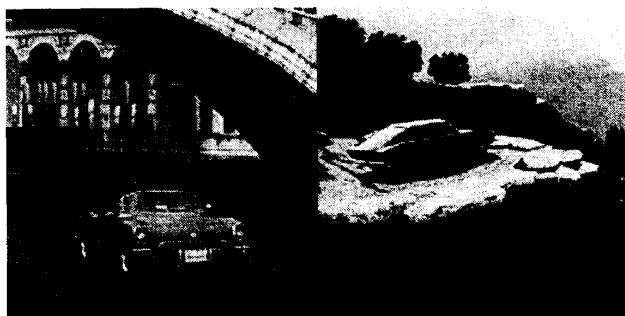
を L_b とする. $Mod(s/3)=1$ である第 s ピクセルにおいては自然画像 B および自然画像 C のピクセルの輝度レベルを, $Mod(s/3)=2$ である第 s ピクセルにおいては自然画像 C および自然画像 A のピクセルの輝度レベルを, それぞれ L_a , L_b とする.

- (3) 変調画像の高速切替表示によって知覚されるグレイ画像の輝度レベルを G とすると, $n=3$ であるので, $G=255^{\gamma}/3$ である. ここで, L_a , L_b に対して, 輝度レベルが

$$L_c = 3G - (L_a + L_b) \quad (1)$$

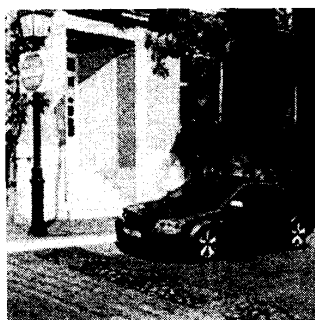
であるピクセル作ってやれば, L_a , L_b , L_c のピクセルの高速切替表示の際に輝度レベルが G のグレイ画像を知覚させることができる.

- (4) ただし, PC 内の色の階調レベルが 0 から 255 までであるので, L_c は 0~255 $^{\gamma}$ の間に収まらなければならない. 式(1)より L_c は $L_a = L_b = 0$ の場合に 255 $^{\gamma}$ となるため, L_a , L_b がいかに暗い色であっても L_c の階調レベルが 255 を超えることはない.

