A Wireless Steganography Technique by Embedding DS-SS Signal in Digital Mobile Communication Systems

Takayasu KITANO*, Hisato IWAI* and Hideichi SASAOKA*

(Received March 23, 2011)

We propose a new secret communication system in which the secret information signal is embedded in the other signal waveform. Because the proposed system has similarity to digital steganography techniques in the information processing field in that the secret data is hidden in the publicly known signal (cover data), we call it wireless steganography. In this paper we propose a realization of the system using spectrum spreading signal into other information signal. To quantitatively analyze the performance of the proposed techniques, computer simulations are carried out. The results of the simulation show the effectiveness of the proposed scheme to realize the confidential and secure communications.

Key words : information hiding, steganography, direct sequence spread spectrum, radio communication, radio propagation

キーワード :情報秘匿，ステガノグラフィ，直接拡散方式，無線通信，電波伝搬

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

北野　隆康，岩井　誠人，笹岡　秀一

1. まえがき

近年の無線通信の普及に伴い，盗聴対策技術が重要になっている．現在は，共通鍵暗号方式[1-3]や公開鍵暗号方式[4,5]などの暗号方式を用いて情報を暗号化して伝送することが一般的である．しかし，これらの暗号方式を無線通信に適用する場合，前者は暗号化に用いる秘密鍵の配送が問題となり，後者は復号時の計算量が膨大になることが問題となる．

そこで，電波伝搬の特徴を活用して秘密鍵を配送せずに共有する，電波伝搬特性に基づく秘密鍵共有方式[6-10]が提案されている．この方式は，暗号化した情報の伝送を行う 2 局の正規局の間で，電波伝搬の可逆性や場所依存性といった特徴を活用して秘密鍵を生成･共有する方式である．この方式により，少ない計算量で安全な秘密鍵共有が可能になり，無線通信における情報のセキュリティ（安全性）を確保できる．

しかし，これらの方式では，情報の安全性は確保できるものの，第三者でも暗号を用いた情報伝送行為自体を検出することが可能である．暗号を用いた情報伝送行為を悪意ある第三者（盗聴局）が検出した場合，正規局間での情報伝送を妨害することなど

* Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6289, Fax: +81-774-65-6801, E-mail: eti1101@mail4.doshisha.ac.jp

が考えられ，より安全な情報伝送を行うには通信行為自体を秘匿する技術が重要となる．

そこで本研究では，無線通信における通信行為の秘匿を実現する情報伝送方式として，電波伝搬特性を活用して変調信号を秘匿する方式を提案する．なお，情報伝送を秘匿する方式として既にディジタルステガノグラフィ [11-15] が提案されているが，これは，ディジタル情報の秘匿であり，変調信号の秘匿を行う提案方式とは秘匿形態・秘匿手法が異なる．

なお，本研究では，用語や名称についてはディジタルステガノグラフィに準拠 [16,17] したものを用い，本提案方式についても無線ステガノグラフィと呼ぶことにする．

2. 通信秘匿による伝送行為の秘匿と秘密情報伝送

2.1. 電波伝搬の特徴を用いた通信秘匿

無線ステガノグラフィ方式の概要を Fig. 1 に示す．本研究では，Fig. 1 のように，秘密情報の送受信を行う送信局 A と正規受信局 B，さらに，その情報の盗聴を試みる盗聴局 E が存在する環境を想定する．

無線ステガノグラフィでは，秘密裏に情報伝送を行う埋込信号（Embedded signal）を，別の情報の信号であるカバー信号（Cover signal）と同時に送信することで，盗聴局などの第三者から埋込信号の存在を秘匿して伝送する．このとき，埋込信号には，受信局で受信する場合に検出・復調が可能で，それ以外の局で受信する場合には，雑音などの自然現象による劣化と識別が困難になるような処理を行って送信する．

