論　文

スペクトル拡散モデルにおける非同期確率アルゴリズム及び温度スケジューリングによる復号の性能評価

寺西　直緒[†]　　川村　正樹[†a)]

Performance Evaluation for Decoder with Asynchronous Stochastic Algorithms and Temperature Schedules for Spread Spectrum Model

Nao TERANISHI[†] and Masaki KAWAMURA[†a)]

あらまし　スペクトル拡散モデルにおいて，非同期型確率ダイナミックスを導入した復号方法を提案する．従来のベイズ推定に基づく復号アルゴリズムでは，同期型決定論的ダイナミックスが用いられていた．非同期方式により，振動解の発生が抑えられ，確率を導入した有限温度復号では，極値にとどまることがなく最適値に向かうことが期待できる．また，有限温度による復号については，初期から温度固定で更新する手法のほかに，絶対零度まで冷却する従来型 SA や，最適温度で冷却を止めてそれ以後はその温度を維持するように修正した有限温度止め SA を検討し，これらを性能評価する．計算機シミュレーションの結果，従来手法に比べ，非同期有限温度復号の性能がよいことが分かった．有限温度の中でも，有限温度止め SA の方が絶対零度まで下げる SA よりも性能が良く，温度固定の復号よりも温度誤差に対して耐性があることが分かった．

キーワード　スペクトル拡散，復号アルゴリズム，電子透かし，非同期方式，確率ダイナミックス，焼きなまし法

1. まえがき

スペクトル拡散技術は，伝達メッセージを拡散符号系列により拡散して，冗長性を持たせることで，安定した情報伝達を可能にする技術である．スペクトル拡散技術は，Code Division Multiple Access（CDMA）[1]～[3] や電子透かし技術 [4]～[7] で使われている．ここでは，この技術を用いたモデルをスペクトル拡散モデルと呼ぶ．

CDMA は携帯電話における通信技術として使われており，拡散符号を用いて多数のユーザによる同時通信を可能とする技術である．各ユーザの端末では，それぞれメッセージ信号を拡散符号で拡散し，送信する．一方，基地局ではノイズが乗った受信信号から拡散符号を用いてユーザのメッセージを推定する [2]．

受信側では複数の信号が足し合わされているため，復調時に信号間の干渉が生じる [8]．この干渉を減少させることで，より誤りの少ないメッセージ信号が得られる．CDMA の復号において，最大事後確率（MAP）推定や周辺事後確率最大化（MPM）推定がある．これらの通信路容量が情報統計力学で評価されている [9]～[11]．また，マルチステージ復調 [2], [3], [12] や部分干渉除去法 [13]～[15] などが提案されている．

電子透かしとは，画像や音楽などのディジタルコンテンツに著作者情報などを秘密裡に埋め込む技術である．埋込情報が検出できることで，コンテンツの不正利用を抑制する技術として期待されている．画像電子透かしには，埋め込む著作者情報などの各メッセージを拡散符号で拡散して，画素の輝度値 [4] や DCT 係数 [5], [6] に埋め込む手法がある．埋込にはメッセージを重ね合わせて埋め込む多重化 [16] を行う．透かしが埋め込まれたステゴ画像には JPEG などの符号化や画像加工の処理が行われる．受信者は加工された画像と拡散符号からメッセージを推定する．このような手法をスペクトル拡散型電子透かしという．

復号するときには CDMA と同様，多重化に起因する透かし間干渉が問題になる．これまでに，ゆう度比に基づく最適な復号方法 [17] やベイズ推定に基づく最

[†] 山口大学大学院理工学研究科，山口市
Graduate School of Science and Engineering, Yamaguchi University, 1677–1 Yoshida, Yamaguchi-shi, 753–8512 Japan
a) E-mail: kawamura@sci.yamaguchi-u.ac.jp

適な復号方法 [18], [19] が提案されている．このように，スペクトル拡散型電子透かしモデルは，拡散符号によるメッセージの拡散や，干渉を除去して復号を行う点で CDMA モデルに対応する．したがって，共通の復号手法が適用でき，これらをスペクトル拡散モデルと呼ぶ．

スペクトル拡散モデルにおいて，メッセージ推定の理論的なアプローチの一つがベイズ推定である．ベイズ推定とは，各メッセージに関する事後確率を求め，それを最大にするメッセージを推定メッセージとする方法である．しかしながら，全てのメッセージの組合せについて事後確率を求めるには，多くの計算量を必要とするため実用的ではない．そのため，復号アルゴリズムを求める必要がある．事後確率を最大化する問題は，それに対応するエネルギー関数を最小化する問題と表現することができる．すなわち，最適化問題で用いられる最適化アルゴリズムを応用することが可能である．

本論文では，電子透かしモデルの復号アルゴリズムを例として説明する．これまでのベイズ推定に基づく準最適な復号アルゴリズムでは，決定論的な復号法 [19] が用いられていた．最適化アルゴリズムでは，決定論的な方法のほかに，確率的な要素を導入した方法もある．また，メッセージの推定には，全メッセージを同期して一括更新を行う方式のほかに，一つずつ個別に更新する非同期方式が知られている．そこで，本論文では，Senda と Kawamura の方法 [19] に確率ダイナミックス及び非同期方式を導入した復号方法を提案し，計算機シミュレーションによって，その性能を評価する．また，確率的手法は次の状態の採択を行う上で温度パラメータを用いるため，このパラメータの扱いが問題になる．そこで，温度パラメータの設定方法についても検討する．以上のように，確率ダイナミックスや非同期方式を導入した復号アルゴリズムに対して，それらの性能を比較することによって，最良の復号アルゴリズムを求める．

本論文は，次のように構成される．**2.** では，スペクトル拡散モデルの例としてスペクトル拡散型電子透かしモデルについて説明し，**3.** では，各復号ダイナミックスについて説明する．**4.** では，有限温度アルゴリズムについて説明する．**5.** では，計算機シミュレーションを行い，各復号ダイナミックスについて比較し，考察する．**6.** でまとめる．

