＜報文＞

三重電子透かし画像づくり

青森職業能力開発短期大学校　佐々木隆幸*
千葉職業能力開発短期大学校　川守田　聡

Constructing Triple Digital Watermark image

Takayuki SASAKI, Satoshi KAWAMORITA

要約　これは個人情報画像を、より秘匿に、より安全に、より多く、伝達することを目的とする論文である。「より秘匿に」を実現するために、個人情報画像を離散コサイン変換によって暗号画像に変えている。「より安全に」を実現するために、送り手と受け手の 2 人だけが所有するカギ画像とカギ数値について提案する。2 人だけが所有するカギ画像は、暗号画像を埋め込む土台画像として使用される一方､他方では電子透かし画像から個人情報画像を抽出するときの抽出画像として用いられる。2 人が所有するこのカギ画像は 2 人にとってはカギの役割を果たす画像である。したがって、このカギ画像を所有してない盗聴者は電子透かし画像から個人情報画像を抽出できないので、安全性が高まる。また、カギ数値は暗号画像をカギ画像の中に埋め込むときの割合比であり、カギの役割をする。このカギ数値を知らない盗聴者がカギ画像を所有し得たとしても、盗聴者は暗号画像を正確に抽出することはできない。カギ数値によって安全性はさらに高まる。「より多く」の画像を伝達するために、1 枚のカギ画像の中に 3 枚の個人情報画像を埋め込む方法を提案する。その方法は、空白の画像の赤色、緑色、青色のデータ系列にそれぞれ単色の個人情報画像を書き込み、それをカギ画像の中に埋め込む方法である。

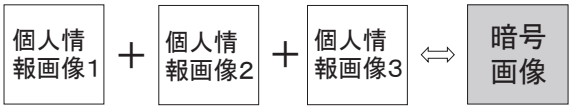
I　はじめに

ディジタル技術の進歩により、医療診断画像のような大きな画像を容易に秘かに伝達[(1)]できるようになってきた。その反面、画像をいとも簡単に盗聴あるいは改ざんすることができるようになり、社会的トラブルを生んでいる。これらの対策として、著作権の多重化透かし[(2)(3)]や秘匿情報の二重化電子透かし[(4)(5)(6)(7)]などがある。しかし、三重の電子透かしに関するものはほとんどみられない。

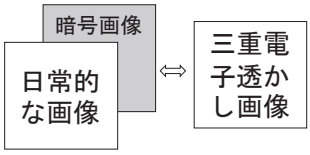
そこで、医療診断画像のような個人情報画像を一度に 3 枚伝達でき､しかも安全に伝達できる方法として、ここに三重電子透かしの制作･再生の方法を提案する。

その提案概要を述べる。図 1(a)に示すように、送り手は､3 枚の個人情報画像を暗号化し､1 枚の暗号画像にまとめる。図 1(b)のように、それを土台となる日常的な画像に埋め込み、1 枚の三重電子透かし画像をつくる。送り手はこの画像を受け手に伝達する。

受け手は、伝達された 1 枚の三重電子透かし画像から、送り手と同じ日常的な画像を差し引くことで、1 枚の暗号画像を抽出し、その画像を復号化して、3 枚の個人情報画像を個々に再生する。



(a)　個人情報画像 3 枚と暗号画像



(b)　暗号画像と日常的な画像と三重電子透かし画像

図 1　三重電子透かし画像の構成

論文受付日　H28. 12. 6

なお、電子透かし画像に埋め込む画像は、著作権侵害防止のための画像ではなく、医療診断画像のような画面全体が秘匿となる画像を想定している。

以降で用いる用語を整理しておく。透かし情報として埋め込む秘匿な個人情報を個人情報画像、その画像を離散コサイン変換した画像を暗号画像、暗号画像を埋め込むための土台となる日常的な画像をカギ画像、暗号画像を埋め込んだカギ画像を電子透かし画像、そして電子透かし画像から再生した個人情報画像を再生画像と呼ぶ。

併せて、電子透かし画像づくりにおける条件を次のように設定する。暗号画像をカギ画像の中に埋め込むときの割合比を1/8とし、これをここではカギ数値といい、βで表す。画像形式はすべて BMP 形式とする。画素数をNと表し、$N = 128$とする。ここで取り扱う画像サイズはすべて128×128とする。画像の伸長や縮小などのスケール変換はないものとする。

