I-057

KLT を用いた電子透かし通信容量の計算方法

Calculating Information Hiding Capacity of Digital Watermarking Using Karhunen-Loeve Transform

新名 麗† 菅井 豊和† 藤井 亮介† 鈴木 光義† 伊藤 浩† 浅井 光太郎† 村上 篤道‡
Urara Shimmyo Toyokazu Sugai Ryosuke Fujii Mitsuyoshi Suzuki Hiroshi Ito Kotaro Asai Tokumichi Murakami

1. まえがき

電子透かし通信容量の計算方法として，画像などのホスト信号を複数のチャネルに分割し，チャネルの信号をガウス雑音と仮定して求める手法がある．従来では，チャネル分割に DCT やウェーブレット変換などを用いていた．しかし，これらの変換はチャネル間の相関を完全には除去できず，通信容量が大きめに計算されていた．したがって，チャネル間の相関を完全に除去する KLT を用いれば，通信容量をより厳密に求められると考えられる．実験により，エッジ部分においては，KLT による相関の除去が正確な通信容量を計算するのに有効であることがわかった．そこで，さらなる展開として，画像を規則性の有無によって領域分割し，それぞれの領域に対して KLT を用いて通信容量を求め，それらを足し合わせてより厳密に通信容量を求める手法を提供する．実験によれば，自然画像の場合，従来の計算方法よりも 10～40%程度通信容量が小さく計算されることがわかった．

2．Moulin らの手法

電子透かしの通信容量とは，電子透かしによって秘密に伝達される情報量であり，通信路には情報を破壊する攻撃者が存在してよい．Moulinらは，DCTやウェーブレット変換などを用いて信号を複数の周波数チャネルに分割し，各チャネルの信号を独立なガウス信号と仮定して電子透かしの通信容量を求めている[1]．ここで，実際の信号がガウス信号でない場合，この値は上限を与える．以下，通信容量という場合はその上限を指す．

この方法では，σ_k^2 をチャネル $k(1\le k\le K)$ の信号電力，r_k をチャネル k のビットレート，d_{1k}，d_{2k} をチャネル k における電子透かしおよび攻撃から導入される歪み電力とすると，通信容量は

$$C=\max_{D_1}\min_{D_2}\sum_{k=1}^{K} r_k\Gamma(\sigma_k^2,d_{1k},d_{2k}) \tag{1}$$

から求められる．ただし，

$$\Gamma(\sigma_k^2,d_{1k},d_{2k})=\frac{1}{2}\log\left\{1+\frac{d_{1k}}{d_{2k}-d_{1k}}\left(1-\frac{d_{2k}}{\sigma_k^2}\right)\right\}$$
$$=\frac{1}{2}\log\frac{d_{2k}(\sigma_k^2-d_{1k})}{\sigma_k^2(d_{2k}-d_{1k})} \tag{2}$$

である．ここで，D_1，D_2 は電子透かしおよび攻撃に関する歪み制約であり，埋め込み者は D_1 の制約の下で d_{1k} を調節して C を最大にしようとする．一方，攻撃者は D_2 の制約の下で d_{2k} を調節して C を最小にしようとする．

しかし，この方法を画像に適用する場合，DCT などを用いて分割した信号は，互いに無相関であると仮定しているが，必ずしもそうとは限らない．例えば，エッジ部分ではエッジの方向に強い相関があり，大きな信号電力が発生するため，実際よりも通信容量が大きく計算されてしまう．そこで，本論文では，各チャネルの相関を完全に除去する方法として知られる KLT（Karhunen-Loeve Transform）による有効性を示し、より厳密な通信容量を求める手法を提供する．

3．KLT を用いた手法

3.1 KLT による計算方法

KLT は，K 次元の信号ベクトル $X=(X_1,X_2,\ldots,X_K)$ の共分散行列

$$A=\begin{pmatrix} A_{1,1} & \cdots & A_{1,K} \\ \vdots & \ddots & \vdots \\ A_{K,1} & \cdots & A_{K,K} \end{pmatrix} \tag{3}$$

