Wireless Steganography using a Spectrum Spreading Technique

Akihito TAKAI*, Hideichi SASAOKA* and Hisato IWAI*

(Received March 10, 2014)

As a countermeasure to information tapping in wireless communications, a wireless steganography technique was proposed and the fundamental performance of the technique was evaluated. In the technique, the existence of the transmitted confidential signal is hidden to the anyone other than the legitimate receiver. In this paper we propose a new wireless steganography technique using the spectrum spreading approach. We evaluate the transmission performance of the embedded secret signal and the anti-attacking performance against eavesdroppers by computer simulation. As a result of the evaluation, we clarify the requirements of the various parameters of the technique by which signal detection by third-party eavesdroppers is made almost impossible.

Key words: wireless steganography, spread spectrum (SS), cover signal, secret signal

キーワード： 無線ステガノグラフィ，スペクトル拡散，カバー信号，秘匿信号

スペクトル拡散信号を用いた無線ステガノグラフィ方式の検討

高井　昭人，笹岡　秀一，岩井　誠人

1. まえがき

近年，電波を用いた無線通信セキュリティ技術が発展している．その中でも情報ハイディングの概念を用いた無線信号秘匿が盗聴や妨害の脅威も小さく注目されている．これまで，無線通信のセキュリティ対策として，電波伝搬の可逆性やマルチパスフェージングの時間場所依存性などの電波伝搬の特徴を利用し，受信信号強度などの伝搬路情報に基づいて秘密鍵を生成・共有し暗号通信を行う方式や，盗聴通信路モデルにおける通信容量の差に基づく秘密通信方式などが提案されている [1]．これらの方式では，電波伝搬路を暗号として有効活用することにより通信の当事者以外の第三者に対する通信内容の秘密性を十分に確保でき，セキュリティ上安全な通信を行うことが可能であるが，第 3 者でも暗号通信の行為のみを検出することは可能である．

無線通信における通常の伝送信号に対して，通常では雑音のような自然現象と識別が困難になるような信号を埋め込んで送受信を行い，埋め込んだ信号における通信行為の秘匿を実現する．無線伝送における変調信号の埋め込みによるステガノグラフィと考えることが可能であり，この方式を無線ステガノグラフィと呼ぶ．

無線ステガノグラフィでは，信号秘匿の基本原理や秘匿信号の存在を推定する攻撃に対する耐性の原理のような基本的な特性は研究されている [2]．し

* Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6267, Fax: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

かしながら，秘匿信号の検出の危険性は，十分に解明されていない．本稿では，この問題に焦点をあて，コンピュータシミュレーションを通じて盗聴による検出特性を評価する．

2. 無線ステガノグラフィ

2.1 ステガノグラフィの概要

ステガノグラフィとは，通信の当事者間でのみ伝達したい情報に，別のディジタルデータを媒体とし，そのデータを加工することによって当事者以外の第三者には，データ通信行為自体を知られることなく情報を秘匿して伝達する技術である [3-6]．

ステガノグラフィでは，媒体となるデータはカバーデータと呼ばれ，カバーデータを改変して別の情報を加えることを埋め込みという．また，当事者以外には秘匿にしておく情報のことを埋め込みデータと呼び，埋め込み処理を行った後のカバーデータをステゴデータと呼ぶことがきめられている [7]．

ステガノグラフィの構成を Fig. 1 に示す．画像などをカバーデータとし，そこに文字列などのデータを埋め込むステガノグラフィ技術である．送信側では，埋め込みデータを，ステゴ鍵を用いてカバーデータに埋め込む処理を行っている．一方，受信側では，受信したステゴデータから情報の抽出処理を行い埋め込みデータを取り出している．なお，ステガノグラフィにおいては，埋め込みデータがカバーデータのどの部分に埋め込まれているかが第三者にわからないようにするのが原則である．

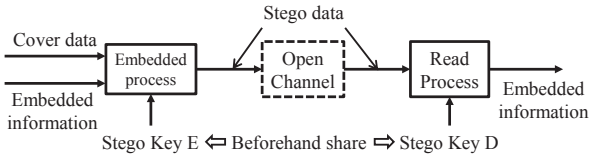


Fig. 1. Composition of steganography.

