電子透かし(2)

コンテンツ配信技術10

菊池浩明

LSB置換の限界

- 攻撃に対する安全性が弱い
  - 透かしを＿＿＿＿，取り除く.
- 攻撃の種類
  - 変換（回転，縮尺，拡大）
  - ＿＿＿＿＿＿＿＿攻撃（ノイズ付加）
  - JPEG攻撃（圧縮率の変化）

3. ドメイン変換法

- 原理
  - DCTやウェーブレット変換により＿＿＿＿変換した領域に埋め込む
- 利点
  - 画像全体に変化が及び，取除くのが困難

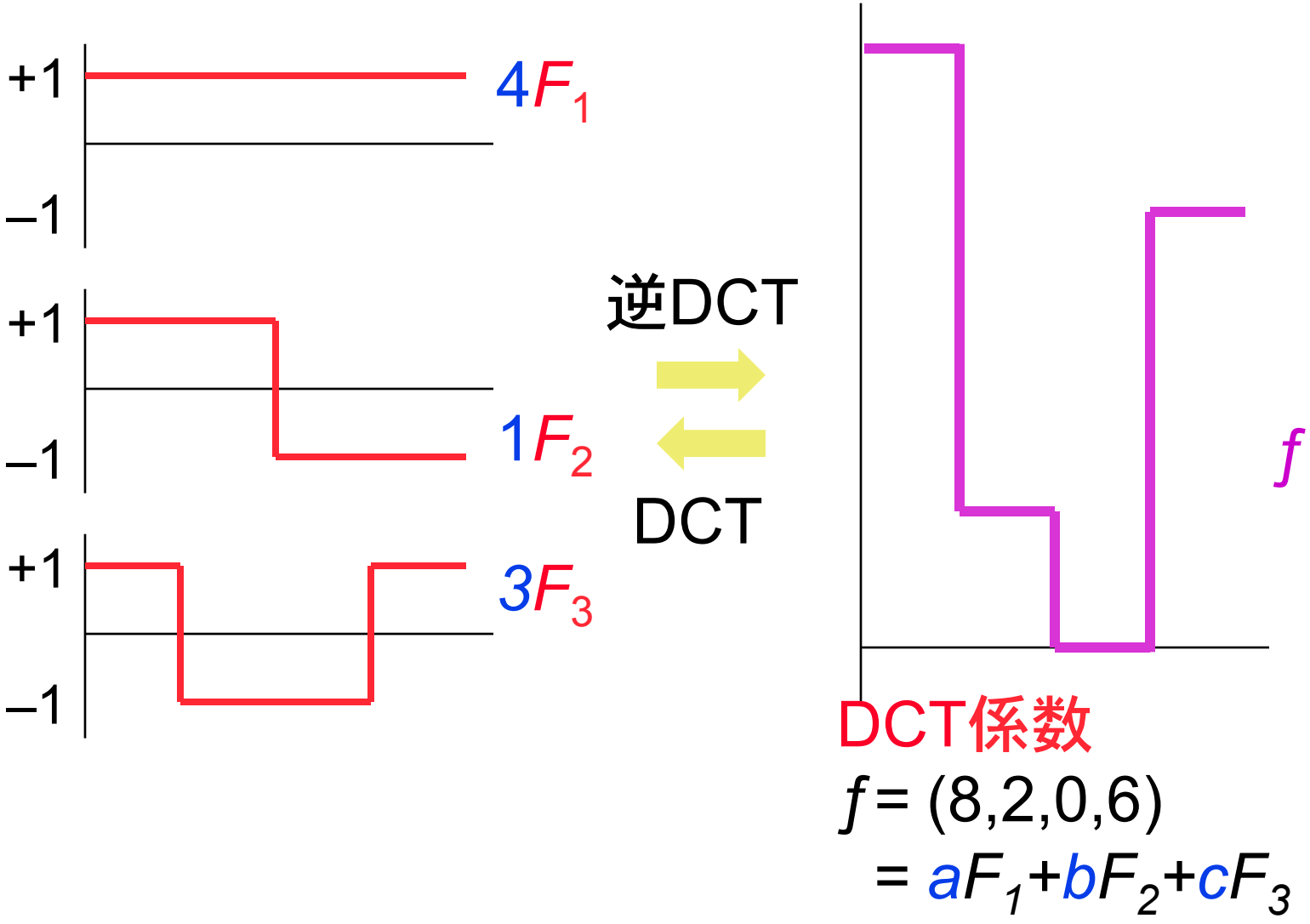
JPEGの原理

- 離散コサイン変換
  - Discrete Cosine Transform: DCT
  - 画像データ f(x,y) (-128~+127)
  - インデックス x, y, u, v = 0,1,...,7

$$F(u,v) = \frac{1}{4} C(u) C(v) \left(\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \right)$$