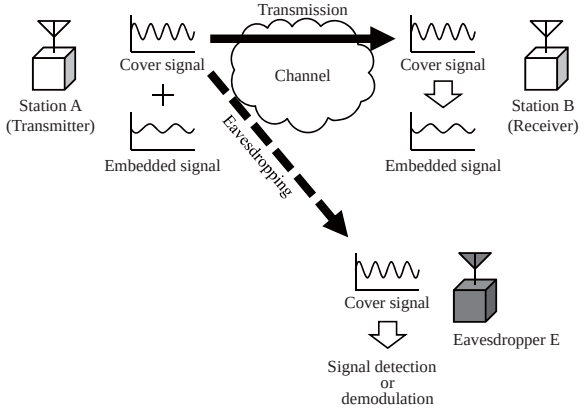


Fig. 1. Concept of information hidding in wireless communication

以上により，受信局で受信する場合には，カバー信号と埋込信号の両方の信号を検出・復調可能となるが，盗聴局では，カバー信号のみの検出・復調が可能であり，埋込信号を検出することが困難となる．

2.2. 通信秘匿に関する要件

無線ステガノグラフィによる通信秘匿を実現するためには，盗聴局における埋込信号の検出が困難であることが重要である．そこで，本節では通信秘匿を実現するためにカバー信号が満たすべき条件と，埋込信号が満たすべき条件を述べる．

2.2.1. カバー信号の品質保持

カバー信号は，埋込信号の秘匿とともに，情報伝送を行うことも期待されており，受信局以外の局でも情報を取り出せるよう設計されている必要がある．カバー信号に埋込信号を埋込む場合，埋込信号の電力によってはカバー信号の伝送を妨げ，カバー信号の品質を劣化させる可能性がある．この劣化は，埋込信号の存在を知らない局にとっては不自然な劣化であり，盗聴局でもこの不自然さをもとにして埋込信号を検出する可能性がある．そこで，埋込信号をカバー信号に埋込む際，カバー信号の品質の劣化を抑える処理を行う必要がある．

なお本研究では，埋込信号によるカバー信号の品質劣化を抑えるため，埋込信号を可能な限り小さい電力で埋込むことを想定する．

2.2.2. 埋込信号が満たすべき性質

埋込信号をそのままの形でカバー信号に埋込むと，盗聴局でも受信した信号からカバー信号を除去するだけで埋込信号の検出が可能になる．そのため，通信秘匿を実現する上では，埋込信号自体を盗聴局での検出が困難になるような形にすることが重要である．

2.3. 埋込信号による秘密情報伝送

2.3.1. 埋込信号の秘匿の重要性

埋込信号を秘匿するためには前節の条件を満た

せば良い. しかし, 通信秘匿が実現される場合でも, 埋込信号の存在を仮定した上で受信局と同じ復調処理を行い, 埋込信号の情報を取り出すことも考えられる.

このような盗聴の試行に対しても, 埋込信号に変調されている情報の安全性が保たれる必要がある. そこで本研究では, 埋込信号に電波伝搬特性を活用した秘密情報伝送方式 [18,19] を適用し, 埋込情報の耐盗聴性能を向上させる.

2.3.2. 事前歪み補償を用いた秘密情報伝送

ここで, 埋込信号に適用する電波伝搬特性を用いた秘密情報伝送について述べる. なお, 本研究では, 埋込信号に電波伝搬特性と事前歪み補償を用いた秘密情報伝送を適用する. ここで, Fig. 2 に, 事前歪み補償を用いた秘密情報伝送の概要を示す.

Fig. 2 は, 秘密情報伝送を行う送信局 A と正規受信局 B, さらに, その伝送情報の盗聴を試みる盗聴局 E が存在しているようなモデルである. 秘密情報伝送を行う前に, 受信局 B から送信局 A へ既知信号を送信し, 送信局 A で受信局 B との間の伝搬路 h を測定する. そして, 送信局 A は受信局 B に向かって信号 $s(t)$を送信するが, このとき, 受信局で $s(t)$ が正しく受信されるよう, 下式を満たす重み $w(t)$ で重み付けを行う.

$$h(t)\cdot w(t)=1 \tag{1}$$

この信号を受信局 B で受信する場合, 受信信号 $r(t)$がは次式のようになる.