2.2 無線ステガノグラフィの概念

無線ステガノグラフィとは，ステガノグラフィにおけるデータを信号に置き換えたものである．通常の情報で変調された無線通信信号をカバー信号とし，秘密情報で変調された埋め込み信号をカバー信号に埋め込み，ステゴ信号とする．正規者 A（送信側）では，アンテナ送信前に埋め込み処理が行われ，ステゴ信号が送信される．正規者 B（受信側）では，カバー信号や埋め込み処理内容が既知などの前提の下で，ステゴ信号から埋め込み信号が分離され，埋め込み信号から秘密情報が抽出される．

攻撃者は，正規局 B と同様な手法で，利用可能な情報に基づいてステゴ解析を実施する．ステゴ解析では，はじめにカバー信号の情報を得ることを試みる．カバー信号は，通常の情報で変調された信号であり，一般に攻撃者もカバー信号の復調によりその情報を取得できるとするのが妥当である．ディジタル変調の場合，これは通常のステガノグラフィと異なり，無線ステガノグラフィの特徴的な課題である．この解決には，検知されない程度のダミー信号（かく乱信号）を付加し，さらにそのダミー信号に埋め込み信号を隠すことが必要となる．

2.3 無線ステガノグラフィの基本構成

Fig. 2 に無線ステガノグラフィの基本構成を示す．送信側では，カバー信号，ダミー信号，埋め込み信号を合成して送信する．受信側では，初めにステゴ信号を復調して得たカバー情報に基づき，変調諸元と電波伝搬特性情報から受信カバー信号（再生可能成分）を再生する．ステゴ信号からカバー信号（再生可能成分）を取り除き，残留信号を得る．この残留信号には，受信カバー信号の再生困難成分（受信カバー信号の残差成分），受信機雑音，ダミー信号，埋め込み信号が含まれる．この信号より埋め込み情報の抽出処理を行い，埋め込み情報を得る．

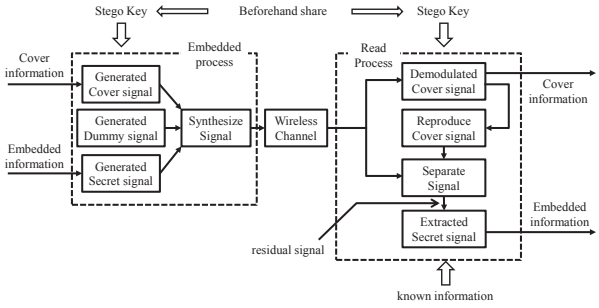


Fig. 2. Composition of wireless steganography.

2.4 盗聴者による攻撃のモデル

Fig. 3 に無線ステガノグラフィに対する盗聴者の

システムモデルを示す．この攻撃は，はじめに受信信号がステゴ信号である可能性を判別することから始められる．このため，受信信号がカバー信号として不自然でないかが試験される．次に，正規受信者と同様にカバー信号を復調して，受信カバー信号を再生することで，残留信号に対して埋め込み信号を検出するための攻撃を行う．この攻撃には，各種の信号解析（スペクトル解析，振幅分布解析，相関解析など）が考えられる．

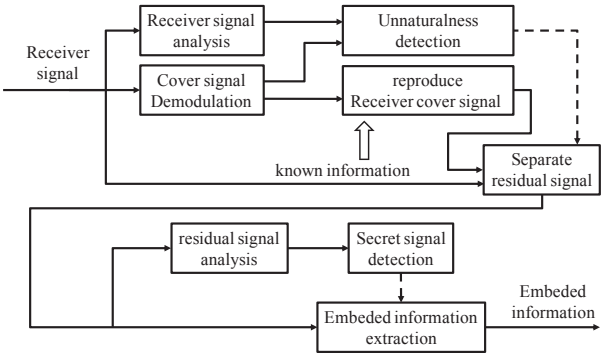


Fig. 3. Model of stego analysis.