2. スペクトル拡散型電子透かしモデル

スペクトル拡散モデルを画像電子透かしに適用した例に沿って説明していく．スペクトル拡散モデルの復号アルゴリズムを比較するために，電子透かしの埋込方法には，一番簡単な画像置換法の場合を考え，攻撃の影響が加法的白色ガウス雑音（AWGN）で表されると仮定する．電子透かしを実用化する上では，画像を変換し，その係数などに埋め込む手法もある [18]．その場合には，埋込誤差や攻撃によるノイズ項の扱いが異なってくる．

2.1 埋込方法

二次元のグレースケールの画像の中に，透かし情報を埋め込む対象の画素が N 画素あるとする．この N 画素からなるブロックを $\boldsymbol{f} = (f_1, f_2, \ldots, f_N)^\top$ とする．以下ではこのブロックを単に画像と呼ぶ．埋込処理の流れを図 1 に示す．原画像に K ビットのメッセージ $\boldsymbol{s} = (s_1, s_2, \ldots, s_K)^\top$ を重ねて埋め込むとする．ただし，$s_i = \pm 1$ とする．各メッセージ s_i はそれぞれ拡散符号 $\boldsymbol{\xi}_i = (\xi_i^1, \xi_i^2, \ldots, \xi_i^N)^\top$ で拡散され，K 重に重ね合わせて埋め込まれる．ここで，拡散符号長は画像の大きさ N に等しいとする．拡散符号の各要素は ± 1 の値を確率，

$$P[\xi_i^\mu = \pm 1] = \frac{1}{2}, \tag{1}$$

でとる．これより，μ 番目の画素に埋め込まれる透かし情報 w_μ は，

$$w_\mu = \sum_{i=1}^{K} \xi_i^\mu s_i, \quad \mu = 1, 2, \ldots, N, \tag{2}$$

となる．また，ステゴ画像 $\boldsymbol{X}$ は原画像 $\boldsymbol{f}$ に透かし情報 $\boldsymbol{w}$ を加算したものとなる．

$$X_\mu = F_0\left(f_\mu + w_\mu\right) \tag{3}$$

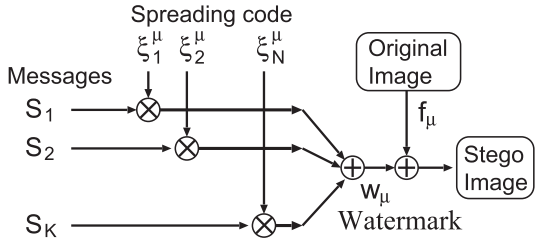


図 1　メッセージの拡散と透かしの埋込方法
Fig. 1　Diagram of spreading messages and embedding of digital watermark.

$$\approx f_\mu + w_\mu + \eta_\mu, \tag{4}$$

ここで，関数 F_0 は輝度値制限関数であり，整数 x に対して，

$$F_0(x) = \begin{cases} 0, & x < 0 \\ x, & 0 \le x \le 255 \\ 255, & x > 255 \end{cases}, \tag{5}$$

を与える．また，近似的に F_0 の影響を加法的に (4) の η_μ で表す．この非線形な関数の影響は，黒（0）や白（255）が多い画像で発生する．中間の値が多い自然画像ではこの影響が小さい．以上の操作で作成されたステゴ画像 $\boldsymbol{X}$ が流通される．

2.2 劣化過程

ステゴ画像 $\boldsymbol{X}$ は，JPEG 圧縮などの不可逆な操作や不正なユーザから攻撃を受けたりする．これらの攻撃はノイズとして扱うことができる．ここでは，AWGN であると仮定し，ノイズ n_μ で表す．復号時に原画像が既知である場合を考える．この場合，攻撃を受けたステゴ画像 $\boldsymbol{X}$ を受信し，これから原画像 $\boldsymbol{f}$ を引いたものが抽出情報となる．すなわち，抽出情報 $\boldsymbol{r}$ は，

$$r_\mu = X_\mu + \eta_\mu + n_\mu - f_\mu \tag{6}$$

$$= w_\mu + \eta_\mu + n_\mu, \tag{7}$$

と表すことができると仮定する．以下の議論では，n_μ は画像 f_μ や透かし情報 w_μ に対して独立であると仮定し，平均 0 分散 σ_0^2 のガウス分布，

$$P(n_\mu) = \frac{1}{\sqrt{2\pi\sigma_0^2}} \exp\left[-\frac{n_\mu^2}{2\sigma_0^2}\right], \tag{8}$$

に従うとする．また，輝度値制限の影響 η_μ は測定できない量であり，中間値の多い自然画像では十分に小さく無視できると考えられる．そこで，η_μ は無視する．もし，η_μ の影響が無視できないほど大きく現れる場合は，η_μ と攻撃によるノイズは区別されずに測定され，実際の分散 σ_0^2 よりも大きな分散として現れる．

2.3 シングル復号

メッセージを 1 ビットずつ独立に推定する方法をシングル復号と呼ぶことにする．抽出情報からメッセージを復号する方法を述べる．抽出情報に，埋込で用いた拡散符号 $\boldsymbol{\xi_i}$ を積和すれば復号することができる．$(\xi_i^\mu)^2 = 1$ が成り立つことに注意すれば，i 番目の相関検出器の出力 h_i は，

$$h_i = \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu r_\mu \tag{9}$$

$$= s_i + \frac{1}{N}\sum_{\mu=1}^{N}\sum_{j\neq i}^{K} \xi_i^\mu \xi_j^\mu s_j + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu n_\mu, \tag{10}$$

となる．ここで，(10) の右辺第 2 項は透かし間干渉項であり，第 3 項はノイズ項である．これらが，第 1 項に比べて小さい場合，推定メッセージ $\hat{s}_i$ は，

$$\hat{s}_i = \mathrm{sgn}(h_i), \tag{11}$$

と求めることができる．ここで，符号関数 $\mathrm{sgn}(h)$ は，

$$\mathrm{sgn}(h) = \begin{cases} +1, & h \ge 0 \\ -1, & h < 0 \end{cases}, \tag{12}$$

