

Performance of GIG Codes in Jamming Environment

Dr. Usha Kamale

Professor, Department of Electronics and Communication Engineering, Maturi Venkata Subba Rao Engineering College, Hyderabad, India

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.1408000142>

Abstract: This paper analyzes the performance of 6-bit & 12-bit Gray and Inverse Gray (GIG) Codes in Jamming environment. Gray and Inverse Gray codes are binary orthogonal codes generated by parallel concatenation of Gray and Inverse Gray codes. Direct sequence spread spectrum communication using orthogonal spreading sequences is a common practice for secured data transmission. Performance evaluation over noisy channel conditions is carried out using bit error rate. Along with popular Walsh codes, 12 and 16-length GIG codes are used as spreading sequences and bit error rate analysis is carried out in the presence of Additive white Gaussian noise and Pulsed jammer. GIG Codes perform on par with existing Walsh codes.

Index Terms - Gray Inverse Gray codes; Direct Sequence spread Spectrum; AWG Noise; Pulsed Jamming.

I. Introduction

Spread spectrum techniques have many applications, such as jam-resistant communication systems, global positioning systems (GPS), wireless local area networks (WLAN), cordless phones, long range wireless phones for home and industry, cellular base station interconnection, and code division multiple access (CDMA) radio, which allows multiple users to access and use the communication system simultaneously. Spread spectrum is a means of transmission where the signal uses a wide range of frequencies to send the information. The signal spreading is accomplished by different means of code generation at the transmitter and this signal spreading is independent of the data. The spread signals would be collected and then converted to their original frequency at the receiver after synchronizing the generated code with the code at the receiver. By spreading the transmitted signals they become more transparent, so it is unlikely that they will be intercepted by an opponent, or interfered with by other signals intended for other users, even if they use the same frequencies.

Although spread spectrum was developed primarily to secure military communications, it was later used for commercial developments such as mobile radio networks (radio telephony, packet radio, and amateur radio), timing and positioning systems, specialized applications in satellites, etc. There are many reasons for spreading the spectrum, and if it is done properly, many benefits can accrue simultaneously. Some of these benefits are Interference rejection, Anti-jamming, Low probability of intercept, Multiple access, High resolution ranging, Multi-path suppression, and Diversity reception.

Secured Communication in Jamming Environment

There are several methods used to implement the spread spectrum technique. Each has its own design and features. The main spread spectrum methods are Direct sequence, Frequency hopping, Time hopping, and Hybrid (a combination of direct sequence and frequency hopping). Each of these methods effectively provide a further level of modulation not directly associated with the information or sinusoidal carrier signal, thereby providing some immunity against interfering signals without a significant loss of information, or alternatively, reducing the likelihood of signal detection or interception. This is particularly important when intentional signal jamming is present in a hostile communication environment. Jamming is the ability to interfere, distort, or prevent the signal transmission before it received by its desired receiver. There are different ways to place the jamming signal within the spread spectrum bandwidth.

In [14] presents a robust CDMA receiver design and jamming evaluation under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. First, we analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. Second, by exploiting the small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver can be redesigned to achieve robust performance under disguised jamming.

Different Types of Jammers

Barrage noise jammer: The jammer transmits band limited white Gaussian noise. It is usually assumed that the jammer power spectrum covers exactly the same frequency range as the spread spectrum signal. The effect of the barrage noise jammer on the spectrum is to increase the Gaussian noise level at the output of the receiver down converter. If the power of the jammer signal is P_J watts, and signal has a bandwidth of W Hz, the single-sided power spectral density (PSD) of the jammer is $N_J = P_J/W$.

ON-OFF Jammer: The ON-OFF jammer (pulsed noise jammer) transmits a pulsed band limited Gaussian noise signal whose power spectral density just covers the spread spectrum system bandwidth W . The duty factor (the fraction of time during which the jammer turns on) for the jammer is denoted by ρ . The received jammer power spectral density is $P_J/\rho W$. This pulsed technique can also be used for single tone, multiple tone and partial band jammers.

Partial Band Jammer: To jam a spread spectrum signal, it is typically more effective to transmit all the available jamming power in a limited bandwidth. This is called a partial band jammer. If the fraction of the spread spectrum signal bandwidth which is jammed is denoted by q , the PSD of the partial band jammer is $NJ = PJ/qW$, where PJ is the total jamming power and, qW is the limited bandwidth of the signal which is jammed. The partial band jammer is particularly effective against frequency hopping spread spectrum systems because the signal will hop in and out of the jamming band and can be seriously degraded in the jamming band.