2.5 無線ステガノグラフィが満たすべき性質

無線ステガノグラフィにおいて，カバー信号で伝送される情報（カバー情報）がごく自然なものであること，変調方式や伝送方式がごく一般的なものであることを前提とする．したがって，カバー信号自体から無線ステガノグラフィの存在を検知されないとする．その場合に，無線ステガノグラフィが満たすべき性質は，①ステゴ信号がカバー信号との差異により検知されないこと，②カバー信号を再生して得られる残留信号からダミー信号が検知されないこと，③残留信号から埋め込み信号が検知されないこと，④埋め込み信号の存在を想定した攻撃（埋め込み情報の抽出）に耐性があること，⑤正規者がダミー信号等で隠された秘匿信号から埋め込み情報を誤りなく取り出せること，などである．

3. 提案方式と提案方式に対する攻撃モデル

3.1 提案方式の構成

提案方式の構成を Fig. 4 に示す．カバー信号は，カバーデータを 1 次変調したものをスペクトル拡散したものである．スペクトル拡散信号を活用することで，処理利得が得られ，受信機雑音が大きい環境でも使用可能となる [8-9]．また，受信機雑音が大きい環境は，ダミー信号や秘匿信号を抽出しにくくするために有効である．ダミー信号としては，雑音（カバー雑音）を用いている．ダミー信号としてガウス雑音を用いたのは，受信機雑音との識別がより困難になるためである．秘匿信号は，秘匿データを 1 次変調したものをスペクトル拡散している．秘匿信号にスペクトル拡散を用いたのは，雑音の方が大きい環境において，信号の品質を維持するためである．それぞれを合成して送信する．

受信側では，カバー信号を復調しカバーデータを得るとともにカバーデータから 1 次変調とスペクトル拡散を行い，カバー信号のレプリカを作成する．このレプリカ信号を受信信号から除去することで，残留信号（受信機雑音とカバー雑音と秘匿信号の和）が得られる．この残留信号を逆拡散して 1 次復調することで秘匿データを得る．なお，無線ステガノグラフィにおいて秘匿信号の埋め込みは常時行う必要はなく，不規則に間欠的に行われ，ステガノグラフィの場合と同様に埋め込み区間は盗聴者に非公開とする．

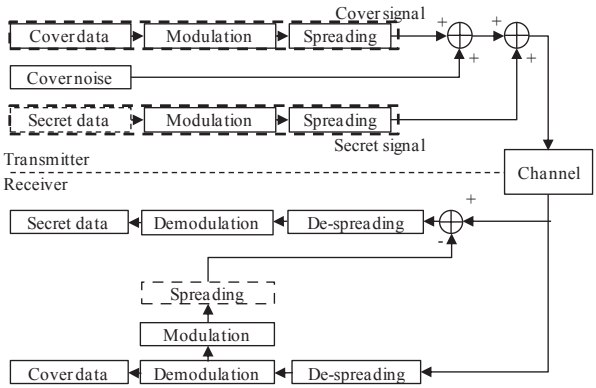


Fig. 4. Block diagram of wireless steganography.

3.2 ステゴ解析

3.2.1 盗聴者による攻撃の提案モデル

盗聴者による攻撃の提案モデルを Fig. 5 に示す．本稿では，Fig. 3 における不自然さ検出，残留信号解析についてモデル化した．盗聴者は，カバー信号

を復調しカバーデータを得るとともにカバーデータから 1 次変調とスペクトル拡散を行い，カバー信号のレプリカを作成する．このレプリカ信号を受信信号から除去することで残留信号を得る．

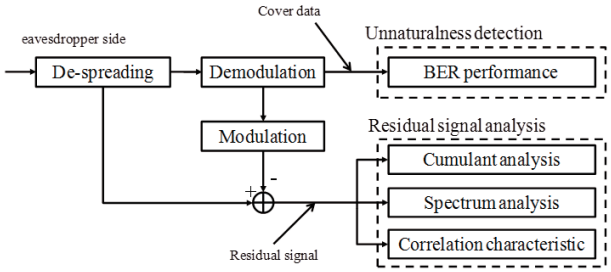


Fig. 5. Proposed model of stego analysis.