で与えられる．

3. マルチ復号

1 ビットのメッセージを N ビットの拡散符号でスペクトル拡散しているため，埋め込める情報は $1/N$ 倍になっている．一方で，メッセージを拡散することによって複数のメッセージを同じ画素に重ねて埋め込むことができる．このとき，透かし間干渉が生じてしまう．前述のシングル復号器では，各メッセージを個別に推定するため，透かし間干渉項が残る．透かし間干渉項を低減する方法として，メッセージを同時に推定するマルチステージ復号が提案されている [19]．

3.1 事後確率

K ビットのメッセージが取り得る組合せは 2^K 通りあるので，一様分布を仮定すると，メッセージの事前確率は，

$$P(\boldsymbol{s}) = \frac{1}{2^K}, \tag{13}$$

となる．また，抽出情報 $\boldsymbol{r}$ を受信したときメッセージ $\boldsymbol{s}$ が得られる事後確率は，

$$P(\boldsymbol{s}|\boldsymbol{r}) = \frac{P(\boldsymbol{r}|\boldsymbol{s})P(\boldsymbol{s})}{\sum_{\boldsymbol{s}} P(\boldsymbol{r}|\boldsymbol{s})P(\boldsymbol{s})}, \tag{14}$$

で表される．条件付き確率 $P(\boldsymbol{r}|\boldsymbol{s})$ は劣化過程を表している．これは画像への攻撃が AWGN である場合，(8) より，

$$P(\boldsymbol{r}|\boldsymbol{s}) = \prod_{\mu=1}^{N} P(r_\mu|\boldsymbol{s}) \tag{15}$$

$$= \frac{1}{(2\pi\sigma_0^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma_0^2}\sum_{\mu=1}^{N}\left(r_\mu - \sum_{i=1}^{K}\xi_i^\mu s_i\right)^2\right], \tag{16}$$

となる．ここで，事後確率 $P(\boldsymbol{s}|\boldsymbol{r})$ がギブス分布に従うとすると，

$$P(\boldsymbol{s}|\boldsymbol{r}) = \frac{1}{Z}\exp\left[-\beta_0 H\left(\boldsymbol{s}\right)\right], \tag{17}$$

$$Z = \sum_{\boldsymbol{s}} \exp\left[-\beta_0 H\left(\boldsymbol{s}\right)\right], \tag{18}$$

と表すことができる．ただし，$\beta_0 = N/\sigma_0^2$ とおく．β_0 は逆温度と呼ばれる．事後確率の最大化は，(17) より，エネルギー関数 $H(\boldsymbol{s})$ の最小化と等しいことが分かる．$H(\boldsymbol{s})$ は，

$$H\left(\boldsymbol{s}\right) = \frac{1}{2}\sum_{i=1}^{K}\sum_{j=1}^{K} J_{ij}s_i s_j - \sum_{i=1}^{K} h_i s_i, \tag{19}$$

となる．ただし，

$$J_{ij} = \frac{1}{N}\sum_{\mu=1}^{N}\xi_i^\mu \xi_j^\mu, \quad h_i = \frac{1}{N}\sum_{\mu=1}^{N}\xi_i^\mu r_\mu, \tag{20}$$

である．

得られた事後確率より，事後確率が最大となるメッセージを推定すればよい．最大事後確率（MAP）推定や周辺事後確率最大化（MPM）推定により，ベイズ最適なメッセージを推定することができる．

$$\text{MAP}：\hat{\boldsymbol{s}} = \arg\max_{\boldsymbol{s}} P\left(\boldsymbol{s}|\boldsymbol{r}\right), \tag{21}$$

$$\text{MPM}：\hat{s}_i = \arg\max_{s_i} \sum_{\boldsymbol{s}\setminus s_i} P\left(\boldsymbol{s}|\boldsymbol{r}\right), \tag{22}$$

ここで，$\sum_{\boldsymbol{s}\setminus s_i}$ はあらゆるメッセージ $\boldsymbol{s}$ の中で s_i 以外の要素に関して和を取ることを表す．MAP 推定 (21) は全ての状態から，最も可能性が高い解の組合せを選ぶ推定である．一方，MPM 推定 (22) は，状態の 1 要素ずつに対し，確率の高い値を選ぶ推定である．これらのベイズ最適な復号方式は，CDMA の場合と同様に NP 困難である [8]．そこで，系の平衡状態に到達するような準最適な復号アルゴリズムを考える必要がある．これまでに，原画像が既知の場合の電子透かしについて，決定論的な復号アルゴリズムが提案されている [19]．エネルギー関数が多峰性をもつ場合，確率を導入することによって，極値にとどまることなく最適値に向かうことが期待できる．また，非同期方式を取り入れることで，推定メッセージにおいての振動解の発生を抑えることができると考えられる [20]．

3.2 絶対零度マルチ復号法

ベイズ推定をもととする準最適な復号アルゴリズムは，エネルギー関数 (19) より導くことができる．(19) より，s_i に対してこう配方向下向を求めると，

$$-\frac{\partial H\left(\boldsymbol{s}\right)}{\partial s_i} = h_i - \sum_{j\neq i}^{K} J_{ij}s_j, \tag{23}$$

となる．(23) より，全てのメッセージの推定値を用いながら，各メッセージを同時に再推定する手法をマルチステージ復号と呼ぶ [3], [19]．従来の決定論的な復号アルゴリズムでは，こう配方向下向に単調に状態を繰り返し更新していく．$\hat{s}_i^t$ を用いることで，メッセージの推定値 $\hat{s}_i^{t+1}$ は，

$$\hat{s}_i^{t+1} = \text{sgn}\left(h_i - \sum_{j\neq i}^{K} J_{ij}\hat{s}_j^t\right), \tag{24}$$

と求めることができる．ただし，J_{ij} と h_i は (20) で与えられる．ここで，初期の推定メッセージ $\hat{s}_i^0$ の値は，シングル復号器 (11) により得られた値とする．

このような決定論的な復号アルゴリズムを用いた手法を，絶対零度復号と呼ぶことにする．絶対零度復号ではエネルギーが低い解へと常に遷移するため，局所解にとどまってしまい，最適解が得られない可能性を含んでいる．また，この手法は全てのメッセージを同時に更新するため同期型の復号法である．