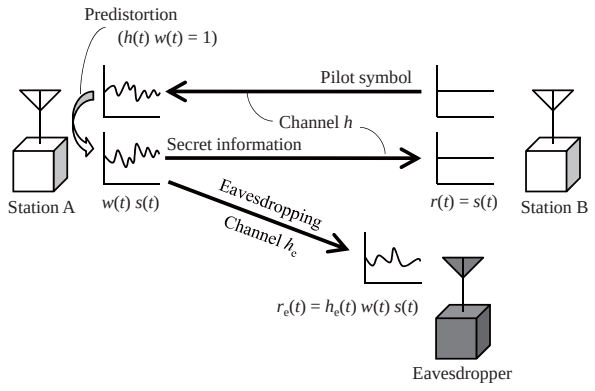


Fig. 2. Principle of secret information transmission using predistortion.

$$r(t)=h(t)\cdot w(t)\cdot s(t)=s(t) \tag{2}$$

受信信号が式(2)のようになる場合, 復調して情報を取り出すことが容易である.

一方, 盗聴局では, 伝搬路 h_e が受信局と異なる ($h(t)\neq h_e(t)$)ため, 受信信号 $r_e(t)$は,

$$r_e(t)=h_e(t)\cdot w(t)\cdot s(t) \tag{3}$$

となり, 適切な $w(t)$ の値を設定することで, 情報の抽出が困難になる.

3. 直接拡散信号の埋込による通信秘匿

3.1. 雑音の付加による埋込信号の秘匿

埋込信号には伝搬路歪みの事前補償に基づく秘密情報伝送方式 [18,19] と同じ手法を用いており, 盗聴局で埋込信号の情報を盗聴することは困難である. しかし, 通信路状態が良好で盗聴局がカバー信号を正確に推定可能であるような環境下では, 盗聴局でもカバー信号の除去が可能であるため, 埋込信号が容易に抽出される.

そこで本研究では, 埋込信号より電力が大きい雑音を送信局で付加し, 埋込信号を雑音に埋もれさせることで, 盗聴局での埋込信号検出を困難にする手法を用いる. ただし, 雑音をそのまま付加するだけでは埋込信号の特性が大きく劣化してしまい, 埋込信号を用いた情報伝送が困難になる. これに対して, 本研究では埋込信号に直接拡散 [20] を適用し, 拡散利得により埋込信号の特性を改善し, 情報伝送を可能にする.

3.2. インタリーブによる歪み分散

本研究では, 埋込信号に対して伝搬路の事前歪み補償を用いた秘密情報伝送を適用し, 埋込信号を用いた情報伝送の安全性を確保する. このとき, 埋込信号を拡散したそのままの形で埋込むとすると, 同じシンボル内ではほぼ同じ伝搬路特性となるため, 拡散符号との相関検出などにより, 埋込信号検出が可能になる場合がある. また, 盗聴局の場所によっては, 瞬時的に受信局と相関の高い伝搬路特性が得られることもあり, 盗聴局が埋込信号の一部を得る可能性がある.

そこで, 耐盗聴性能の向上のため, 直接拡散処理

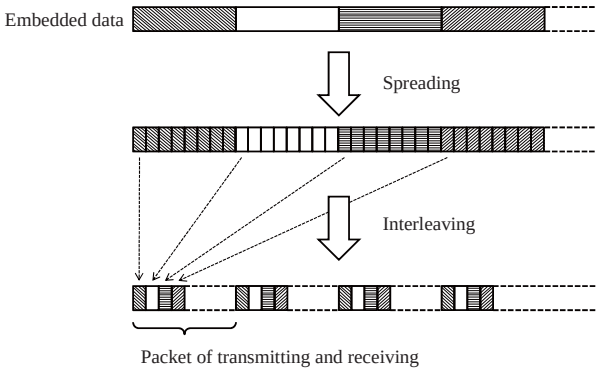


Fig. 3. An example of interleave.

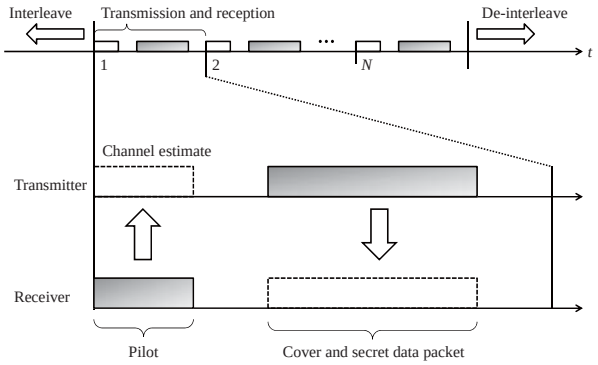


Fig. 4. Transmission and reception.