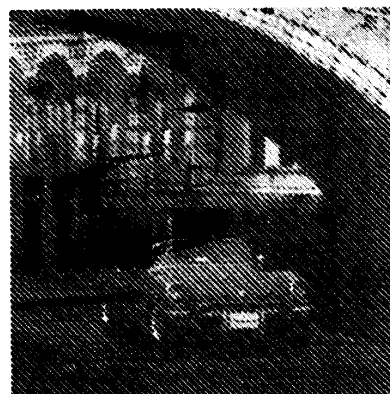


自然画像 A

自然画像 B



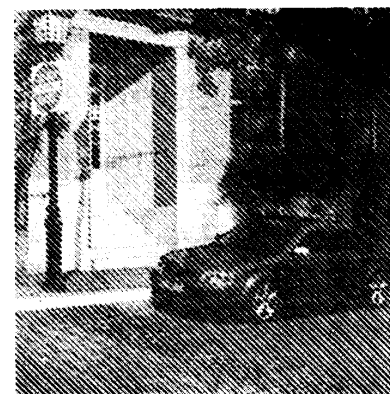
自然画像 C



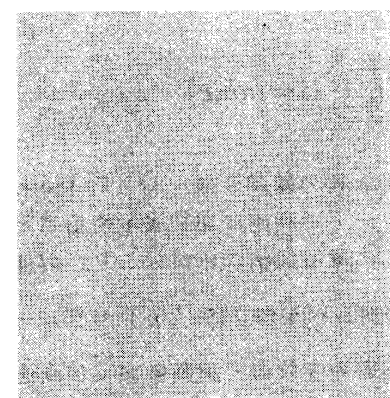
変調画像 1



変調画像 2



変調画像 3



高速切替表示画像

図 3. グレイ画像を復元する変調画像の例

これが、本方式では「 n 枚の変調画像を高速に切替表示するにあたって、輝度レベルが $255^r/n$ のグレー画像が知覚される」ようにする理由である。

一方、 L_a , L_b が明るい色である場合には L_c が 0 よりも小さくなってしまふことがあり得る。

- (5) $L_c \geq 0$ が成立していない場合、以下の処理により

L_a または L_b を調整することにより $L_c=0$ を補償する。なお、ここでは $L_a \leq L_b$ であるとして説明する。

$$d = L_a + L_b - 3G$$

$$\text{If } d \leq L_b - L_a \text{ then } L_b = L_b - d$$

$$\text{else } \begin{aligned} L_b &= L_b - d + (L_a - (L_b - d))/2 \\ L_a &= L_a - (L_a - (L_b - d))/2 \end{aligned}$$

- (6) $\text{Mod}(s/3) = 0$ である場合には、自然画像 C の第

s ピクセルの輝度レベルを L_c に置き換える。自然

画像 A および自然画像 B の第 s ピクセルの輝度レベルは L_a , L_b のままである。 $\text{Mod}(s/3) = 1$ であ

る場合には自然画像 A の、 $\text{Mod}(s/3) = 2$ である

場合には自然画像 B の第 s ピクセルの輝度レベル

を L_c に置き換える。この操作によって、自然画像

A, B, C がそれぞれ変調画像 A, B, C に変わる。

- (7) 変調画像の輝度レベルから階調レベル l_a , l_b , l_c

を計算する。

$$l_i = \sqrt[r]{L_i} \quad (i = a, b, c)$$

この方法で作られた 3 枚の変調画像をおよそ 150Hz 以上のリフレッシュレートで高速に切替表示することにより、人間の知覚的に継時加法混色が起こり、輝度レベルが $255^r/3$ (階調レベルが $255/\sqrt[r]{n}$) のグレー画像が視覚される。実際の 3 枚の変調画像および高速切替表示画像の例を図 3 に示す (高速切替表示画像はイメージ図)。

3.2. 自然画像の高速切替によるテキスト画像の復元

2.3 節で説明した 2 枚の変調画像による VTSS におい

ては、 $\beta = 0$ のピクセルの輝度レベルを u^r , $\beta = 1$ の

ピクセルの輝度レベルを v^r とするという応用が可能

である。この場合、変調画像の高速切替表示によって、

輝度レベルが $(u^r - v^r)/2$ のグレー画像の上に、輝度

レベルが u^r または v^r のピクセルからなるランダムド

ット画像状の文字が知覚されることになる。また、これを 3 枚の変調画像を用いて行うことも可能である。

そこで本稿では、3.1 節の方法で作成した変調画像に VTSS の変調を重畳するというアプローチで、自然画像の高速切替表示による秘密テキストの復元を実現することを試みる。変調方法は以下のとおりである。

なお、ここで D は $u^r - v^r$ である。

- (1) まずは、後ほどテキスト画像の変調を重畳することを見越して

$$G = (255^r - 3D)/3$$

$$l_i = \sqrt[r]{l_i^r \times ((255^r - 3D)/255^r)} \quad (0 \leq i \leq 2)$$

とした上で、3.1 節の手順(1)~(5)によって、3 枚の

変調画像の各ピクセルの輝度レベル L_a , L_b , L_c

を計算する。

- (2) L_a , L_b , L_c に対して、次の E_0 , E_1 を用いてテキスト画像の変調を加える。

$$E_0 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

テキスト画像の背景の領域に含まれるピクセルで

は E_0 からランダムに 1 つの列を選び、テキスト画

像の文字の領域に含まれるピクセルでは E_1 から

ランダムに 1 つの列を選ぶ。選んだ列の値は上か

ら順に L_a , L_b , L_c に対応しており、これらの値

を e_i ($i = a, b, c$) と表すとすると、テキスト画像の

変調を重ねる操作は以下の計算となる．

$$L_i = L_i + 3D \times e_i \quad (i = a, b, c)$$

テキスト画像の背景の領域に含まれるピクセルでは、必ず、 L_a 、 L_b 、 L_c のいずれか1つに3Dが加わるため、 L_a 、 L_b 、 L_c の高速切替表示により知覚される輝度レベルはG+Dとなる．テキスト画像の文字の領域に含まれるピクセルでは、 E_1 の第