3.2.2 カバー信号の不自然さ検出

カバー信号との差異によってステゴ信号が検知又は推定されないために，ステゴ信号の BER(Bit Error Rate)特性が劣化しないことが必要である．カバー信号のみの場合に比べステゴ信号の場合では，ダミー信号と埋め込み信号の影響により，カバー情報のビット誤り率が多少とも必ず劣化する．ここで，カバー信号のみの場合のビット誤り率が攻撃者に既知と仮定する場合，ビット誤り率の僅かな差も長時間測定すれば必ず検出される．しかし，その場合でもステゴ信号がある有限区間に限定されているとすると，短区間で測定されたビット誤り率には統計的なばらつきがある．そして，ビット誤り率の分布の重なり部分が多くなると，ビット誤り率に有意な差が検出できるかが問題となる．

3.2.3 残留信号解析

残留信号解析にはキュムラント解析，スペクトル解析，同期特性により評価する．

キュムラント解析は，信号の振幅の分布による評価である．評価する尖度αの値は以下の式により与えられる．

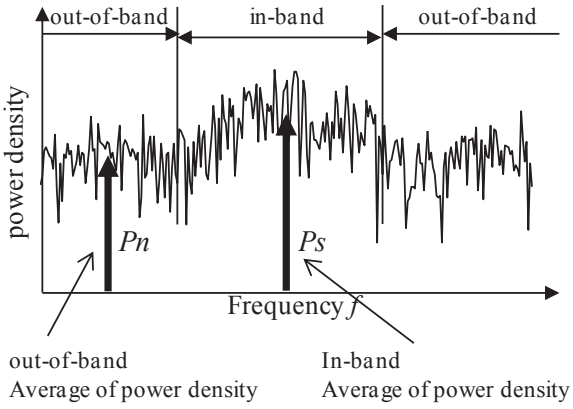
$$\alpha = r^4/(r^2)^2 \qquad (1)$$

α：Kurtosis

r：amplitude

正規分布に従う信号の場合，尖度αの値は3となる．雑音は正規分布に従うので，同様に雑音のみの信号の場合，尖度αの値は3となる．秘匿信号成分が増加すると尖度αの値はばらつくようになる．このばらつきにより秘匿信号対雑音電力比を求める．

スペクトル解析は，秘匿信号の帯域内と帯域外のスペクトル電力比による評価である．Fig. 6 にスペクトル電力比の導出を示す．信号が雑音のみの場合，スペクトル電力比は 1 となる．しかし，秘匿信号が付加された場合，帯域内電力平均が高くなるので，スペクトル電力比は 1 より大きくなる．このスペクトル電力比により秘匿信号対雑音電力比を求める．



Power ratio of Spectrum $P = \frac{Ps}{Pn}$

Fig. 6. Spectrum analysis method.