後の埋込信号に対して，拡散チップ単位のインタリーブを行って伝送するシンボルを分散させ，各チップがそれぞれ異なる伝搬路変動を受けるようにする．ただし，拡散周期とインタリーブの周期が重なる場合に，相関検出が可能になるという問題 [21] があるため，インタリーブと拡散の周期を異なるものにする必要がある．

ここで， Fig. 3，Fig. 4 に，インタリーブと送受信するパケットのタイムチャートを示す．Fig. 3 は，埋込信号のインタリーブの例を示している．Fig. 3 のようにインタリーブされた埋め込み信号は，それぞれ送受信パケットに分けられ，Fig. 4 に示すように，パケットごと一定時間間隔で送受信される．なお，各パケットの送受信の際には，送信局がそれぞれのパケットを伝送する直前に，あらかじめ受信局から送信された既知シンボルを元に伝搬路特性を推定し，埋込信号に対して伝搬路を経ることで歪みが元に戻るように事前歪み補償を行う．また，受信局では，パケットすべてを受信した段階でデインタリーブを行い，埋込情報を取り出す．

Fig. 4 に示したパケットの送受信において，伝搬路変動が無相関となる時間の間隔を空けて送受信を行うと，1 シンボル内の各拡散チップに対して，それぞれ異なった歪みを与えることができる．

3. 3. 送受信機構成

提案方式の送受信機構成を Fig. 5 に示す．送信機では，埋込信号に対して直接拡散処理を行い，インタリーブを行って複数のパケットに分割する．分割された埋込信号のパケットに対して，伝搬路歪みの事前補償を行い，正規局間での通信における伝搬路歪みによる振幅および位相の変動に対して元に戻るようにあらかじめ歪ませておく．そして，事前歪み補償を行ったパケットを，カバー信号を用いた通常の伝送を想定する場合に雑音と同程度と見なされる電力（本研究ではカバー信号電力対雑音電力比 20dB を想定した）で埋込むと同時に，付加雑音を加えて埋込信号を秘匿する．

受信局での埋込信号抽出の際は，まず受信信号をそのまま復調することでカバー情報が得られる．これを再変調し，その要素を受信信号から除去することで埋込信号を抽出することができる．このとき抽出された埋込信号は，正規の受信局では送信時に行われた事前補償処理により伝送路における歪みが補償され，抽出された信号が埋込信号であることが判別できる．一方，盗聴局では，事前歪み補償とインタリーブの効果により，埋込信号のチップごとに

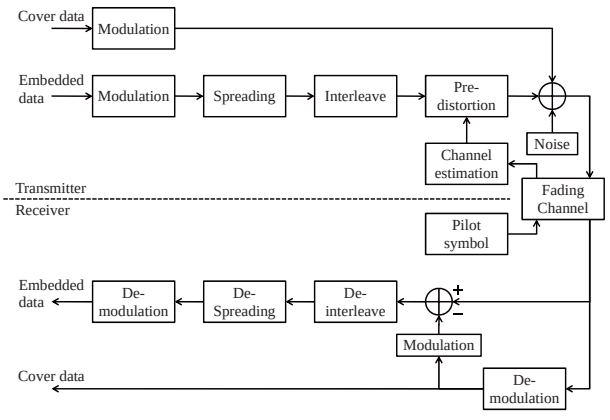


Fig. 5. A block diagram of transmitter and receiver of proposed system.

歪みが異なるため，埋込信号に相当する波形が変調信号であることを検出すること，および，そこから情報を取り出すことが非常に困難となる．

受信局では抽出した埋込信号を蓄積しておき，全パケット分を受信した時点でデインタリーブを行う．デインタリーブ処理を行った後の信号に対して逆拡散を行い，復調して埋込情報を取り出すことが可能となる．

4. シミュレーションによる評価

4.1. シミュレーションモデル

本研究では，提案方式における埋込信号の秘匿性，および，埋込信号の秘密情報の安全性について，シミュレーションにより評価を行う．シミュレーションモデルは，Fig. 1 と同じように，正規局 A, B，および，盗聴局 E が存在するモデルを想定する．シミュレーションパラメータは Table 1 に示すものを用いる．埋込信号とカバー信号の変調方式には QPSK を用い，埋込信号の拡散率を 63 とする．また，埋込信号 1 チップがカバー信号の 1 シンボルに対応するように設定し，埋込信号 64 シンボルに対してカバー信号は 4032(=63×64)シンボルとする．さらに，A 局と B 局の間の伝搬路 h と A 局と E 局の間の伝搬路 h_e は，それぞれ互いに独立なレイリーフェージング伝搬路であるとし，パケット内では変動しない準静的なものを想定する．また，埋込信号電力はカバー信号電力に対して–20dB とし，埋込信号を秘匿するために付加する雑音電力は，埋込信号電力に対して 10dB とする．

Table 1. Simulation parameters.