  - C(0)=1/√2, C(1)=...=C(7)=1

DCTと逆DCT



(1) 周波数成分への置換

- 置換法
  - DCT係数 G =(x1, x2, x3), 埋込み情報 b
  - 埋込み係数 G' = (x1, x2, b)
  - 例) G=(4,1,3), b=2の時,
    G'= (4,1, 3)
  - 逆DCT変換
    f' = 4 F1+1 F2 + 2 2= (_____) ≠ (8,2,0,6)

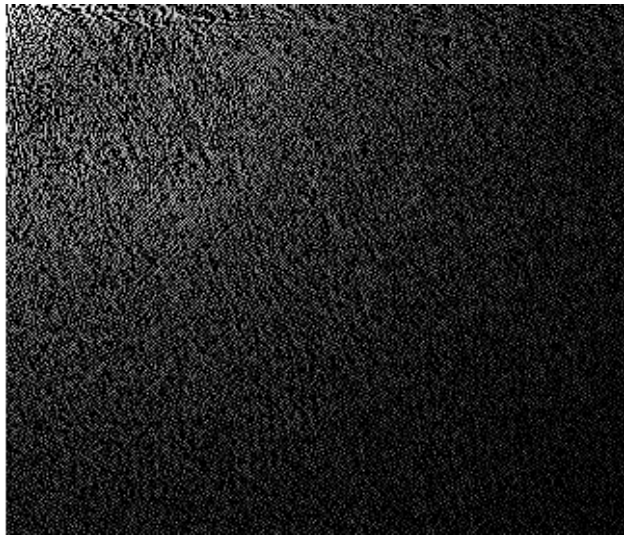
埋込む領域

- 秘密の数列
  - x1=h(h0), x2=h(x1), x3,…
  - 例) x1=28, x2=42, x3=9, x4=39
    複数繰り返し同じ透かしを埋込む

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

2次元DCT

- 周波数成分
- 原画像



逆変換
(IDCT)

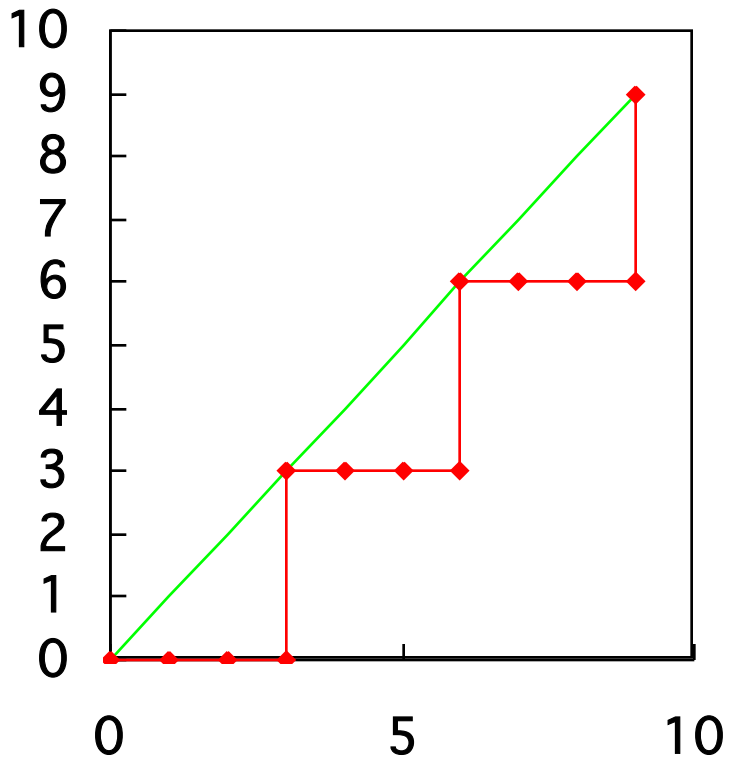
周波数
変換
(DCT)