Single Tone Jammer: The single tone jammer transmits an unmodulated carrier with power PJ somewhere in the spread spectrum signal bandwidth. The single tone jammer is easily to generate and is rather effective against direct sequence spread spectrum systems. To achieve the maximum effectiveness of this jammer, the jamming tone should be placed at the center of the spread spectrum signal bandwidth. The single tone jammer is less effective against frequency hopping, since the frequency hopping instantaneous bandwidth is small and, for large processing gains the probability of any hop being jammed is small.

Multiple Tone Jammer: A better tone jamming strategy against frequency hopping systems is to use several tones instead of a single tone. However, the power of the single tone jammer will be shared by these multiple jamming tones. The jammer selects a number of tones so that the optimum degradation occurs when the spread spectrum signal hops to a jamming tone frequency. The optimum number of tones is a function of the received ratio of signal power to jammer power (P_S / P_J). Multiple tone jamming is also effective against hybrid systems.

Gray and Inverse Gray (GIG) Codes

An n -bit Gray code is a list of all 2^n bit strings such that the hamming distance between any two adjacent code words is always equal to one [2]. On the contrary, Inverse Gray codes exhibit maximum possible hamming distance between any two successive code words [10]. Like Walsh codes, the binary user codes discussed in this paper are available in sizes of power of two and additionally code sets of length 6 and their even multiples are also available. The simple construction technique and generation of code sets of different sizes are the salient features of the proposed codes.

Construction of GIG Code sets

The construction procedure of the proposed binary user codes is as follows: First, Generalized Gray Code generation algorithm [12] is used for constructing the Gray codes. Inverse Gray codes are generated using the algorithm in [14]. By appending Inverse Gray Code to the Gray Code we obtain a $2n$ -length GIG Code (Gray Inverse Gray). Each row of this GIG Code is a Binary spreading Code of length $2n$. This construction procedure is explained in detail in our previous work [15] and this allows us to construct a set of 2^n user codes of length $2n$ using n -bit Gray and Inverse Gray Codes. This procedure can be applied to $n=3$ or 4 only. Table 3.1 displays one such 6-length binary GIG user code set. With $n=3$, it is noted that $2^3 = 8$ code words each of length '6' can be constructed by concatenating 3-bit Gray and 3-bit Inverse Gray codes. Out of $3!$ ($= 6$) permutations used for generating GIG codes, three different 6-length binary spreading code sets are obtained. Some code words are common in these three Code sets. With $n=4$, in the obtained GIG code it is observed that the bottom-half of the code words are logical inverses of top-half. Hence, only top-half or bottom-half of the code words form a code set comprising of '8' code words of length 8 each. All the $4!$ ($=24$) permutations used for generating GIG codes result in same binary user code set. Table 3.2 gives the three different binary user code sets of length 6 (GIG₆ Set I, GIG₆ Set II, GIG₆ Set III) and one 8-length binary user code set (GIG₈) along with Walsh codes of length 8 (W_8) in decimal notation.

Table 3.1: Construction of 6-bit GIG Code

3-bit Gray code	3-bit Inverse Gray code	6-bit GIG code	6-bit GIG code set in decimal notation
000	000	000000	0
001	110	001110	14
101	101	101101	45
100	011	100011	35
110	100	110100	52
111	010	111010	58
011	001	011001	25
010	111	010111	23

Table 3.2: Three different 6-bit GIG Code sets, 8-bit GIG Code set and 8-bit Walsh Code set (in Decimal)

W₈	GIG₈	GIG₆ set I	GIG₆ set II	GIG₆ set III
0	0	0	0	0
85	30	14	14	21
51	51	27	45	54
102	45	21	35	35
15	102	50	52	44
90	120	60	58	57
60	85	41	25	26
105	75	39	23	15

Recursive Construction of Higher Length GIG Code sets

Considering the 6 & 8-length code sets as basic sets, Binary GIG Codes of any even multiples of lengths 6 & 8 can be generated recursively using the following relationship

$$C_{2M} = \begin{bmatrix} C_M & C_M \\ C_M & \overline{C_M} \end{bmatrix}$$

Recursive constructions of Binary GIG Code sets of lengths 12 & 16 in integer form are given in Table 3.3 along with 16-length Walsh Code set for comparison.

Table 3.3: Recursively Constructed 12-bit GIG Code sets, 16-bit GIG Code set and 16-bit Walsh Code set (in Decimal)

W₁₆	GIG₁₆	GIG₁₂ Set I	GIG₁₂ Set II	GIG₁₂ Set III
0	0	0	0	0
3855	7710	910	910	2275
13107	13107	1755	2925	3510
26985	11565	1365	2275	1365
26214	26214	3250	3380	1690
23130	30840	3900	3770	3705
21845	21845	2665	1625	2860
15420	19275	2535	1495	975
255	255	63	63	63
4080	7905	945	945	2268
13260	13260	1764	2898	3465
23205	11730	1386	2268	1386
26265	26265	3213	3339	1701
27030	30855	3843	3717	3654
21930	21930	2646	1638	2835
15555	19380	2520	1512	1008

Results of Bit Error Rate Analysis

Performance analysis of binary data communication over jamming environment is presented in this section. Binary sequence generated using a random data generator is transmitted using spread spectrum communication. Bit error rate over a noisy channel is evaluated. Data communication over a channel in the presence of Additive White Gaussian Noise and Pulsed jammer is carried out using different spreading codes such as GIG codes of length 12 and 16 bits and a comparison with Walsh codes of length 16.