	Cover	Embedded
Modulation	QPSK	QPSK DS–SS
Spreading factor	–	63
Number of symbol	4032	64
Period of symbol	1	63
Number of pilot	4	4
Channel	Quasi-static Rayleigh channel	

埋込信号の秘匿性については，埋込信号における信号振幅の確率密度分布，埋込信号における信号点配置，および，カバー信号の品質により評価する．振幅確率密度分布と信号点配置の特性より，埋込信号が雑音に近い特性を示すことや，カバー信号の品質は埋込信号の有無で変化がないことを示すことができれば，埋込信号を秘匿することが可能であるといえる．一方，埋込信号の秘密情報の秘密性については，埋込信号のビット誤り率により評価する．

4.2. 埋込信号の秘匿に関する評価

4.2.1. 信号振幅の確率密度分布

ここでは，埋込信号の秘匿性評価として，埋込信号が統計的に雑音に近い分布となることを示す．

そこで，Fig. 6 に，盗聴局での受信信号をカバー信号の振幅を基準（0）として表した確率密度分布（PDF: Probability Density Function）を示す．なお，同図には，参考のためガウス分布も併せて示している．Fig. 6 より，埋込信号自体がガウス分布に近い分布に従っていることが確認できる．これより，盗聴局が受信信号を統計的な分布により盗聴を試みる場合でも，埋込信号の検出が困難であることを確認できる．

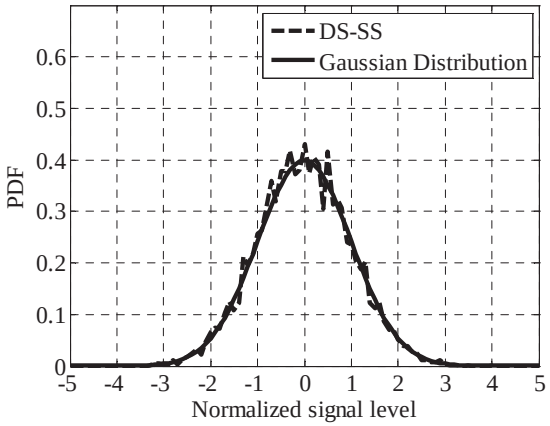
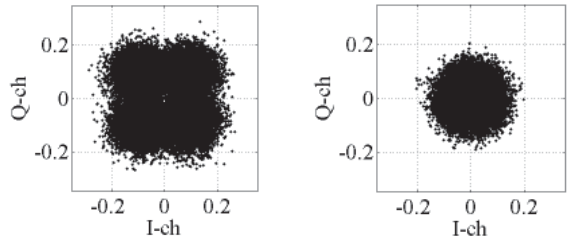


Fig. 6. Probability density function of embedded signal.

4.2.2. 埋込信号の信号点配置

埋込信号の秘匿性の検討として，受信信号からカバー信号成分を取り除いて埋込信号を抽出し，逆拡散処理を行った後の信号点配置により評価する．



(a) Authorized receiver (b) Eavesdropper

Fig. 7. Constellation of embedded signal.