(2) 量子化 quantization

- cによる量子化

$$q_c(x) = \left\lfloor \frac{x}{c} \right\rfloor \times c$$

  - $\lfloor x \rfloor$ floor of x = xを超えない最大の整数
  - $q_3(19)$ =floor(19/3)x3 =(6.333)x3 =18
  - $q_3(20)$ =6.666x3=
  - $q_3(21)$ =7x3 =
  - $q_3(22)$ =7.333x3=



量子化を用いた埋め込み

- 量子化処理
  - x = 入力（DCT係数），b = 透かし情報
  - c = 量子化定数

$$q_{c,b}(x) = \begin{cases} \left\lfloor \frac{x}{c} \right\rfloor \times c & \text{if } b = 0 \\ \left\lceil \frac{x}{c} \right\rceil \times c & \text{if } b = 1 \end{cases}$$

  - 例）$q_{3,0}(8)$ = floor(8/3)*3 = floor(2.6)*3 = $q_{3,0}(8)$ = celling(8/3)*3 = celling(2.6)*3 =

その他のドメイン変換法

- 直交＿＿＿＿＿＿＿＿＿＿変換によるすかし
- スペクトル拡散によるすかし
- パッチワーク法
  - 統計量の利用

歪曲法の例

- 元文書

  ネットワーク基盤の発達などによって，電子的にやりとりされる情報量がめざましく増加している．それに伴い，電子化されたコンテンツに対する著作権保護が大きな問題となっている．

- 埋込文書

  ネットワーク基盤の発達などにより，電子的にやりとりされる情報量が目覚ましく増加している．それに伴って，電子化されたコンテンツに対する著作権の保護が大きな問題となっている．

他の情報ハイディング技術

ステガノグラフィ

ステガノグラフィ (Steganography)

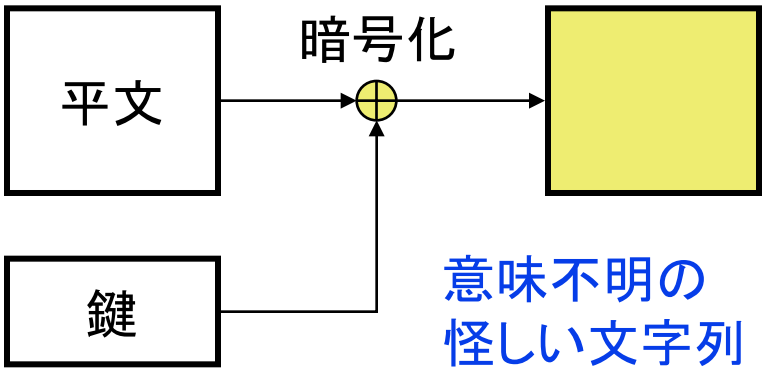
- 定義
  - 通信している＿＿＿を隠す技術
  - ギリシャ語の “*hidden writing*”
  - 「奴隷の頭に入れ墨」
  - 「あぶり出し」“invisible ink”
  - “Doll Woman” 第二次大戦中の人形の発注で戦艦の数を伝えたスパイ