相関特性は，信号の拡散に用いる PN 符号の周期性を利用した評価である．一般に秘匿信号の方式設定が既知であるとは言えないが，ここでは盗聴者にとって，秘匿信号の PN 符号情報は既知であると仮定する．信号がスペクトル拡散信号である場合，ブロック毎に周期性が現れることは明確である．よって PN 符号によって信号との相関を求めることが可能である．盗聴者にとってブロックの送信タイミングは不確かであるとしても，各シンボル毎に相関処理を行うことは十分に考えられる．この相関係数により秘匿信号対雑音電力比を求める．

4. シミュレーションシステム

正規局の通信は Fig. 4 に従って行い，盗聴者の攻撃シミュレーションは Fig. 5 に従って行う．Fig. 7 にフレーム設定のタイムチャートを示す．カバー信

号は常に送信し続けていると想定する．カバー雑音，秘匿信号のブロック長を 200 [symbol] とし，ブロックの送信タイミングは正規局間のみ既知の情報とする．つまり，盗聴局にとって，このブロックの送信タイミングは不確かである．シミュレーション諸元を Table 1 に示す．

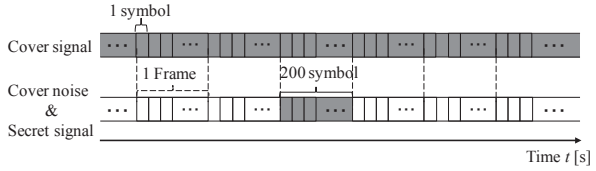


Fig. 7. Frame configuration.

Table 1. Simulation parameters.

Cover signal	Modulation: QPSK modulation Spread spectrum modulation: DS-SS Process gain: 15 [chip], 11.8 [dB] Continuous transmission
Secret signal	Modulation: QPSK modulation Spread spectrum modulation: DS-SS Block size: 200 [symbol] Secret signal to noise power ratio (before de-spreading): -14 [dB]
Cover noise	Process gain: 255 [chip], 24.1 [dB] Cover signal to cover noise power ratio (after de-spreading): 18 [dB]
Receiver noise	Cover signal to receiver noise power ratio (after de-spreading): 10 [dB]
Channel	Gaussian channel

5. シミュレーション結果

5.1 カバー信号の BER 特性

Fig. 8 にカバー雑音を付加した場合のカバー信号の BER 特性（ガウス伝送路）を示す．横軸はカバー信号対受信機雑音電力比を示し，縦軸はカバー信号の BER を示している．グラフからわかるとおり，カバー雑音を無限長区間に埋め込むと仮定すると，カバー信号対カバー雑音電力比が 20[dB]の場合でも，BER 特性は理論値と離れるため，カバー雑音の存在を認識されてしまうことが確認できる．しかし，カバー雑音を本提案方式に基づく有限長で埋め込んだ場合は，BER 特性は理論値と差異がなくなり，カバー雑音の存在が識別されにくいと考えられる．

BER 特性は無限長観測した場合の平均であり，今回のようにあるタイミングに有限長のカバー雑音と秘匿信号を送信する場合，瞬時のビット誤り個数を用いて評価を行わなければならない．なおガウス伝送路の今後のシミュレーションでは，カバー信号の BER10^3 を満たす，カバー信号対受信機雑音電力比を 10[dB]と設定する．

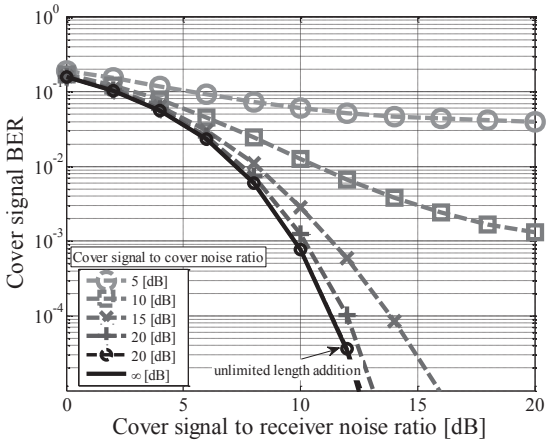


Fig. 8. Cover signal BER vs. cover signal to receiver noise ratio.