3.3 非同期型絶対零度復号法

前述の同期型絶対零度復号は，更新ステージごとに全てのメッセージを同時に推定した．この方法では，更新する過程で振動解が発生し，最適解に収束しない場合が起こり得る．この問題を解決するため，非同期更新を導入する．非同期方式では，1 度につきランダムに選ばれた一つのメッセージのみを推定し，他のメッセージは推定せずに更新を行う方式である．そのため，振動解の発生を抑え，最適解に収束することが期待できる．本論文では，全メッセージの推定回数が同じになるように復号していく．

非同期方式の推定メッセージの更新アルゴリズムは，次のようになっている．

（1） 初期ステージ（$t = 0$）では，シングル復号により，全てのメッセージを推定する．後に，ステージ t を一つ増やす．

（2） 推定していないメッセージを対象として，一様ランダムに一つのメッセージを選ぶ．選ばれたメッセージの番号を i 番目とする．i 番目のメッセージの推定値 $\hat{s}_i$ を，

$$\hat{s}_i = \mathrm{sgn}\left(h_i - \sum_{j\neq i}^{K} J_{ij}\hat{s}_j\right), \tag{25}$$

により更新する．

（3） 全てのメッセージが 1 回ずつ更新されるまで，（2）を繰り返す．その後ステージを一つ上げる．

（4） ステージ t_F まで繰り返す．

3.4 同期型有限温度復号法及び非同期型有限温度復号法

絶対零度復号では，エネルギー関数の値が常に減少するように，メッセージを推定した．本論文で提案する確率的な復号アルゴリズムでは，エネルギー関数の値が増加することも確率的に許容する方法である．(23) より，ステージ t における内部状態の値を，

$$u_i^t = h_i - \sum_{j\neq i}^{K} J_{ij}\hat{s}_j^t, \tag{26}$$

と置く．この内部状態の大きさに基づいて，確率的にメッセージを推定する．同期方式の場合には，各推定メッセージを同時に，

$$P(\hat{s}_i^{t+1} = \pm 1 | u_i^t) = \frac{1}{2}\left(1 \pm \tanh\frac{u_i^t}{T}\right), \tag{27}$$

で確率的に決定する．ここで，T は温度と呼ばれる正のパラメータである．u_i^t の値が大きい場合 $\hat{s}_i^{t+1} = 1$ となる確率は大きく，小さい場合 $\hat{s}_i^{t+1} = 1$ となる確率は小さくなる．

温度パラメータ T が小さい場合，より決定的に推定メッセージを更新するようになり，$T \to 0$ の極限においては，$P(\hat{s}_i^t = 1 \mid u_i^t)$ は前述の決定論的な復号アルゴリズムと一致する．この手法を同期型有限温度復号と呼ぶ．

また，非同期方式と確率的手法を共に取り入れる復号法が考えられる．この非同期型有限温度復号法の場合では，非同期型絶対零度復号に対して手順（2）だけ異なり，一度につき一つのメッセージのみを選び出し，(27) と同様の考え方で，確率的にメッセージを推定していく．

確率を導入したことにより，エネルギー関数の最小解に近づいた際も確率的に離れてしまうことが起きる．性能評価では，推定メッセージの期待値 $\langle s_i^t \rangle$ が利用される．しかしながら，何度も試行し，その期待値を求めるのでは，時間がかかりすぎてしまい実用的ではない．そこで，実際のメッセージの推定では，メッセージごとにその時間平均を求め，その値より推定値を決定する．すなわち，最終的な推定メッセージ $\langle s_i^t \rangle$ は，時間平均を用いて，

$$\langle s_i^t \rangle = \mathrm{sgn}\left(\frac{1}{L}\sum_{\tau=t-L+1}^{t} \hat{s}_i^\tau\right), \tag{28}$$

により決定する．ただし，L は時間平均に用いる長さを表す．

決定論的な復号アルゴリズムにおいて，解が振動することが知られている [19]．また，確率の導入の有無での性能の違いを比較するため，決定論的な復号アルゴリズムにおいても，時間平均を導入し，(28) で推定値を求めることにする．

4. 温度パラメータと有限温度推定

前述の有限温度復号において，温度 T はエネルギーが増大する方向への遷移確率に重大な影響を与えるパラメータである．有限温度復号を扱う上で，温度について考える必要がある．温度スケジューリングに関して，特定の温度を決めて温度固定で更新する方法や，焼きなまし法（SA）[21]～[23] のように冷却を導入する方法がある．温度固定の手法において，スペクトル拡散透かしモデルでは，最適温度は攻撃ノイズの分散に依存し，σ_0^2/N に等しいときが最適と考えられる．そこで，温度固定の手法は最適温度 $T_c = \sigma_0^2/N$ を温度パラメータに用いる．

4.1 焼きなまし法

最適化問題に対する確率を用いたアルゴリズムの一つに焼きなまし法（SA）[21] がある．SA は遷移確率 (27) の温度パラメータの値を徐々に減少させていく方法である．SA は，初期段階において大域的な解空間を探索することが可能である．温度スケジューリングによって，冷却していくことにより，エネルギーが低い状態を徐々に優先して選ぶようになり，最終的には，その近傍で最も良い解に収束していく．

一般的に SA は目的関数の大域的最適解を求めるよい近似アルゴリズムとして知られている．解の状態が有限である任意の問題に SA を適用する場合は，最適解の漸近収束性が保証されている対数型 SA 以上に緩慢に時間をかけて冷却することで，解空間を十分に探索でき，大域的最適解を得る確率を理論上 1 に近づけられることが知られている [22], [23]．しかしながら，対数型では収束に膨大な時間を要するため，本論文では温度パラメータを指数関数的に減少させる指数型

SA [24] を採用する．すなわち，温度を，

$$T_{t+1} = \gamma T_t \ , \tag{29}$$

で更新する．ここで，γ は 1 未満の正の数である．初期温度 T_0 は局所解に陥らないよう十分に高温とする [25]．本論文では，初期温度 T_0 を $T_0 = 4T_c$ に設定した．温度の変化を図 2 の曲線 SA に示す．