S-Tools

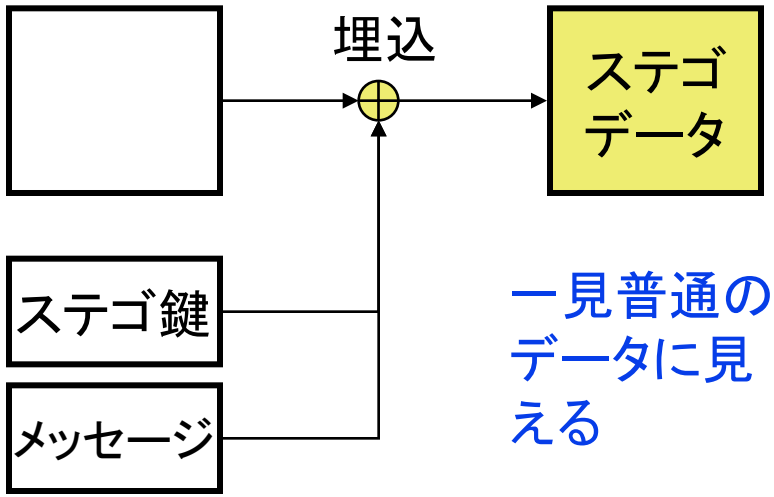
- S-Tools
  - BMP, GIFにデータを埋め込む
  - 共通鍵で暗号化
  - 埋込レベルを選択
    - » Akito.gif (395 kbytes)
    - » deCSS.c (10.4 kbytes)
    - » akito-hidden.gif (290 kbytes)

ステガノグラフィと暗号化

- 暗号



- ステガノグラフィ



ステガノグラフィと電子透かし

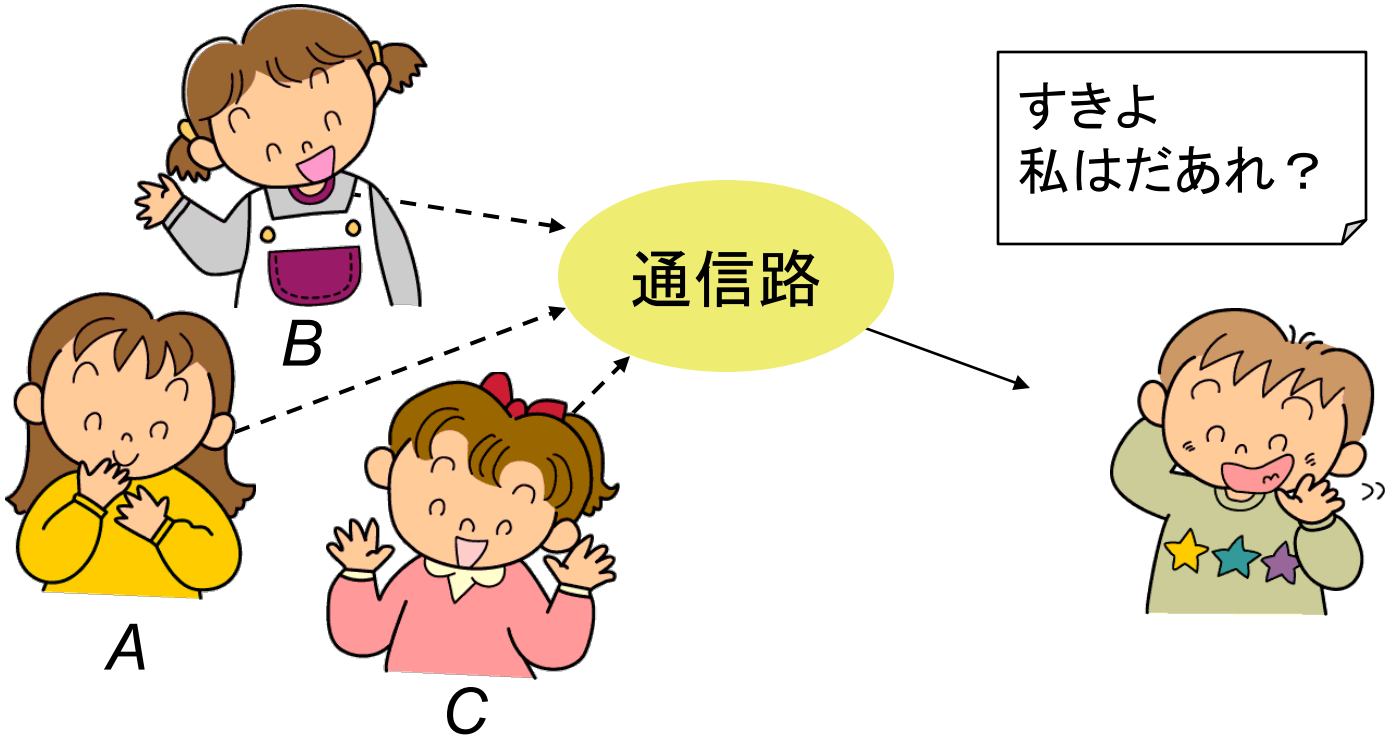
	電子透かし	ステガノグラフィ
目的	コンテンツを守る	メッセージを伝える
埋込情報	著作者情報，コピー制御情報	
攻撃	回転，移動，拡大，差分などにより透かしを取り除く（　　耐性）	どのメッセージが疑わしいか確率的に判別（　　耐性）
技術	歪曲法，置換法，ドメイン変換法	