Ⅱ　画像伝達の必要性

相手に情報を秘匿に伝えるとき、従来は文字や記号などの言語で伝達することが一般的であった。

しかし、コンピュータおよびその周辺の情報機器の進展により、文字や記号だけでなく、図 2 に示す医療画像や図案画像なども多く取り扱われるようになってきた。加えて、コンピュータ・グラフィックスのような人工的画像も創られるようになった。さらには、データ分析結果を図やグラフなどの画像で表現する場合も多くなってきた。

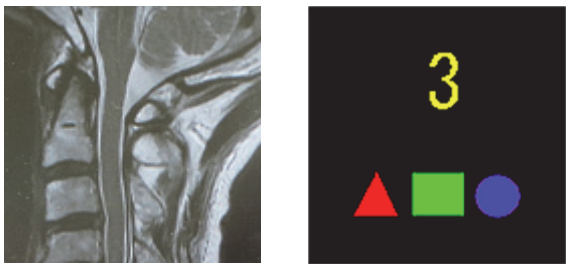


図 2　画像例

このように、相手に画像を直接みせることができるならば、相手は瞬時にそれらの情報を理解することができる。文字や記号などの言語だけでは伝達できない情報も画像ならば、容易に伝えることができるのである。したがって、画像を伝達する意義は大きい。とくに、精確さが求められる医療画像を伝達する場合[8]は、個人情報の観点からも、他人に知られずに、盗聴されずに、画像を精確に届けなければならない。このような事情から、秘匿に、安全に、多くの画像を伝達する機会は今後ますます増加するだろうと考える。

ただし、問題点もある。画像の情報量は文字や記号に比較して膨大であるため、コンピュータや情報機器で画像を取り扱うには、1 つ 1 つの処理時間が長くなる。伝達する場合でも当然に長時間を要する。

したがって、コンピュータやその他の情報機器の負担を軽減するには、画像の情報量を圧縮する必要がある。圧縮に関する技術開発も盛んに行われている。

画像圧縮において、有歪の圧縮の方が無歪の圧縮よりサイズを小さくできるが、医療画像を有歪で圧縮するのは適切でない。このような観点から、この論文では個人情報画像がもつ情報量すべてを伝達することを優先し、画像圧縮は必要に応じて行うものとする。

Ⅲ　秘匿のために

1　離散コサイン変換

個人情報画像を秘匿な暗号画像に変換するために、ここでは離散コサイン変換を採用する。なお、ここでは暗号画像は離散コサイン変換した画像で目視的に意味不明な画像を指し、秘匿性は画像全体が一様に平坦化されることを指す。その変換を式(1)に表し、そのグラフ例を図 3 の(a)、(b)、(c)、(d)に示す。

$$\varphi_{ji} = \left\{\cos j\frac{\pi}{2N}(2i+1)\right\} \tag{1}$$

ただし $i, j = 0,1,2,3,\cdots,N-1$とする。

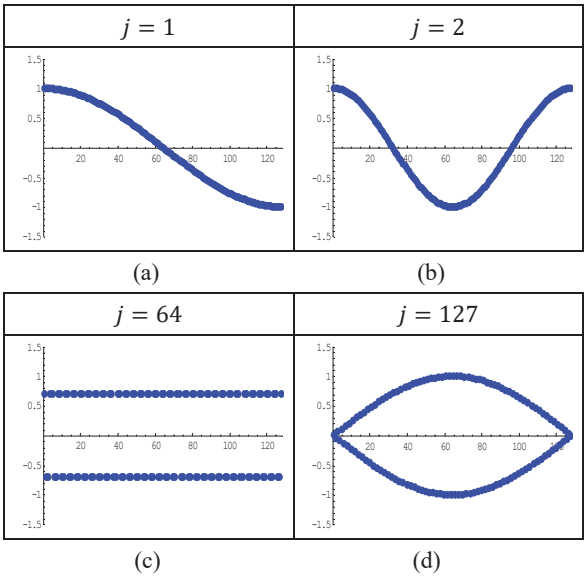


図 3　式(1)のグラフ例

2　離散コサイン変換による暗号化

横×縦の画素数が128×128で、横方向位置i、縦方向位置jの画素値をf_{ji} とする個人情報画像がある。この個人情報画像を、横方向位置m、縦方向位置nの関数値をφ_{nm} とする離散コサイン変換で展開する。そのとき算出される横方向位置m、縦方向位置nにおける展開係数をa_{nm} とすると