4.2 SA と有限温度 SA

SA をどのように導入するかを述べる．前述の有限温度復号に対して，SA では各メッセージ s_i^t の推定を一通り行い，ステージが一つ増えるたびに，温度パラメータを (29) で更新していく．組合せ最適化問題等では，一般に絶対零度まで冷却する手法により解が求まる．これを従来型 SA と呼ぶ．

一方，スペクトル拡散モデルの復号問題などでは，通信路ノイズがあり，西森温度と呼ばれる最適温度が存在する．西森温度で復号することによって，理論的に最適解が求まることが知られている [11], [26]．従来型 SA と同様に，西森温度固定ではなく，高温から西森温度へ向けて冷却しながら復号することで解が改善する可能性がある．Fielding [24] は，冷却の途中で推定を止めることにより，良い解が得られることを示している．そこで，スペクトル拡散モデルの復号アルゴリズムにおいて，従来型 SA に対して最適な有限温度 T_c まで冷却し，それ以後はその温度を維持するように修正した有限温度 SA を検討する．この手法の温度 T の推移を図 2 の finite-SA に示す．(27) により，推定メッセージを更新しながら，温度を下限温度 T_c まで冷却した後，その温度を保ちながら推定を続ける．すなわち，T_c に到達してからは定温の有限温度復号と同様の推定を行う．有限温度復号に対し，温度スケジューリングの導入による差異を見るため，下限温度は有限温度復号と同じく，西森温度 $T_c = \sigma_0^2/N$ としている．

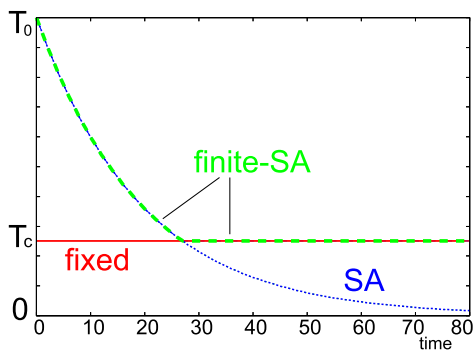


図 2　温度スケジューリング
Fig. 2　Temperature scheduling.

5. 計算機シミュレーションによる評価

提案した各復号法を用いてメッセージ推定した結果を評価する．メッセージの性能評価にビット誤り率を用いる．ビット誤り率 P_b は，

$$P_b = \frac{1-M}{2} \ , \ M = \frac{1}{K}\sum_{i=1}^{K} s_i \hat{s}_i, \tag{30}$$

で表される．ここで，M は真のメッセージ s_i と推定メッセージ $\hat{s}_i$ の間のオーバラップ，または，一致度を表す．

評価に用いた画像は，SIDBA 標準画像の 256×256 のグレースケール画像である．その中でも，自然画像の例として MOON を，人工画像の例として TITLE の結果を述べる．人工画像に透かしを埋め込む場合には輝度値制限 (5) の影響を強く受けると考えられる．これら画像に拡散符号長を $N = 256$ として，透かし情報を画像に埋め込んだ．その画像に，攻撃ノイズとして加法的白色ガウス雑音を与えた．ガウス雑音の大きさは，$N(0, \sigma_0^2)$ である．ノイズの大きさの指標として，1 ビット当りの信号電力と雑音密度の比 E_b/N_0 がある．これは，

$$\frac{E_b}{N_0} = 10\log_{10}\left(\frac{1}{2\sigma_0^2}\right) \ \text{[dB]}, \tag{31}$$

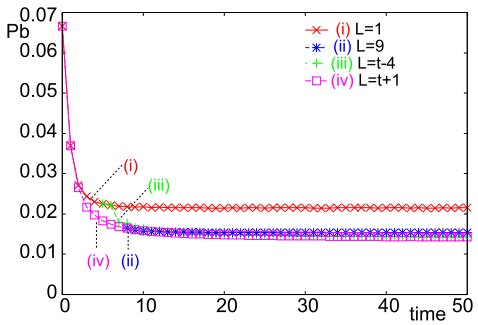
で求められる．

5.1 時間平均の取り方

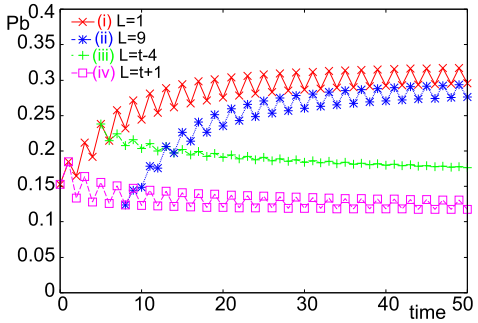
(28) において，時間平均を用いて最終的なメッセージを推定することを述べた．このとき，どのくらいの時間平均を求めればよいかが問題になる．まずはじめに，どのような時間平均のとり方が良いかを検討する．本論文では，次の方法を検討した．

（i）　$L = 1$：時間平均しない方法
（ii）　$L = 9$：過去 9 時刻の時間平均を用いる方法
（iii）　$L = t - 4$：時刻 $\tau = 5$ から $\tau = t$ までの時間平均を用いる方法
（iv）　$L = t + 1$：時刻 $\tau = 0$ から $\tau = t$ までの全時間平均を用いる方法

画像 MOON に透かしを埋め込み，同期型有限温度マルチ復号で取り出した場合の各方法における平均ビット誤り率（1000 回平均）の時間発展を図 3 に示す．横軸は時刻を表し，縦軸は平均ビット誤り率 P_b である．時刻 $t = 0$ の平均ビット誤り率はシングル復