を求め，この行列に対して固有値問題を解くことにより与えられる．ただし，

$$A_{i,j}=\frac{1}{N}\sum_{n=1}^{N}X_i(n)X_j(n),\qquad 1\le i,j\le K \tag{4}$$

とし，N はデータの総数を表す．ここで，A の固有値は変換係数の電力に等しく，画像電子透かしの通信容量を求めるには，例えば 512×512 画素の画像に対し，$X(n)$ $(1\le n\le 4096)$ を，8×8 ブロックを並び替えた 64 次元信号ベクトルとして式(3)とその固有値を求め，固有値から式(1)にしたがって求めればよい．

3.2 有効性

KLT による効果を示すために，以下のような設定で通信容量を求め，比較実験を行った．

DCT：8×8 の DCT を用いてチャネル分割する（従来法）．

KLT：8×8 のブロックを並び替えた 64 次元の信号ベクトルから KLT によりチャネル分割する．

ここで，各手法において，D_1 は画像の信号電力の 1/10000 とし，D_2 は D_1 の 5，10，20，50 倍に設定して，図 1 の各画像において通信容量を求めた．

結果として，LENA および BABOON では DCT と KLT の違いはほとんどないが， DIAGONAL では DCT よりも KLT の方が 40～90%程度，SQUARE では 55～65%程度通信容量の値を小さく計算した．これは，自然画像では DCT がよくチャネル間の相関を除去しているが，単純なエッジと平坦部分からなる図形では，KLT による相関の除去が厳密な通信容量を求めるのに有効であると言える．

†三菱電機（株）情報技術総合研究所，Information Technology R & D Center, Mitsubishi Electric Corporation
‡三菱電機（株）開発本部，Corporate Research and Development, Mitsubishi Electric Corporation

3.3 KLT を用いた効果的手法

3.2 節より，エッジ部分では，KLT を用いれば DCT より厳密な通信容量を計算するのに有効であることがわかった．そこで，自然画像においてもより厳密な値を求めるために，画像を複数のプロセスから生じた信号と仮定し，プロセスごとに通信容量を求める方法を考える．その方法として，初めに画像のブロックを規則性の有無によって領域分割する．次に，各領域において，互いに独立になるように KLT を用いて K 個のチャネルに分割し，それぞれの通信容量を求める．最後に各領域の算出結果を足し合わせることにより，画像全体の通信容量を求める．

3.2 節と同様の設定で実験した結果，LENA では DCT よりも 10～30％程度通信容量の値を小さく計算したが，BABOON ではほとんど変化がなかった．これは，LENA は人物の輪郭における明確なエッジ部分が存在し，その部分においてうまく相関の除去ができたことを示している．しかし，BABOON は動物の毛並みのようにテクスチャ部分が多く存在し，エッジ部分が少なく，DCT が相関をよく除去しているため，変化がなかったと考えられる．また，単純図形において，DIAGONAL では DCT よりも 65～95％程度，SQUARE では 85～90％程度小さく計算しており，エッジと平坦部分を切り分けることにより，エッジの相関をより効果的に除去できたと考えられる．その他 8 種類の画像について DCT と比較した結果，自然画像については 60～90％程度小さく計算された．したがって，チャネル分割には DCT よりも KLT を用い，さらに領域分割を考慮すれば，より厳密な通信容量が求められる．

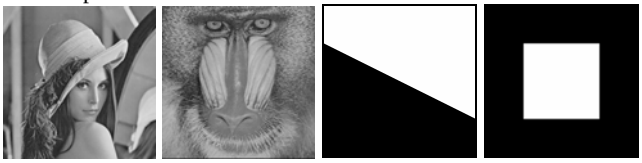
なお，実験結果を 3.2 節の結果とともに，表 1 に $D_2 = 5D_1$ の場合の通信容量の計算例を，図 2 に各画像における 3 つの手法の計算結果を示した．ただし，領域分割を考慮した手法を KLT+α として表記している．