$$f_{ji} = \sum_{n=0}^{N-1}\left(\sum_{m=0}^{N-1} a_{nm}\varphi_{mi}\right)\varphi_{nj} \quad (2)$$

$$a_{nm} = \frac{\sum_{j=0}^{N-1}\left(\sum_{i=0}^{N-1} f_{ji}\varphi_{mi}\right)\varphi_{nj}}{\left(\sum_{i=0}^{N-1}\varphi_{mi}\varphi_{mi}\right)\left(\sum_{j=0}^{N-1}\varphi_{nj}\varphi_{nj}\right)} \quad (3)$$

i、j、m、$n = 0$、1、2、…、$N-1$

と表されることが知られている。この展開係数a_{nm}で構成する画像が暗号画像である。

離散コサイン変換による暗号画像の例を示す。図 4 を個人情報画像とすると、その暗号画像は図 5 となる。

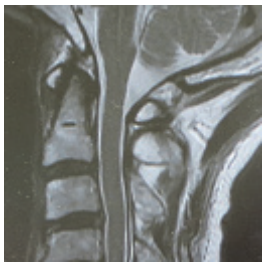


図 4　個人情報画像

図 5　暗号画像

離散コサイン変換によって暗号化された暗号画像には、大きく変化する部分とほとんど変化しない部分があることがわかる。このように変化の激しい画像をカギ画像にそのまま埋め込むと、変化が目立ったままの画像になる。したがって、暗号画像の画面全体を一様で平坦な画像に変える必要がある。

3　個人情報画像のランダム化

一様で平坦な暗号画像につくり変える方法を述べる。その方法は、個人情報画像にランダム系列を乗算し、個人情報画像をランダム化する方法である。

たとえば、個人情報画像の赤色データ系列{R}の k 番目の値を、値の範囲が[0,1]の一様乱数系列randを利用して、式(4)のように書き換える。$rand_k$は k 番目の rand の値とする。

$$R_k = \begin{cases} +R_k & (0.5 \le rand_k \le 1) \\ -R_k & (0 \le rand_k < 0.5) \end{cases} \quad (4)$$

この操作を緑色、青色のデータ系列にも施す。

ランダム系列を二値乱数$\{+1, -1\}$とした理由は、復号化し再生するとき、$|\pm 1|$のように絶対値処理すると元の値に容易に戻すことができるからである。

ランダム系列を乗算した個人情報画像とその暗号画像を示す。図 4 の個人情報画像にランダム系列を乗算した画像(以降ではランダム化画像と呼ぶ)が図 6 である。そのランダム化画像を離散コサイン変換で暗号化した暗号画像が図 7 である。

図 6　図 4 のランダム化画像

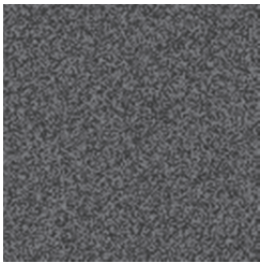


図 7　図 6 の暗号画像

ランダム化画像の暗号画像は平坦化され画面全体が一様に変化しているのがわかる。このランダム化処理方法は提案の 1 つである。

画素数 128×128 の図案画像例として、図 8 の個人情報画像をランダム化処理し、離散コサイン変換で暗号化した場合の暗号画像を図 9 に示す。暗号画像が一様で平坦化されていることがわかる。以降は、ランダム化処理してないデータ系列と区別を必要としない限り、ランダム化処理後のデータ系列をも単にデータ系列という。

図 8　個人情報画像

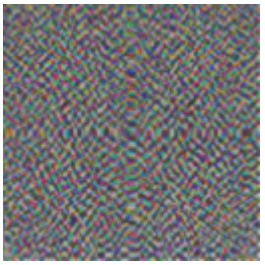


図 9　暗号画像

離散コサイン変換後の展開係数を暗号画像に記録するとき、展開係数を量子化する必要がある。BMP 形式画像の画素値は 0～255（8 ビット）という正の整数値に制限されている。したがって展開係数を暗号画像として記録に残すためには、最小値が 0、最大値が 255 の範囲に入るように画素値を量子化する必要がある。