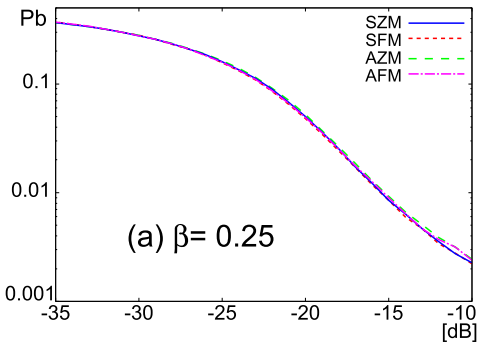


(a) $\beta = 0.25$

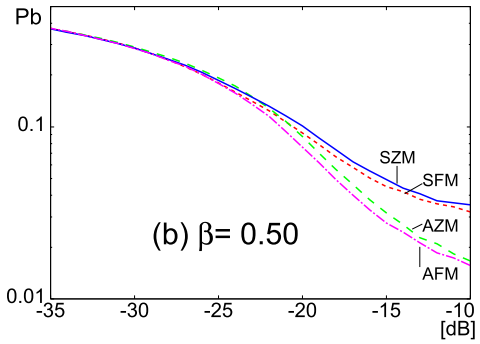


(b) $\beta = 0.75$

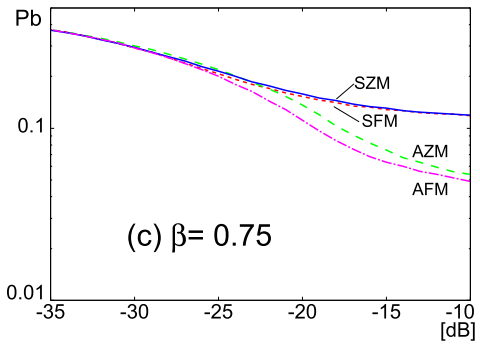
図 3　各時間平均の取り方におけるビット誤り率の時間発展
Fig. 3　Time evolutions of bit error rate P_b for each time average methods.



(a) $\beta = 0.25$



(b) $\beta = 0.5$



(c) $\beta = 0.75$

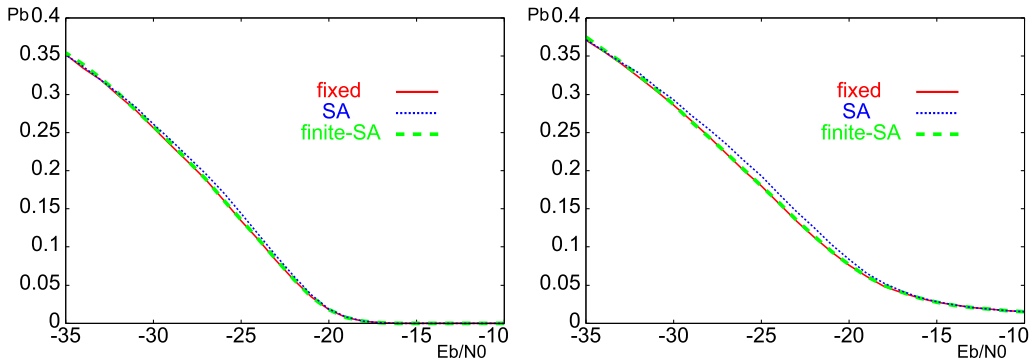
図 4　各種アルゴリズムを用いた手法のビット誤り率
Fig. 4　BERs for methods with each algorithm.

号器 (9) により求めた結果である．また，ガウス雑音の大きさは $\sigma_0^2 = 50$（−20 dB）とした．各線はそれぞれ，（i）時間平均なし（$L = 1$）と，（ii）過去 9 時刻の時間平均（$L = 9$），（iii）$\tau = 5$ 以降の時間平均（$L = t - 4$），（iv）全時間平均（$L = t + 1$）により推定したメッセージの平均ビット誤り率である．

図 3 (a) は埋込率が $\beta = K/N = 0.25$ の場合であり，(b) は $\beta = 0.75$ の場合である．埋込率 β によらず，時間平均なしに比べ，時間平均を取り入れることで，ビット誤り率を低減できることが分かる．（ii）過去 9 時刻の時間平均や（iii）初期の推定値を無視した平均と，（iv）全時間平均の平均ビット誤り率を比べてみると，埋込率が小さいときには，これらに違いは特に見られない．しかしながら，埋込率が大きいときには，全時間平均が最も性能がよい．この結果から，時間平均のとり方は，時刻 $t = 0$ からの全ての時間平均をとった全時間平均の方法がよい．以後の結果では，$L = t + 1$ とする．

5.2　アルゴリズムの比較

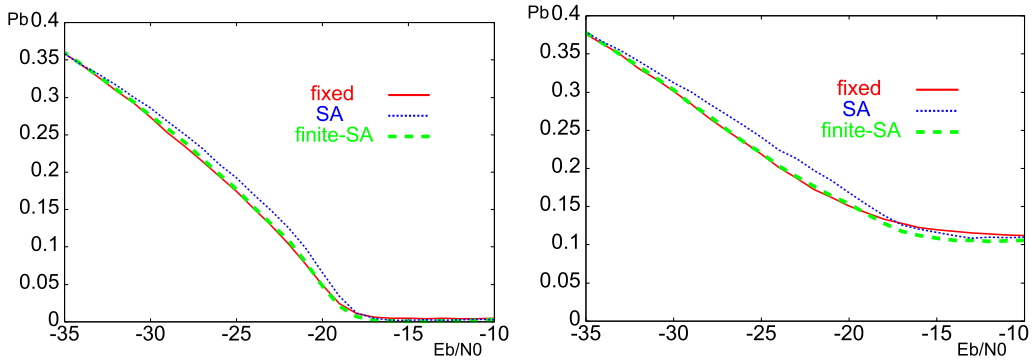
攻撃ノイズの大きさに対するビット誤り率で復号アルゴリズムを評価する．まず，同期型絶対零度（SZM），非同期型絶対零度（AZM），同期型有限温度（SFM），非同期型有限温度（AFM）の 4 手法の性能を比較する．画像 TITLE に透かしを埋め込み，加えるガウス雑音の大きさを −35 dB から −10 dB まで変化させたときの，4 手法のビット誤り率 P_b を図 4 に示す．時刻 $t = 80$ のときのビット誤り率を求め，300 回試行した平均値で示している．全ての方法で時間平均を採用した．メッセージのビット数を $K = 64, 128, 192$ とする．



(a) MOON　(b) TITLE

図 5　各温度スケジュールの復号性能（埋込率 $\beta = 0.50$）

Fig. 5　Performance for SA decoders with different temperature schedules (embedding rate $\beta = 0.50$).