1列が選ばれた場合には、 L_a 、 L_b 、 L_c のすべてに3Dが加わるため、 L_a 、 L_b 、 L_c の高速切替表示により知覚される輝度レベルはG+3Dとなる．

E_1 の第2列または第3列が選ばれた場合には、 L_a 、

L_b 、 L_c は不変であるため、 L_a 、 L_b 、 L_c の高速切替表示により知覚される輝度レベルはGとなる．

(3) 3.1節の手順(6)～(7)にしたがって、3枚の変調画像を得る．

この方法で作られた3枚の変調画像をおよそ150Hz以上のリフレッシュレートで高速に切替表示することにより、人間の知覚的に継時加法混色が起こり、「グレー（輝度レベルはG+D）の背景に、ランダムドット（各ピクセルの輝度レベルはGまたはG+3D）で文字が描かれた画像」が知覚される． $D = 0.05 \times 255^{\gamma}$ とした場合の例を図4に示す．

PCが行っている処理は変調画像の高速切替表示だけであるため、テキスト画像を閲覧する際に、メモリやVRAMなどの記憶装置上にテキスト画像のデータが復元されることは無い．さらに、テキスト画像に関する情報は視覚型秘密分散によって3枚の変調画像それぞれにノイズとして加えられているため、各変調画像1枚からテキストに関する情報は全く得られない．

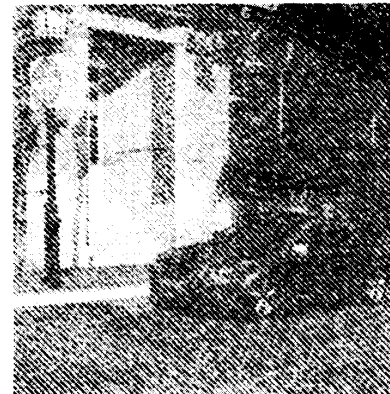
しかし、テキスト画像の変調を重ねることにより、各変調画像の2/3の領域に残存していたそれぞれの自然画像の画質が大きく劣化してしまっている．以下の章では、提案方式の評価に加え、変調画像の劣化の問題の改善について検討する．



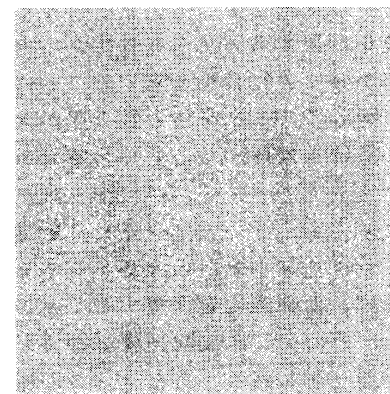
変調画像 1



変調画像 2



変調画像 3



高速切替表示画像

図4. テキスト画像を復元する変調画像の例

4. 提案方式の評価と画質の改善

残念ながら、現時点の方法では、変調画像の品質は自然画像に遠く及ばない。3.1 節の方法により作成された3枚の変調画像（高速切替表示によりグレー画像が知覚される）と3.2 節の方法により作成された3枚の変調画像（高速切替表示によりテキスト画像が知覚される）のそれぞれに対し、もとの自然画像とのDCT係数の差の絶対値の合計を計算した結果を表1に示す。

3.1 節の変調画像における画質の劣化は、自然画像の内の1/3の領域が手順(6)の操作によって置き換えられたことに起因するものであり、3.2 節の変調画像における画質の劣化は、その上にさらにテキスト画像の変調を重ねたことに起因するものである。特に3.2 節の方法による変調画像は見た目にも劣化がひどく、テキスト画像の変調を重ねるという操作が、画質の劣化に大きく影響を与えていることが分かる。