そこで、式(5)を用いて展開係数を 0～255 の整数に

量子化する。ただし、展開係数の値をp、暗号画像の値をqとする。

$$q = \frac{p-min}{max-min} \times 255 \qquad (5)$$

式(5)のグラフを図 10（代表点 20 個）に示す。なお、小数点以下は四捨五入する。またmax、minはそれぞれpの最大値、最小値を意味する。

式(5)の量子化処理後の再生画像（図 11）と量子化する前の個人情報画像（図 8）との相関係数は赤色、緑色、青色においてそれぞれ 0.998、0.998、0.998 である。

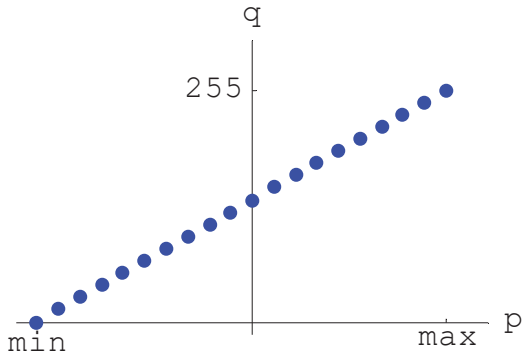


図 10　式(5)のグラフ

図 11　式(5)処理後の再生画像

Ⅳ　安全のために

電子透かし画像が伝達中に盗聴されても、個人情報画像の安全性を確保できる方法を 2 つ提案する。一つはカギ画像を用いる方法で、もう一つは暗号画像をカギ画像に埋め込むときのカギ数値である。それらを順に述べる。

1　カギ画像

三重電子透かし画像の安全性確保の 1 つ目は、送り手と受け手の 2 人だけが所有する共通のカギ画像である。カギ画像は特殊な画像でなく、家庭や職場に満ち溢れている日常的な画像であれば、どのような画像であってもよい。送り手はカギ画像の中に個人情報画像の暗号画像を埋め込み受け手に伝達する。図 1(b)に示すように、受け手は三重電子透かし画像からカギ画像を差し引くことで、暗号画像を抽出することができる。

仮に、送受信する間に三重電子透かし画像が盗聴されたとしても、盗聴者はカギ画像を所有してないので、三重電子透かし画像からカギ画像を差し引くことはできない。したがって、暗号画像を三重電子透かし画像から抽出することができない。このことが個人情報画像の安全性を確保してくれる。

2　カギ数値

2 つ目の安全性確保はカギ数値である。カギ数値は暗号画像をカギ画像の中に埋め込むときの割合比である。カギ数値は送り手と受け手の 2 人だけが知っている数値であるから、カギの役割を果たすことができる。

送り手が受け手に送る三重電子透かし画像は式(6)で表される。

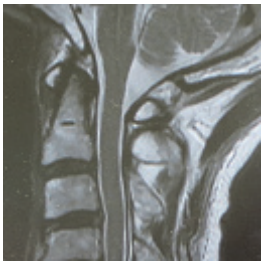
$$w = (1-\beta)f_0 + \beta \times h \qquad (6)$$

w：三重電子透かし画像　f_0：カギ画像
h：暗号画像　β：カギ数値

カギ数値βがカギの役割を果たすことを定量的に例示する。カギ数値を1/8として、図 4 の電子透かし画像を制作する。そして、カギ数値を1/4、1/6、1/10、1/12と変えて再生した画像を表 1 に示す。相関係数はカギ数値が1/8の再生画像に対する値である。制作するときのカギ数値と異なるカギ数値で再生すると、再生画像が劣化することが示されている。

表 1　異なるカギ数値による再生画像と相関係数

カギ数値	再生画像	相関係数
$\frac{1}{4}$		0.563
$\frac{1}{6}$		0.883

$\frac{1}{8}$		1.0
$\frac{1}{10}$		0.808
$\frac{1}{12}$		0.691

V　三重化のために

ここでは、1 枚の画像の中に 3 枚の画像を埋め込む方法を記述する。BMP 形式画像は赤(R)、緑(G)、青(B)の 3 色で構成されている。それらの画素値は赤色、緑色、青色のデータ系列として記録されている。したがって、各色のデータ系列に単色の暗号画像を埋め込むと、三重の暗号画像を 1 枚の暗号画像としてつくることができる。

一般的な三重の埋め込みは、カラー画像 3 枚を埋め込むことを指すが、ここでは図 12 のように赤色の単色画像、緑色の単色画像、青色の単色画像の 3 枚を赤色、緑色、青色のデータ系列に埋め込む。