4. むすび

従来の通信容量の計算方法では，チャネル分割に DCT などを用いていたが，エッジを含む画像においてチャネル間の相関を完全には除去できなかったため，KLT の特徴を活かした手法を提供した．その方法として，画像信号を複数のプロセスから生じた信号と仮定し，まず，画像のブロックを規則性の有無によって領域分割する．次に，各プロセスにおいて，互いに独立になるように KLT を用いて複数のチャネルに分割する．そうすることにより，多くの自然画像に対して電子透かしの通信容量を厳密に求めることができる．なお，本研究は，情報通信研究機構の委託研究「誰でも使用・改良・評価できる安全な電子透かし技術の研究開発」の成果である．

参考文献

[1] P. Moulin and M. K. Mihcak, “The Parallel-Gaussian Watermarking Game,” UIUC Coord. Sci. Lab Tech. Report, Sept. 2003.

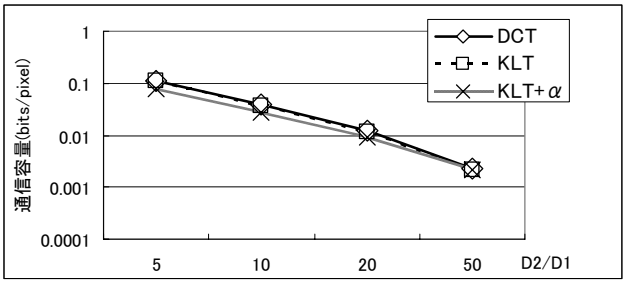


(a)LENA (b)BABOON (c)DIAGONAL (d)SQUARE

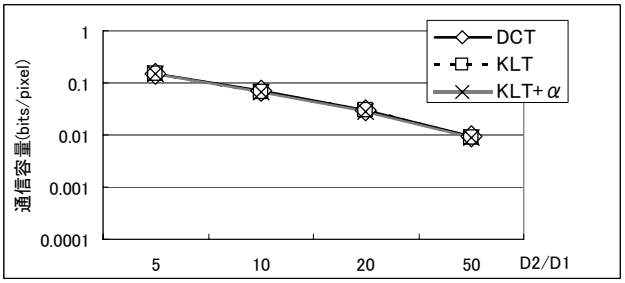
図 1：実験対象画像（512×512 画素）

画像	歪み D_1	DCT (bits/pixel)	KLT (bits/pixel)	KLT+α (bits/pixel)
LENA	1.768	0.1103	0.1076	0.0781
BABOON	1.753	0.1535	0.1531	0.1482
Diagonal	3.251	0.0582	0.0073	0.0026
square	1.600	0.0391	0.0135	0.0030

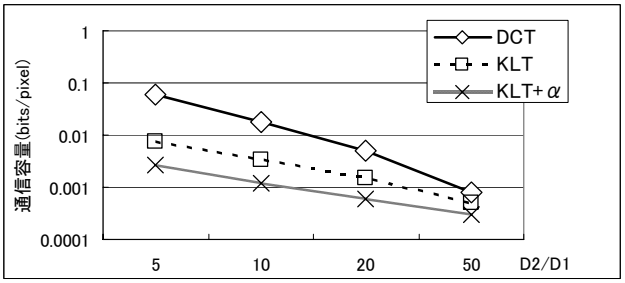
表 1： $D_2 = 5D_1$ の場合の通信容量の計算例



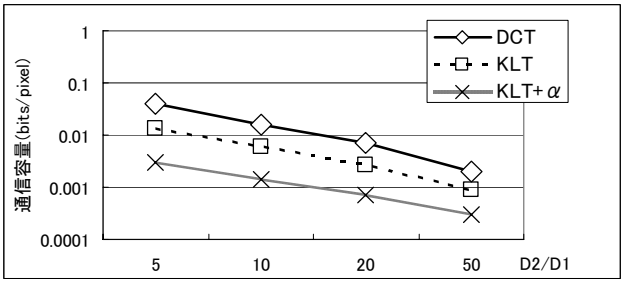
(a) LENA（ D_1 =1.768）



(b)BABOON（ D_1 =1.753）



(c)DIAGONAL（ D_1 =3.251）



(d)SQUARE（ D_1 =1.600）

図 2：各手法における通信容量の計算結果