次に Fig. 9 に観測長 200[symbol]の場合のカバー信号のビットエラー個数の累積分布を示す．横軸はビット誤り個数の累積分布を示し，縦軸は 1 ブロック当りのビット誤り個数を示す．グラフの実線は，カバー信号対カバー雑音電力比に依存する．カバー信号対カバー雑音電力比を高く設定した時，ビット誤り個数は増加する．Fig. 9 の結果をビット誤り個数毎の確率分布で表した図を Fig. 10 に示す．カバー雑音を付加していない場合，最大ビット誤り個数は 4 個である．また，誤りがない場合の確率は約 70[%]である．グラフからわかるように誤り個数ごとの確率の差はあるものの，1 回のみの観測では，カバー雑音をどの程度の電力で埋め込まれているかの認識は困難である．

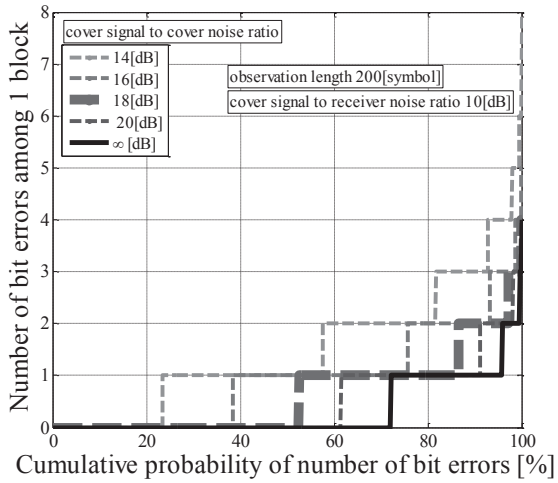


Fig. 9. Cumulative distribution of number of bit errors.

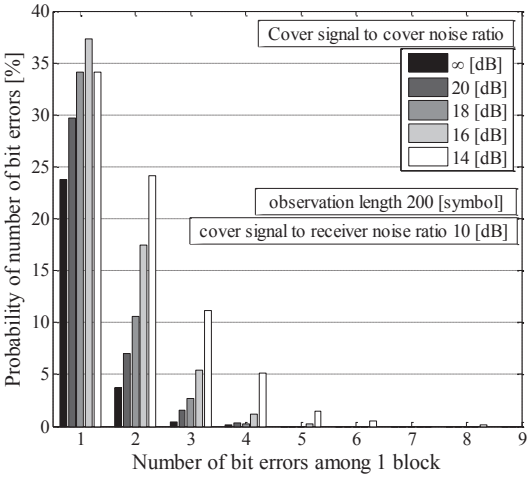


Fig. 10. Probability of number of bit errors vs. number of bit errors among 1 block.

今回は，最大個数に基づく評価を行う．カバー雑音を付加しない場合，ビット誤り個数の最大は 4 個である．カバー信号対カバー雑音電力比を 16[dB]で埋め込む場合，ビット誤り個数が 5 個出現する可能性がある．カバー雑音を付加しない場合と同様にビット誤り個数の最大が 4 個であるのはカバー信号対カバー雑音電力比が 18[dB]の場合である．よって以降のシミュレーションではカバー信号対カバー雑音電力比を 18[dB]に設定する．

5.2 残留信号解析

5.2.1 キュムラント解析

Fig. 11 に残留信号に対するキュムラント解析の結果を示す．グラフの実線は信号と雑音の加算信号の尖度αの値であり，点線は雑音のみの尖度αの値である．グラフからわかるとおり，SN 比が低くなると，秘匿信号加算時の尖度αは，雑音のみの場合の尖度αの値に近づき，SN 比が-14dB の時はほぼ同値となる．よって，キュムラント解析では，SN 比を-14dB に設定すると秘匿信号の検出は困難になることがわかった．

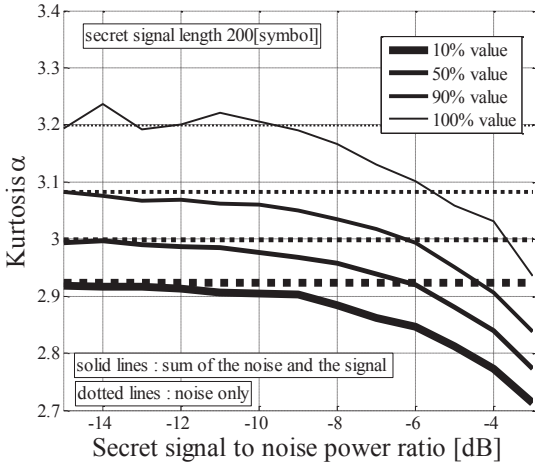


Fig. 11. Cumulant analysis of residual signal.