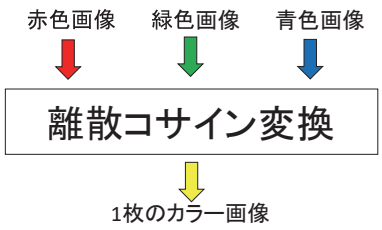


図 12　各色別の三重電子透かし画像

次に、赤色 {R}、緑色 {G}、青色 {B} のデータ系列を式(1)の離散コサイン関数φ_{nm}で変換したときのそれぞれの展開係数$\{r\}$、$\{g\}$、$\{b\}$を式(7)、式(8)、式(9)に示す。

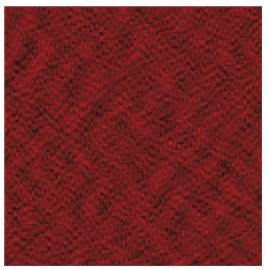
$$r_{nm} = \frac{\sum_{j=0}^{N-1}\left(\sum_{i=0}^{N-1} R_{ji}\varphi_{mi}\right)\varphi_{nj}}{\left(\sum_{i=0}^{N-1}(\varphi_{mi})^2\right)\cdot\left(\sum_{j=0}^{N-1}(\varphi_{nj})^2\right)} \quad (7)$$

$$g_{nm} = \frac{\sum_{j=0}^{N-1}\left(\sum_{i=0}^{N-1} G_{ji}\varphi_{mi}\right)\varphi_{nj}}{\left(\sum_{i=0}^{N-1}(\varphi_{mi})^2\right)\cdot\left(\sum_{j=0}^{N-1}(\varphi_{nj})^2\right)} \quad (8)$$

$$b_{nm} = \frac{\sum_{j=0}^{N-1}\left(\sum_{i=0}^{N-1} B_{ji}\varphi_{mi}\right)\varphi_{nj}}{\left(\sum_{i=0}^{N-1}(\varphi_{mi})^2\right)\cdot\left(\sum_{j=0}^{N-1}(\varphi_{nj})^2\right)} \quad (9)$$

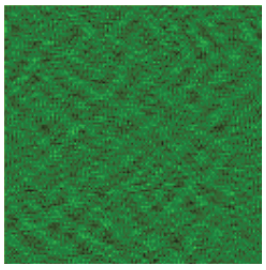
この展開係数がそのまま暗号画像の画素値となる。図 13(a)、(b)に赤色データ系列、図 13(c)、(d)に緑色データ系列、図 13(e)、(f)に青色データ系列の個人情報画像とその暗号画像を順に並べる。図 13(g)に赤色、緑色、青色のデータ系列の三重の暗号画像を示す。

(a)　赤色系列個人情報画像



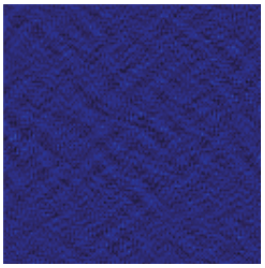
(b)　(a)の暗号画像

(c)　緑色系列個人情報画像

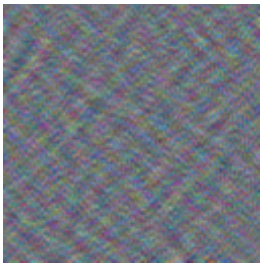


(d)　(c)の暗号画像

(e)　青色系列個人情報画像



(f)　(e)の暗号画像



(g)　(b)、(d)、(f)の三重の暗号画像

図 13　三重の暗号画像

図 13(g)の三重の暗号画像を図 14(a)のカギ画像に埋め込むと、図 14(b)の三重電子透かし画像を制作できる。

(a)　カギ画像　　(b)　三重電子透かし画像

図 14　カギ画像と三重電子透かし画像

なお、カギ画像の中に三重の暗号画像を埋め込む方法は式(6)にしたがう。

VI　再生

三重電子透かし画像から 3 枚の個人情報画像を再生するときは、電子透かし画像の制作手順を逆順にするとよい。

1　カギ画像の除去方法

最初に、三重電子透かし画像からカギ画像を取り除いて、三重の暗号画像を抽出する。三重の暗号画像は、次のように逆算される。

$$h=\{w-(1-\beta)f_0\}/\beta \qquad (10)$$

w：三重電子透かし画像　f_0：カギ画像

h：三重の暗号画像　β：カギ数値

三重の暗号画像は元の三重暗号画像と類似しているが、元の三重の暗号画像そのものではない。それは各色の暗号画像をカギ画像に埋め込むとき、各色のデータ系列の画素値を量子化しているため誤差が発生しているからである。式(10)による三重の暗号画像を例示する。図 14(b)の三重電子透かし画像から、抽出した三重の暗号画像が図 15 である。