表 1. 自然画像と変調画像の DCT 係数の差

	自然画像 A	自然画像 B	自然画像 C
3.1 節方式	733107	685657	693669
3.2 節方式	1184958	1098746	1030107

3.1 節の方法に起因する変調画像の劣化を改善するには、各変調画像における自然画像の残存領域を増加させる必要がある。単純に考えると、使用する自然画像の枚数 n を増やすことによって、自然画像の残存領域を $(n-1)/n$ にすることができるが、1) 変調画像も n 枚となるため高速切替表示のリフレッシュレートを相当高めなければ継時加法混色が適正に働かない、2) 3.1 節の方法の手順(4)において、 $L_c \geq 0$ が成立しなくなるケースが頻出することになる、などの問題が残る。

3.2 節の方法に起因する変調画像の劣化を改善するには、文字情報の性質を活用する方法が有効であると考えている。文字情報が多くの冗長性を有することはすでに知られており、例えば、1) 文章中の数文字が欠落しても、その文章の意味を理解することが可能であったり、2) ある文字が歪んだり、ノイズが付加されたり、一部が隠されたりしても、その文字を正しく認識することができる。これは、文字または文章が有する冗長性の範囲内であれば、変調画像を変更することが許されることを意味し、その分、各変調画像の画質を向上させることができると思われる。ただし、この結果、知覚されるテキスト画像はそれだけ読みにくくなる。

5. 考察とまとめ

VTSS の変調画像に自然画像を用いる方式を提案し、簡単な実装例を示した。

本方式の最大の利点は、自然画像を高速切替表示することで全く関係ないテキスト画像を視覚的に知覚させることが可能であるという特性である。これは言い換えると、高速切替表示中に切替表示を止めたり、または Printscreen をした瞬間に、それまで表示していた情報（テキスト画像）とは全く関係の無い情報（自然画像）を表示させることが可能になるということである。これにより、例えば、秘密の文章が表示されている画面を printscreen によってコピーしたとしても、文章はコピーできず、その部分が自然画像に置き換わってしまうような応用が考えられる。また、自然画像はランダムドット画像とは違い、ホームページなどに掲載されていても不自然ではないため、画像にステガノグラフィ的な性質を与えることができる。さらに、VTSS の特徴であった各変調画像における秘密分散特性も保たれているため、一枚の変調画像から漏れるテキストに関する情報はゼロである。そして、テキスト画像はユーザは頭の中で知覚されるため、PC 内にもテキスト画像データそのものは存在しない。

本方式の問題点として、以下に挙げるものが考えられる。まず、VTSS 方式と同様に、2 枚の変調画像の平均を取るだけで復号画像とほぼ同じ画像を得ることができるという問題が、本提案方式にもそのまま残っている。また、現段階では、変調画像は完全に自然画像であるとは言い難い。さらに、変調画像を n 枚用いることになるため、ユーザに十分な混色を知覚させるには変調画像を $n \times 50$ Hz 以上の高速度で切り替えなければならない、また、データサイズも増加してしまうという問題がある。

今後、これらの問題を改善する方式について検討していく予定である。

文 献

- [1] M.Naor and A.Shamir, Visual Cryptography, Advances in Cryptology - Eurocrypt '94, pp1-12, 1994.
- [2] 檜川, 塩田, 西垣, 曾我, 田窪, 林部, “輝度値変更方変調方式による画像型デジタルコンテンツの不正コピー防止:復元された画像についての視覚実験,” 情報処理学会研究報告, pp253-258, Feb.2002.
- [3] 塩田, 西垣, 曾我, 田窪, 林部, 中村, “視覚特性を利用した画像型デジタルコンテンツの不正コピー防止:並置加法混色型変調の導入,” DICO2003, pp173-176, Jun.2003.
- [4] 宮木, 塩田, 吉田, 西尾, 西垣, “視覚型秘密分散を用いたテキスト型秘密分散方式の提案,” コンピュータセキュリティシンポジウム 2004, pp.73-pp.78, Oct.2004.