5.2.2 スペクトル解析

Fig. 12 に残留信号の周波数帯のスペクトル解析の結果を示す．実線は，残留信号のスペクトル電力比を示し，点線は雑音のみのスペクトル電力比を示す．キュムラント解析と同様に，SN 比が低くなると，秘匿信号加算時の電力スペクトル比は，雑音のみの場合の電力スペクトル比の値に近づき，SN 比が-14dB の時はほぼ同値となる．よって，スペクトル解析によっても，SN 比を-14dB に設定すると秘匿信号の検出は困難になることがわかった．

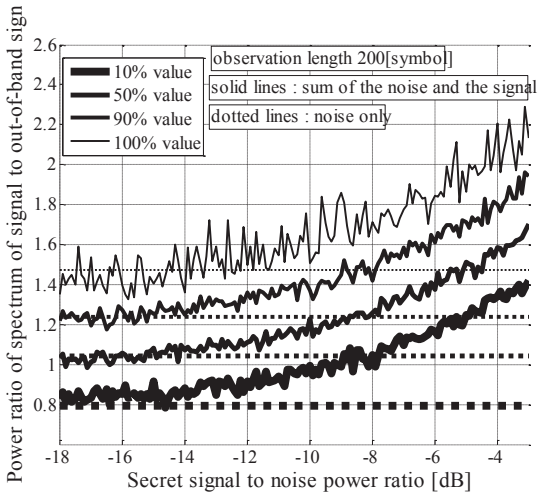


Fig. 12. Spectrum analysis of residual signal.

5.2.3 相関特性

Fig. 13 に残留信号に対する相関特性の結果を示す. 結果からわかるとおり秘匿信号対雑音電力比が-18[dB]の場合でもピークが現れ, 秘匿信号の存在検出が可能であることがわかる．しかし，この問題はPN 符号が周期的に繰り返し使用されることが原因である．PN 符号を周期的に繰り返し使用することをやめ，ほぼ同期のないロングコードから用い，さらにロングコードの初期値を盗聴者に非公開とすることで，この問題を解決できる．

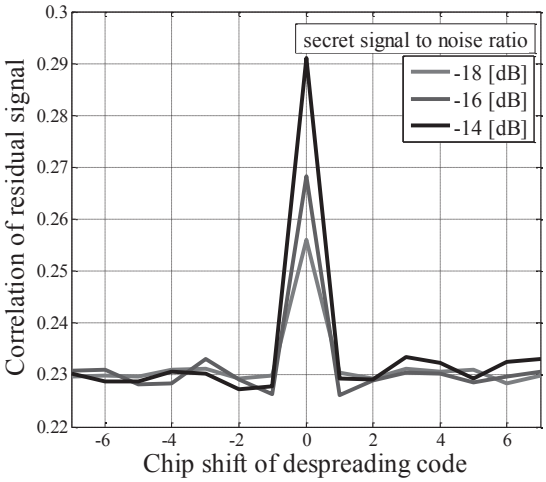


Fig. 13. Correlation characteristic of residual signal.