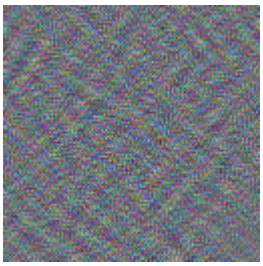


図 15　抽出した暗号画像

2　再生方法

赤色のデータ系列の暗号画像r_{nm}を離散コサイン関数φ_{nm}で再生するには、式(11)を用いる。

$$R_{ji}=\sum_{n=0}^{N-1}\left(\sum_{m=0}^{N-1} r_{nm}\varphi_{mi}\right)\varphi_{nj} \qquad (11)$$

緑色、青色の暗号画像は、それぞれ式(12)、式(13)を用いて再生する。

$$G_{ji}=\sum_{n=0}^{N-1}\left(\sum_{m=0}^{N-1} g_{nm}\varphi_{mi}\right)\varphi_{nj} \qquad (12)$$

$$B_{ji}=\sum_{n=0}^{N-1}\left(\sum_{m=0}^{N-1} b_{nm}\varphi_{mi}\right)\varphi_{nj} \qquad (13)$$

図 15 の三重の暗号画像から赤色、緑色、青色のデータ系列の単色画像 3 枚を再生する。その再生画像が図 16 の(a)、(b)、(c)である。元の個人情報画像とほぼ等しい画像が再生されている。

(a)　再生画像（赤色）

(b)　再生画像（緑色）

(c)　再生画像（青色）

図 16　再生画像

VII　実験例と評価

離散コサイン変換を適用した三重電子透かし画像の制作と再生の実験例を示し、類似性を評価する。

1　制作・再生の実験例

実験に用意した、個人情報画像 3 枚は図 17 の(a)、(b)、(c)で、カギ画像は図 17(d)である。

(a)　個人情報画像 1

(b)　個人情報画像 2

(c)　個人情報画像 3

(d)　カギ画像

図 17　個人情報画像とカギ画像

なお、図 17 の(a)は赤色用、(b)は緑色用、(c)は青色用の画像である。

三重電子透かし画像の制作過程を図 18 に示す。

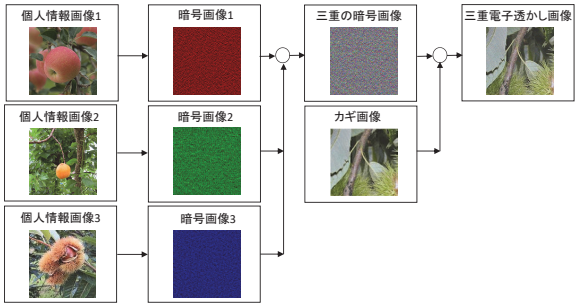


図 18　三重電子透かし画像の制作過程

制作した三重電子透かし画像が図 19 である。

図 19　制作した三重電子透かし画像

次に、三重電子透かし画像の再生過程を図 20 に示す。

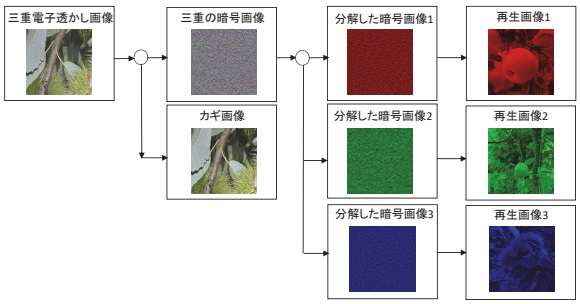
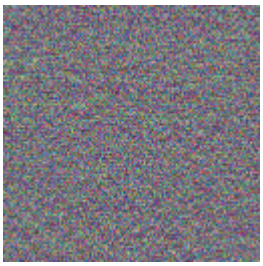


図 20　三重電子透かし画像の再生過程

そして、三重電子透かし画像から抽出した三重の暗号画像を図 21(a)に、赤色、緑色、青色のデータ系列の再生画像を図 21 の(b)、(c)、(d)にそれぞれ示す。