逆拡散後の埋込信号については，正規局ではその情報を正確に取り出す必要があるため，埋込信号に相当する要素がディジタル変調信号の信号点配置となっていることが望ましい．一方，盗聴局では，埋込信号として検出困難であることが重要であるため，信号点配置が雑音のような形になっている必要がある．

Fig. 7 に，正規受信局と盗聴局での逆拡散後の信号点配置を示す．なお，Fig. 7(a) は正規受信局における信号点配置であり，Fig. 7(b) は盗聴局における信号点配置を示している．ただし，これらの図では，提案方式の基本特性を調べるため，伝搬路における雑音が発生しない環境を想定している．

Fig. 7(a) は， QPSK 信号に雑音が加わっているのと同じ信号点配置である．これより，正規受信局では，受信信号からカバー信号の要素を除去することで埋込信号を検出可能であることがわかる．

一方，盗聴局では，Fig. 7(b)に示すように雑音を信号点配置で表したものと類似の信号点配置となっており，ここから，QPSK 信号を検出することは困難である．これより，盗聴局では埋込信号に相当する信号を逆拡散しても雑音との判別が困難であり，埋込信号の検出が困難であるといえる．

以上の結果より，信号点配置の観点から通信秘匿は可能であることが示される．しかし，Fig. 7(a) の正規受信局での信号点配置は，伝搬路で雑音がない場合でも雑音環境下であるかのように分散しており，このままでは伝送品質が大きく劣化することが予想される．そこで本研究では，埋込信号に誤り訂正符号を適用し，埋込信号の特性を改善することを想定する．なお，次節以降の埋込信号の特性に関する検討の際は，埋込信号に誤り訂正符号を適用する．

4.2.3. カバー信号のビット誤り率特性

埋込信号を埋込んだ影響によりカバー信号による伝送品質が大きく劣化する場合，盗聴局でも要因を詳細に分析することで埋込信号検出が可能になる場合がある．特に，ビット誤り率（BER: Bit Error Rate）特性は測定が容易であり，盗聴局でビット誤り率特性を測定し，そこに大きな劣化が確認されると，埋込信号の存在を推定される危険性がある．そこで，カバー信号におけるカバー情報のビット誤り率特性についてのシミュレーションを行い，カバー信号の伝送品質劣化の観点から埋込信号の秘匿性能を評価する．

ここで，SNR に対するカバー情報のビット誤り率特性を Fig. 8 に示す．なお，本研究では，カバー信号電力対雑音電力比を SNR とする．Fig. 8 には，カバー信号に埋込信号が埋込まれている場合と，埋込まれていない場合の特性の両方を示している．ただし，埋込信号を埋込んでいない場合でも，埋込信号を秘匿するために送信局で付加する雑音は付加されているものとする．

Fig. 8 より，カバー情報のビット誤り率特性は，埋込信号の有無によって大きく変化しないことが確かめられる．これにより，カバー信号に埋込信号を埋込む影響による品質劣化は少なく，盗聴局でも，カバー信号の劣化から埋込信号を検出することは困難であると考えられる．

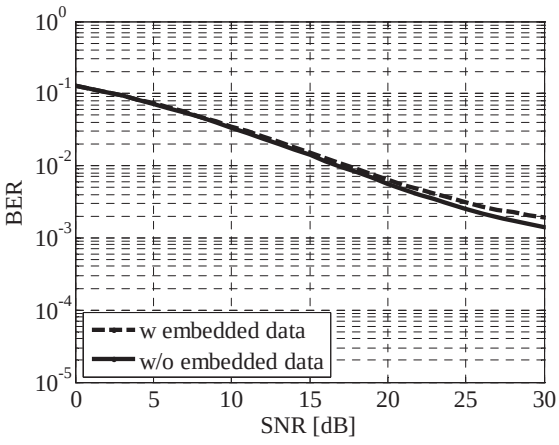


Fig. 8. BER performance of cover signal.

4.3. 埋込信号による秘密情報伝送の評価

盗聴局が埋込信号を検出できない場合でも，埋込信号の存在を仮定して同様の復調処理を行うことにより，埋込情報の盗聴を試みることが予想される．このような場合でも，埋込信号の秘密情報の安全性が保たれる必要がある．そこで，ここでは，盗聴局でも埋込信号の存在を仮定した復調処理を行うことを想定し，埋込信号の情報の安全性を評価する．

Fig. 9 に，平均 SNR に対するビット誤り率特性を示す．なお，本節でも，カバー信号対雑音電力比を SNR とする．ただし，埋込信号の情報に対しては，BCH 符号 (127,64) を適用し誤り訂正を行うとする．

Fig. 9 より，正規受信局において SNR が高くなるほどビット誤り率特性が良好になっており，正規受信局において埋込情報を受信可能であることを確認できる．一方，盗聴局における埋込信号のビット誤り率特性は 0.5 で一定の値になっており，埋込信号の秘密情報を得ることが困難であることがわかる．