匿名通信路

Tor

匿名通信路

- 送信者の匿名性
  - 誰から届いたのかわからない

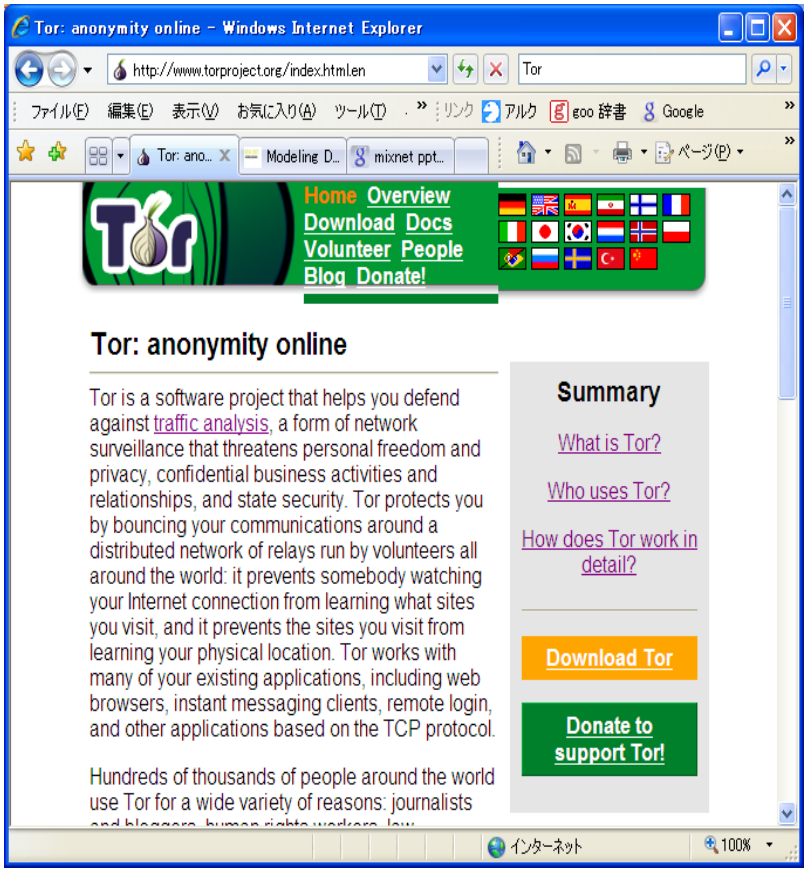


匿名でないと困ること

- 匿名でないと困ること
  - エイズ検査
  - 内部告発
  - 告白記事
  - 投票
  - 犯罪捜査
  - 電子商取引
  - エッチなビデオの購入