(a)　三重の暗号画像

(b)　再生画像（赤色）

(c)　再生画像（緑色）

(d)　再生画像（青色）

図 21　抽出した三重の暗号画像と 3 枚の再生画像

2　実験評価

制作した三重電子透かし画像（図 19）とカギ画像（図 17(d)）との類似性、および再生した 3 枚の再生画像（図 21(b)、(c)、(d)）と元の個人情報画像（図 17(a)、(b)、(c)）との類似性を評価する。類似性の評価は、赤色{R}データ系列、緑色{G}データ系列、青色{B}データ系列ごとに相関係数を尺度として行う。その結果を表 2 に示す。いずれの場合においても、相関係数の値が 0.9 以上である。それぞれの 2 枚の画像間の類似性が高いといえる。

表 2　類似性の相関係数

カギ画像と三重電子透かし画像の相関係数	個人情報画像 3 枚と再生画像の相関係数
(0.995，0.996，0.996) (R,G,B 順)	赤色画像(0.950，0，0) 緑色画像(0，0.911，0) 青色画像(0，0，0.964)

Ⅷ おわりに

1 枚の画像で 3 枚の個人情報画像を安全に伝達することができる三重電子透かし画像について述べてきた。

その三重電子透かし画像は、図 1(b)に示すように、1 枚の暗号画像をカギ画像に埋め込めた画像である。

したがって、この三重電子透かし画像から個人情報画像を再生するには、送り手と同一のカギ画像を三重電子透かし画像から差し引かなければならない。差し引くことで、三重の暗号画像を抽出することができる。その三重の暗号画像を復号化すると、図 1(a)に示すように個人情報画像 3 枚を再生することができる。

この三重電子透かしには特徴が 2 点ある。1 点目は、1 枚の画像の中に 3 枚の個人情報画像を多重に埋め込んだ電子透かしであるから、1 枚の画像で 3 枚の個人情報画像を伝達することができる点である。

もう 1 点は、カギ画像を用いている点である。送り手と受け手の 2 人だけが所有するカギ画像は安全性を高めてくれる。なぜならば、伝達途中に盗聴されたとしても、盗聴者はそのカギ画像を所有してないので、三重電子透かし画像から暗号画像を抽出することができないからである。仮に暗号画像が抽出されたとしても、その暗号画像のカギ数値が不明なままでは、暗号を復号することは困難であるといえる。

最後に、離散コサイン変換以外にも、離散コサイン変換と同じように画像を暗号化できる関数系が数多くある。そのような関数系と、離散コサイン変換を有効に組み合わせることにより、より一層に秘匿で安全性の高い多重電子透かし画像をつくることができるものと期待する。

[参考文献]

(1) U.Mustafa,U.Guzin,V. V.Nabiyev, Menical image security and EPR hiding using Shamir’s secret sharing scheme, Journal of Systems and Software, Vol.84, No.3, 2011, pp.341-353

(2) M.Kaur, R.Kaur, Reversible watermarking of medical images authentication and recovery, Journal of Information and Operations Management, Vol.3, No.1, 2012, pp.241-244

(3) S.Alyammahi,F.Taher,H.Al-Ahmad,T.McGloughlin, A New Multiple Watermarking Scheme for Copyright Protection and Image Authentication , IEEE50th International Midwest Symposium on Circuits and Systems, 2016

(4) G.Coatrieux, C.L.Guillou, J.M.Cauvin, C.Roux, Reversible watermarking for knowledge digest embedding and reliability control in medical images, IEEE Transactions on Information Technology in Biomedicine, Vol.13, No.2, 2009, pp.158-169

(5) 佐々木隆幸、2 枚の電子透かし情報画像を埋め込めた電子透かしの制作と復元、特許庁、特願 2016-217619、2016

(6) 佐々木隆幸、川守田聡、直交関数系でつくる電子透かし、職業能力開発報文誌、Vol.30、No.1、2018、pp.1-12

(7) 佐々木隆幸、偶関数と奇関数を活用した電子透かし画像の制作、Hi-Tec 青森(東北職業能力開発大学校青森港産業技術高度化振興会)、Vol.18、2014、pp.49-53

(8) S.Makhmasi,F.Taher,Al-Ahmad, T.McGloulin, A novel multiple watermarking algorithm for patient identification and integrity control, UKSim-AMSS 17th International Conference on Modeling and Simulation,UK,2015