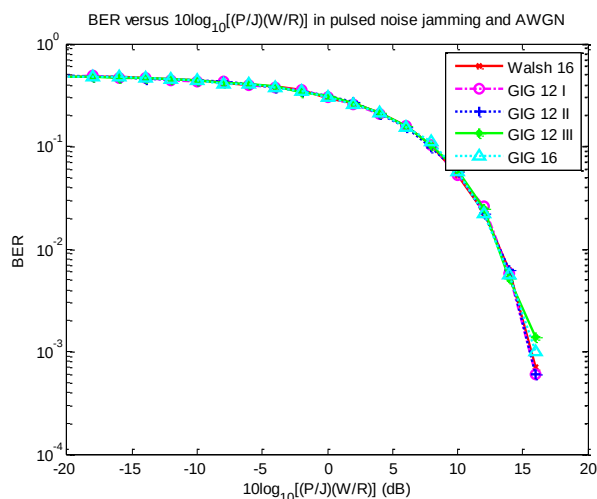


Fig. 1: Bit Error Rate in Pulsed Noise Jamming and AWGN

The bit error rate analysis shows that the performance of GIG Codes is very close to Walsh Codes. With lesser spreading factor GIG codes achieve performance similar to Walsh codes. In other words, information transmission takes place with lesser spreading bandwidth using GIG Codes.

References

1. F. Gray, "Pulse Code Communication", U.S. Patent No. 2632058, 1953.
2. K. J. Sankar, V.M. Pandharipande and P.S. Moharir, "Generalized Gray Codes," Intelligent Signal Processing and Communication Systems (ISPACS'04), pp. 654-659, 2004.
3. Ebrahimzadeh and A. Falahati, "Frequency Hopping Spread Spectrum Security Improvement with Encrypted Spreading Codes in a Partial Band Jamming Environment, Journal of Information Security, 2013, vol.4. 1892, pp.1-6.
4. Rahat Ullah, Amjad Ali and Shahid Latif, "Security Improvement by using Dual Coded FHSS," International Journal of Computer Application, vol. 76, no. 7, August 2013, pp. 1-7.
5. Wali Mohamed S. A. A., Improved Jamming-Resistant Frequency Hopped Spread Spectrum System, Ph.D Thesis, Carleton University, Ottawa, Jan. 2014.
6. Jonathan Min, "Analysis and Design of Frequency Hopped Spread Spectrum Transceiver for Wireless Personal Communications," Final Report, University of California, Jan 1996.
7. K. Fazal and S. Kaiser, Multi Carrier and Spread Spectrum system, John Wiley and Sons, 2003.
8. M. K. Simon, J. K. Omura, R. A. Scholtz and B.K.Levitt, Spread Spectrum Communications Handbook, McGrawHill, 1994.
9. Sabbir Ahmed† and Makoto Kawai, Adaptive Selection of Spreading Code Subsets from Orthogonal Binary Code Sets for Reduced PAPR in MC-CDMA Systems, Journal of Communications, Vol. 5, No. 7, July 2010.
10. K.Usha, k. Jaya sankar, A technique for the construction of Inverse Gray codes, International Journal of Emerging trends in Engineering and Development, ISSN 2249-6149 Issue 2, Vol.2, March 2012
11. K.Usha, K.Jaya Sankar, "Binary Orthogonal Code Generation for Multi-User Communication using n-bit Gray and Inverse Gray Codes," International Journal of Electronics and Communication Engineering, ISSN 0974-2166, Vol. 5, No. 2, pp. 165-174, 2012.
12. K.Usha, K. Jaya Sankar, Performance Analysis of New Binary User Codes for DS-CDMA Communication, Journal of The Institution of Engineers (India): Series B Electrical, Electronics & Telecommunication and Computer Engineering ISSN 2250-2106, Vol. 97, No. 1, 2016.
13. Meher Krishna Patel, Stevan M. Berber and Kevin W. Sowerb, "Anti-jamming Performance of Adaptive Chaos Based CDMA System with MRC in Imperfect Channel Estimation Environment," Wireless Communications and Mobile Computing, Hindawi, 2017.
14. Kai Zhou, Tianlong Song, Jian Ren, Tongtong Li, Robust CDMA receiver design under disguised jamming, 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 20-25 March 2016