講演番号：31

VN-CSK 照明可視光通信における 等重み (2,2) 視覚復号型秘密分散法

A-9 Equal-weight (2,2) visual secret sharing schemes on VN-CSK illumination light communication

真中 佳祐 [1] 陳 力源 [1] 羽渕 裕真 [1] 小澤 佑介 [1]
Keisuke Manaka Liyuan Chen Hiromasa Habuchi Yusuke Kozawa

茨城大学工学部情報工学科 [1]
Department of Computer and Information Science, College of Engineering, Ibaraki University

1 まえがき

視覚復号型秘密分散法 (VSSS) と呼ばれる秘密分散法 [1] は, 秘密画像を n 枚の Share に分散し, そのうちの k 枚を重ね合わせることで, 視覚的に秘密画像を復号する手法である. 各 Share は 0 または 1 の信号で構成され, 照明可視光通信との親和性が高いが, その融合システムの検討はほとんどなされていない.

本稿では,VN-CSK 照明可視光通信 [2] に 2 つの Share を用意する (2,2)VSSS を融合するシステムを提案する. 提案方式では, 各 Share で 0 が偏らないように, 直交 M 系列 [3] を用意して 1,0 の生起確率が 1/2 になるようにする. これにより一定の照明度を達成できる. さらに各 Share の"1"信号に VN-CSK 信号を乗算することにより, 調光制御や各 LED 照明毎の情報伝送も可能になる.

2 システム構成

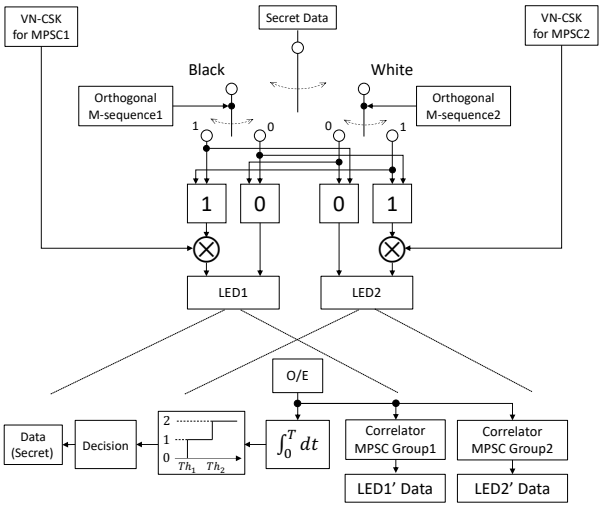

図 1: システムモデル

図 1 に (2,2)VSSS を組み込んだ VN-CSK 照明可視光通信システムを示す. 白黒の秘密画像を Share1,Share2 に分散し,Share1 を LED 照明 #1 に,Share2 を LED 照明 #2 に割り当てる. 秘密画像の白黒により, 各 Share の 0,1 がランダムに決定される. しかしながら, ランダムに決定してしまうと 0 が連続したり,0 の割合が高くなる場合があり, 照明機能を損なってしまう. そのため, 各 Share での 0 と 1 の割合が同程度となるように,0 と 1 の生起確率が 1/2 である直交 M 系列を利用して決定する. さらに, 信号 1 には VN-CSK 信号を乗算して送信する.

受信側では,O/E 変換後,VN-CSK 信号時間ごとに積分され, その積分値により,0 と 1 を判定する.Share1 と Share2 がともに 0 と, ともに 1 の場合は 0 と判定し, 互いに異なる場合は 1 と判定する. つまり, 各 Share の 1 の場合の相関値を y とすると, データが 0 の場合は 0 または $2y$, データが 1 の場合は y となる. したがって,2 つのしきい値 (Th_1, Th_2) を利用して判定する. 各 VN-CSK 信号の復調は, 各 LED の拡張プライム符号と相関検波し, 最尤判定によりデータを抽出する.

3 性能評価

図 2 に信号誤り率特性を示す. ただし, 1000*1000[pixel] のバイナリデータ, 長さ 8 の直交 M 系列を用いている. さらに,VN-CSK 照明可視光通信では M=3 の MPSC を用いる. これにより, 視覚復号データの誤り率が SNR=11.2[dB] のとき,BER=10^{-3} を達成できることが分かった.

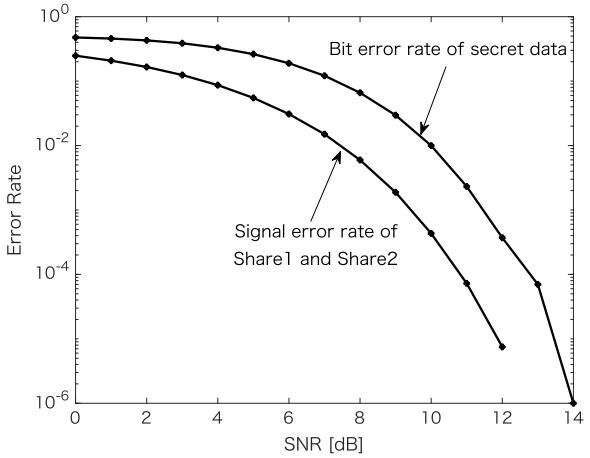

図 2: 誤り率特性

4 むすび

本稿では, 視覚復号型秘密分散法を利用する VN-CSK 照明可視光通信を提案した. 誤り率特性の点から (2,2)VSSS を VN-CSK 照明可視光通信システムに組み込めることが分かった.

謝辞

本研究の一部は, 科学研究費補助金の援助により行われた.

参考文献

[1] 坂本ら,"複数の画像を復元できる視覚復号型 (2,2) 秘密分散法の提案", 信学技報 IT2007-15,2007-07
[2] K,Osawa et al.,“Theoretical Analysis on Bit Error Rate of Visible-Light Variable N-Parallel Code-Shift-Keying”, IEICE Trans. Fundamentals, Vol.E101-A, No.12, pp.2352-2358, Dec. 2018.
[3] 羽渕,"M 系列を基に構成される系列とその通信への応用", Fundamentals Review Vol.3 No.1 pp.32-42. Jul. 2009.

Copyright © 2019 IEICE