(a) MOON　(b) TITLE

図 6　各温度スケジュールの復号性能（埋込率 $\beta = 1.00$）

Fig. 6　Performance for SA decoders with deferent temperature schedules (embedding rate $\beta = 1.00$).

それぞれ，(a) $\beta = 0.25$，(b) $\beta = 0.50$，(c) $\beta = 0.75$ の場合を示す．埋込率が小さい場合では，それぞれの復号によるビット誤り率に大きな違いは見られない．しかしながら，埋込率が大きくなると，非同期型の復号アルゴリズムの方がビット誤り率が小さくなり，絶対零度と有限温度では，有限温度復号の方がビット誤り率が小さくなる．

5.3　温度スケジュールによる比較

前節により，有限温度のアルゴリズムを取り入れた方が性能が上がることが分かった．次に，温度スケジューリングが性能にいかなる影響を与えるかを検証する．

ノイズの大きさを $-35\,\mathrm{dB}$ から $-10\,\mathrm{dB}$ まで変化させたときのビット誤り率 P_b を定温の有限温度復号と，従来型の SA，及び，有限温度 SA で求めた．更新ステージ数 $t = 120$ のときのビット誤り率を計算し，300 回試行した平均値で求めている．全て非同期方式に統一している．図 5 に，メッセージのビット数 $K = 128$，埋込率 $\beta = 0.50$ の場合のビット誤り率を示す．また，図 6 に，$K = 256$，$\beta = 1.00$ の場合の結果を示す．それぞれ，画像 (a) MOON と (b) TITLE を用いた結果を表している．埋込率が $\beta = 0.50$ の場合は，有限温度復号と有限温度 SA がほぼ同性能であり，従来型 SA はそれら二つのアルゴリズムよりビット誤り率が高い．また，埋込率が $\beta = 1.00$ の場合においても，従来型 SA よりも有限温度 SA の方が性能がよい．また，定温の有限温度復号はノイズが大きい場合には有限温度 SA と同じ性能であった．ただし，ノイズが小さい場合，有限温度復号は有限温度 SA 及び従来型 SA よりも性能が悪くなる場合がある．この現象は特に TITLE において顕著に現れる．ノイズが小さい場合には，輝度値制限 (5) の影響 η_μ が強く現

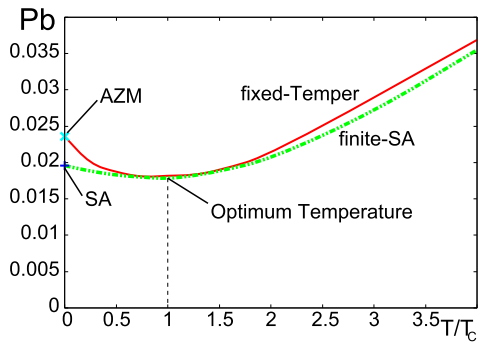


図 7　温度パラメータに対する有限温度復号のビット誤り率
Fig. 7　BER of decoder with fixed finite temperature.

れ，**2.2** で述べたように，ノイズの分散が η_μ により大きくなったため，有限温度復号の性能が十分にでなかったと考えられる．一方，有限温度 SA では T_c より大きい温度を経由するため，有限温度よりも良い結果を与えた．

5.4　最適温度と復号性能

本論文では，復号に最適である温度 $T_c = \sigma_0^2/N$ を既知とした．温度パラメータは復号性能に関わる．有限温度復号と有限温度止め SA において，西森温度に固定せず，様々な温度で復号したときのビット誤り率を図 7 に示す．画像は MOON を使用し，埋込率 $\beta = 0.50$，攻撃の大きさを $-20\,\mathrm{dB}$（$T_c = 0.195$）として求めている．この結果からも，温度パラメータ T の最適値は西森温度 $T_c = \sigma_0^2/N$ であることが確認できる．ただし，攻撃なしでは温度 0 が最適となり，SA と有限温度止め SA は一致する．また，温度パラメータが西森温度 T_c から外れた場合には，温度固定よりも SA を導入した復号法の方が性能よい．TITLE のように，輝度値制限の影響 η_μ によって，西森温度 T_c が σ_0^2/N より大きくなる場合や，T_c が未知のモデルでは，固定温度復号よりも有限温度止め SA を用いる方が，復号性能が落ちにくいことが分かる．

6. むすび

CDMA や拡散符号を用いた電子透かしのモデルは，スペクトル拡散モデルとして統一的に扱うことができる．ここでは，電子透かしを例にして復号アルゴリズムを検討した．その結果は CDMA モデルでも同様に成り立つと考えられる．スペクトル拡散モデルに対して，ベイズ推定による最適な復号から導出された，準最適な解を求める復号が提案されている [19]．このマルチ復号には，決定論的なダイナミックスが用いられている．

本論文では，スペクトル拡散モデルのエネルギーが増加することを確率的に許容する有限温度復号を提案した．また，メッセージの同期的な更新に対して，非同期的な更新を導入した．非同期では同期に比べ，振動解が生じにくい．有限温度復号については，エネルギー関数が多峰性の場合でも，極値にとどまることなく最適値に向かうことが期待できる．確率を導入することで，最適解に近づいた後も，解から離れてしまう可能性を生じる．この解の振れ幅を軽減するために時間平均を検討し，比較実験で最も性能が高かった，初期から今現在までの情報を全て使う全時間平均を採用した．有限温度による復号では，状態遷移に関与する温度パラメータの扱いが問題になる．温度については，初期から温度固定で更新する手法の他に，温度を高温から徐々に下げていく焼きなまし（SA）法 [21] が知られている．本論文では，温度固定復号と，絶対零度まで冷却する従来型 SA に加え，最適温度で冷却を止めてそれ以後はその温度を維持するように修正した有限温度 SA を検討した．