5.3 秘匿信号の BER 特性

秘匿信号の処理利得を増加させた場合の BER 特性の改善結果を Fig. 14 に示す．縦軸は秘匿信号の BER 特性を示し，横軸は秘匿信号対雑音電力比を示している．残留信号解析により，秘匿信号対雑音電力比を-14[dB]以下に設定しなければ, 残留信号から秘匿信号を検出されてしまう恐れがある．しかし, 設定した SN 比では，正規局間で秘匿信号の安定した抽出を行うことは困難である．よって品質改善のため，処理利得を増加させる．

グラフからわかるとおり，処理利得が 24.06[dB]で秘匿信号対雑音電力比が-14[dB]の場合, 秘匿信号の BER が 10^3 を満たすことがわかる．よって，処理利得を 24.06[dB]に設定することで，正規局間で秘匿信号の品質を保つことができることがわかった．

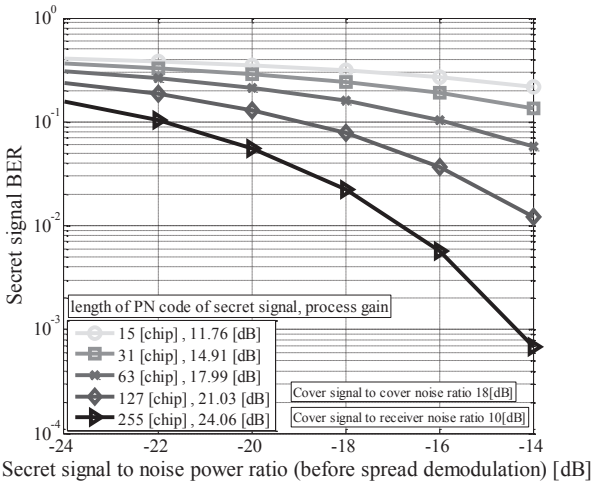


Fig. 14. Secret signal BER vs. secret signal to noise power ratio.

6. 結論

無線通信のセキュリティ技術として，カバー信号, 秘匿信号ともにスペクトル拡散信号を用いた無線ステガノグラフィ方式を提案し, 盗聴者による攻撃耐性を計算機シミュレーションで評価した．

盗聴者の攻撃（ステゴ解析）として，カバー雑音の存在検出, 秘匿信号そのものの存在検出の 2 通りを考慮した．カバー雑音の存在検出は，カバー信号伝送の BER 性能の劣化特性により評価し，秘匿信号そのものの存在検出は，キュムラント解析，受信信号と逆拡散符号とのスライディング相関のパワ

ースペクトルとピーク電力の探索により評価した．これらの評価により信号間の電力比を決定し，ステゴ解析に対する耐性の定量的評価を行った．その結果，適切な電力比を設定することで，盗聴者に知られることなく，また正規局間で安定した通信を行うことができることを確認した．

参考文献

1) R. Liu and W. Trappe, Securing Wireless Communications at the Physical Layer, (Springer, 2009).
2) 北野隆康, 岩井誠人, 笹岡秀一, “OFDM 移動通信における周波数拡散信号の埋め込みによる無線ステガノグラフィ方式”, 信学論(B), **J92-B**, 2-10, (2009).
3) 電子情報通信学会編, 情報セキュリティハンドブック, (オーム社, 東京 2004).
4) R. Anderson, “Stretching the Limits of Steganography”, Lecture Notes in Computer Science, **1174**, 39-48 (1997).
5) L. Boney, A. Tewfik, K. Hamdy, “Digital Watermarks for Audio Signals”, IEEE Proceeding of Multimedia, 473-480 (1996).
6) C. I. Podilchuk and E. J. Delp, “Digital Watermaking: Algorithms and Applications”, IEEE Signal Processing Magazine, **18**, 33-46 (2001).
7) 松井甲子雄, 岩切宗利, 情報ハイディングの基礎, (森北出版, 東京, 2004).
8) 山内雪路, スペクトラム拡散通信, (東京電気大学出版社, 東京, 1994).
9) 北野隆康, 岩井誠人, 笹岡秀一, “ディジタル移動通信における直接拡散信号の埋込による無線ステガノグラフィ方式”, 同志社大学理工学研究報告, **52**, 127-134 (2011).