なお，Fig. 9 の埋込信号の BER 特性は Fig. 8 のカバー信号の BER 特性に比べて良好な特性を示しているが，これは，埋込信号に対する直接拡散処理により拡散利得が得られていることと，誤り訂正符号を付加していることに起因している．

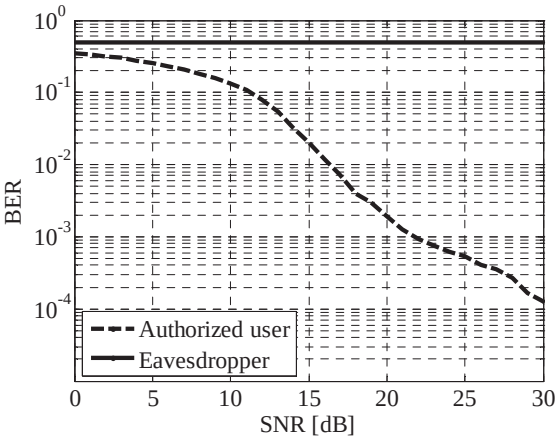


Fig. 9. BER performance of embedded signal.

5. まとめ

無線通信におけるセキュリティ対策として，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を提案した．提案方式は，秘匿を行う埋込信号に対して拡散処理を行い，付加雑音とともにカバー信号に埋込むことで通信秘匿を実現するものである．

秘密情報信号の秘匿性能と耐盗聴性能について，計算機シミュレーションにより評価したところ，通信秘匿が可能であることが確認できた．今後の課題として，より効率的に通信秘匿を行うための送信制御法や，秘匿性能の空間的評価などがあげられる．

本研究は科学研究費補助金基盤研究(C)（課題番号 22560397）の助成を受けたものである．

参考文献

1) 笠原正雄, 境隆一,「暗号」,（共立出版, 東京, 2000）.
2) 岡本龍明，山本博資，現代暗号,（産業図書，東京，1979）.
3) J. Daemen and V. Rijimen, “The Design of Rijindael: AES–the Advanced Encryption Standard,” Springer–Verlag (2002).
4) W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, **22**, 644–654 (1976).
5) R.L.Rivest, A.Shamir, and L.Adelman, “A method for obtaining digital signature and public-key cryptsystems,” Communications of the ACM, 120–126 (1978).
6) J. E. Hershey, A. A. Hassan, and R. Yarlagadda, “Unconventional cryptographic keying variable management,” IEEE Trans. Commun., **43**, 1-6 (1995).
7) A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” Digital Signal Processing, **6**, 207-212 (1996).
8) 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密情報の伝送・共有技術，”信学論(B), **J90-B**, 770-783 (2007).
9) T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless secret key generation exploiting reactance–domain scalar response of multipath fading channels,” IEEE Transaction on Antennas and Propagations, **53**, 3776–3784 (2005).
10) 北浦明人, 笹岡秀一, “陸上移動通信における OFDM

の伝送路特性に基づく秘密鍵共有方式," 電子情報通信学会論文誌(A), **J87−A**, 1320−1328 (2004).
11) R. Anderson, "Stretching the limits of steganography," Lecture Notes in Computer Science, **1174**, 39–48 (1996).
12) 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).
13) L. Boney, A. Tewfik, and K. Hamdy, "Digital watermarks for audio signals," IEEE Proceeding of Multimedia, 473–480 (1996).
14) C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," IEEE Signal Processing Magazine, **18**, 33–46 (2001).
15) Sos S. Agaian, David Akopian, and Sunil D'Souza, "Wireless steganography," SPIE Proc. – the International Society for Optical Engineering, **6074**, 141–152, (2006).
16) B. Pfitzmann, "Information hiding terminology," Lecture Notes in Computer Science, **1174**, 347–350 (1996).
17) 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).
18) H. Koorapaty, A.A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," IEEE Communications Letters, **4**, 52–55 (2000).
19) 折橋雅之, 中川洋一, 小林聖峰, 村上豊, "無線の伝搬特性を利用したセキュリティ無線通信技術," Matsushita Technical Journal, **49**, 409−413 (2003).
20) 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).
21) 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込による無線ステガノグラフィ方式," 信学論(B), **J92-B**, 2-10 (2009).