計算機シミュレーションの結果，非同期有限温度復号が従来の決定論的手法に比べ，ビット誤り率が低く，より良い復号が可能であることを示した．有限温度復号においては，最適温度 T_c の情報を使う場合，絶対零度まで冷却する従来の SA よりも，固定温度復号や有限温度止め SA の方が性能が良くなることが分かった．また，埋込誤差の影響が無視できない場合や，最適温度が未知の場合は，温度固定よりも SA を導入した方が良いことが分かった．その結果，有限温度止め SA がこれらの手法の中で最も復号性能が良いことが分かった．

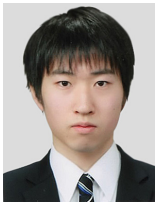
謝辞　本研究の一部は文部科学省科学研究費補助金（若手研究 (B) No. 21700255）の補助を受けて行われた．本研究では山口大学計算機クラスターシステムを利用した．

文　献

[1] A.J. Viterbi, “Spread spectrum communications-myths and realities,” IEEE Commun. Mag., vol.17, no.3, pp.11–18, 1979.
[2] M.K. Varanasi and B. Aazhang, “Multistage detection in asynchronous code-division multiple-access communications,” IEEE Trans. Commun., vol.38, no.4, pp.509–519, 1990.
[3] M.K. Varanasi and B. Aazhang, “Near-optimum de-

tection in synchronous code-division multiple-access systems," IEEE Trans. Commun., vol.39, no.5, pp.725–736, 1991
[4] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," IEEE Int. Conf. Image Processing, vol.3, pp.243–246, 1996.
[5] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol.6, no.12, pp.1673–1687, 1997.
[6] I.J. Cox, M. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed., Morgan Kaufmann, 2007.
[7] N. Hayashi, M. Kuribayashi, and M. Morii, "Collusion-resistant fingerprinting scheme based on the CDMA-technique," LNCS, vol.4752, pp.28–43, 2007.
[8] S. Verdú, "Computational complexity of optimum multiuser detection," Algorithmica, vol.4, no.3, pp.303–312, 1989.
[9] T. Tanaka, "Statistical mechanics of CDMA multiuser demodulation," Europhys. Lett., vol.54, pp.540–546, 2001.
[10] T. Tanaka, "A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors," IEEE Trans. Inf. Theory, vol.48, no.11, pp.2888–2910, 2002.
[11] H. Nishimori, Statistical Physics of Spin Glasses and Information Processing: An Introduction, Oxford University Press, Oxford, U.K., 2001.
[12] T. Tanaka and M. Okada "Approximate belief propagation, density evolution, and statistical neurodynamics for CDMA multiuser detection," IEEE Trans. Inf. Theory, vol.51, no.2, pp.700–706, 2005.
[13] D. Divsalar, M.K. Simon, and D. Raphessi, "Improved parallel interference cancellation for CDMA," IEEE Trans. Commun., vol.46, no.2, pp.258–268, 1998.
[14] M. Sawahashi, H. Andoh, and K. Higuchi, "Interference rejection weigt control for pilot symbol-assisted coherent multistage interference canceller in DS-CDMA mobile raido," IEICE Trans. Fundamentals, vol.E81-A, no.5, pp.957–972, May 1998.
[15] 水谷　智，田中利幸，岡田真人，"部分干渉除去によるマルチステージ検出器の性能改善，" 信学論（A），vol.J87-A, no.5, pp.661–671, May 2004.
[16] P.H.W. Wong, C. Au, and Y.M. Yeung, "A novel blind multiple watermarking technique for images," IEEE Trans. Circuits Syst. Video Technol., vol.13, no.8, pp.813–830, 2003.
[17] T. Fujita, M. Yoshida, and T. Fujiwara, "A new scheme to realize the optimum watermark detection for the additive embedding scheme with the spatial domain," IEICE Trans. Fundamentals, vol.E90-A, no.1, pp.216–225, Jan. 2007.
[18] 宮崎明雄，"電子透かし検出方法のベイズ推定に基づく改良，" 信学技報，SIP2007-41, 2007.
[19] K. Senda and M. Kawamura, "Statistical-mechanical approach for multiple watermarks using spectrum spreading," LNCS, vol.5973, pp.231–247, 2010.
[20] N. Teranishi and M. Kawamura, "Asynchronous stochastic decoder for spread spectrum digital watermarking," 7th Inter. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2011), Dalian, China, 2011.
[21] S. Kirkpatrick, C.D. Gelatt, and M.P. Vecchi, "Optimization by simulated annealing," Science, vol.220, pp.671–680, 1983.
[22] S. Geman and D. Geman, "Stochastic relaxation, gibbs distributions, and the Bayesian restoration of images," IEEE Trans. Pattern Anal. Mach. Intell., vol.PAMI-6, no.6, pp.721–741, 1984.
[23] E. Aarts and J. Korst, Simulated Annealing and Boltzmann Machines, John Wiley & Sons, 1989.
[24] M. Fielding, "Simulated annealing with an optimal fixed temperature," SIAM J. Optimization, vol.11, no.2, pp.289–307, 2000.
[25] S. White "Concepts of scale in simulated annealing," Proc. IEEE Intl. Conf. Comp. Des. (ICCD), pp.646–651, 1984.
[26] H. Nishimori, "Internal energy, specific heat and correlation function of the bond-random ising model," Progress of Theoretical Physics, vol.66, no.4, pp.1169–1181, 1981.

（平成 24 年 11 月 15 日受付，25 年 2 月 20 日再受付）



寺西　直緒　（学生員）

平 23 山口大・理・物理・情報科学卒．平 23 同大大学院理工学研究科博士前期課程入学，現在に至る．平 23 電気・情報関連学会中国支部連合大会奨励賞受賞．

川村　正樹　（正員）

平 6 筑波大・第三・情報卒．平 8 同大大学院修士課程了．平 11 同大学院博士課程了．博士（工学）．同年山口大・理助手．平 15 同大・理講師．平 23 同大大学院・理工准教授，現在に至る．ニューラルネットワーク，記憶に関する研究，及び，CDMA や電子透かしに関する数理モデルの研究に従事．EMM 研究会幹事補佐．平 15 回路とシステムワークショップ奨励賞受賞．日本神経回路学会，日本物理学会，IEEE 各会員．