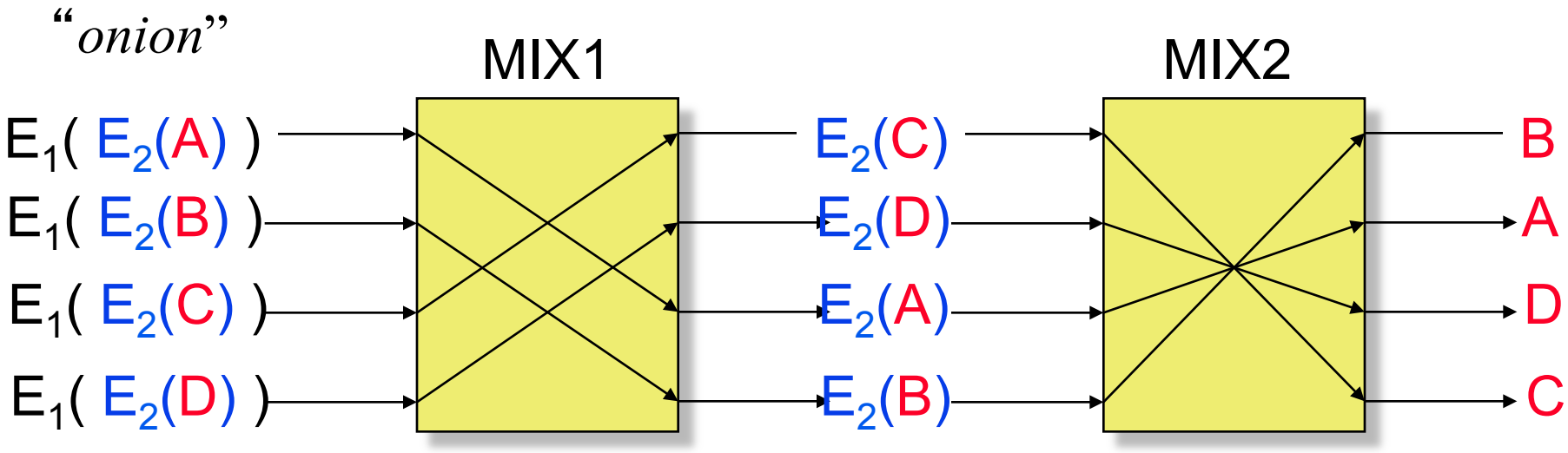
Background: Tor

- Tor: The Second-Generation Onion Router
  - R. Dingledine, N. Mathewson (Free Haven Project) and P. Syverson (Naval Research Lab)
  - USENIX Security Symp. 2004



http://www.torproject.org/

Chaum's MIX-NET



- Pros: Traffic Analysis
- Cons: High Latency, Perfect Forward Security

まとめ

- （　　）変換を用いた電子透かしは，透かしを取り除きに対して安全性が高く，DCT係数の置換法や（　　）法がある．
- ステガノグラフィは，通信している事実を(　　)から隠す技術，匿名通信路は，送信者を（　　）から隠す技術である．これらを電子透かしと合わせて情報（　　）という．
- 匿名通信路Torは，第二世代（　　）ルーティングの略である．

演習

- 画像f = (20, 19, 67, 29)に透かし情報b = 2 = $0010_{(2)}$を埋込みたい.
  - 基底　F_1 = (1,1,1,1), F_2=(1,1,-1,-1), F_3=(1,-1,-1,1), F_4 = (1,-1,1,-1)を用いて周波数成分(x_1,x_2,x_3,x_4)を求めよ.
  - b=$b_1b_2b_3b_{4(2)}$を使い，G' = $q_{1,b1}(x_1)$,..,$q_{1,b4}(x_4)$と埋込め.
  - G'のPSNRを求めよ. $\log_{10}$ 2=0.3を使え.