IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENCRYPTED FHSS USING GENERALIZED GRAY CODES

[1]Dr.K.Usha, [2]N. Kavitha

[1]Professor,[2]Asst.Professor

[1]Department of Electronics and Communication Engineering,

[1]Maturi Venkata Subba Rao Engineering College, Hyderabad, India

Abstract: Information security has become the major objective of wireless communication. Spread Spectrum communication techniques are well known for secured data transmission. This paper discusses encrypted Frequency Hopping Spread Spectrum technique. The proposed method makes use of two different spreading sequences for even and odd data packets. Generalized Gray code generation technique provides the required encrypted random sequence that provides the necessary improvement in the security.

Index Terms **- Generalized Gray codes; Frequency Hopping spread Spectrum; Binary Reflected Gray code;**

I. INTRODUCTION

The usable portion of the radio spectrum is huge ranging from approximately 6 KHz to 300 GHz. Because radio is so well suited to information transmission, however, almost all of the spectrum is already reserved for specific uses. Alas, because bandwidth is so scarce and valuable, the frequencies allocated for unlicensed networking are what one might call junk frequencies ones commercial users are unlikely to want. The 2.4- GHz band, for example, is subject to interference from microwave ovens, and the signals have difficulty penetrating trees, heavy snow, or anything at all that contains water. (the water absorbs a portion of the signal and is heated, just as in a microwave oven.) The 900-MHz band is often plagued by interference from medical and scientific equipment, cordless phones, wireless stereo speakers, and similar devices. Unlicensed users of the band are considered to be secondary users. They take a back seat to licensed, or primary, users, who can transmit stronger signals and are subject to fewer restrictions. A high-power primary user such as a TV station or a vehicle location system can render an unlicensed frequency band useless to anyone else in the vicinity, including wireless LANS. Unlicensed users have no recourse - even if they've already spent tens of thousands of dollars on wireless networking equipment. The requirements imposed by the regulations on unlicensed wireless networking equipment are relatively simple. First, the strength of the signal is limited-usually to less than 1 watt. Second, the signal must be transmitted using one of two spread-spectrum methods. The signal must either be spread out over a certain range of frequencies or hop among a certain minimum number of narrow slots each second.

The idea of spread-spectrum radio transmission was proposed by the military who was seeking ways to prevent radio signals from being monitored or blocked by hostile parties. The two inventors came up with the notion of changing the frequency of a transmission at regular intervals faster than the enemy could retune. A special receiver that knew the frequency-hopping pattern could follow it and pick up the entire transmission. The hopping patterns were controlled by the punched holes in piano rolls became known as frequency-hopping spread spectrum (FHSS).

Later, as digital logic became popular, an- other kind of spread spectrum was developed direct-sequence spread spectrum (DSSS). In this method of transmission, the signal does not hop from one frequency to another but is passed through a spreading function and distributed over the entire band at once. DSSS usually provides slightly higher data rates and shorter delays than FHSS, because the transmitter and receiver don't have to spend time retuning.

Both FHSS and DSSS are resistant to interference from conventional radio transmitters. Because the signal doesn't stay in one place on the band, FHSS can elude a jammer – (a transmitter designed to block radio transmissions on a given frequency). DSSS avoids interference by configuring the spreading function in the receiver to concentrate the desired signal but spread out and dilutes any interfering signal.

Spread-spectrum radio is good at dodging interference from conventional sources – (signals that stay in one narrow area of the frequency band and don’t move. it doesn’t always do as well when there are other spread ,spectrum systems operating nearby, though. The more frequency-hopping transmitters operating on a band, the more likely it is that one or more of them will hop to

the same frequency at the same time, garbling data that must be retransmitted. DSSS is better at resisting noise up to a certain point. However, if the combined interference throughout the band rises above a certain level, throughput dramatically drops-nearly to zero. Unfortunately, it only takes a few nearby FHSS systems to cripple a DSSS system. On the other hand, because a DSSS system is always transmitting on every frequency in the band, a nearby FHSS system may be unable to find any clear channel to hop to. In the presence of interference, FHSS usually degrades more gracefully than DSSS, but neither works well when competing at close range.

Frequency hopping spread spectrum is widely used in military applications to provide communication between command posts, soldiers, vehicles, sensors, missile launchers, etc. It provides good protection against the effects of frequency selective fading, and can be robust in jamming environments. Traditional frequency hopping spread spectrum involves dividing the available spectrum into a large number of sub-bands, and hopping over these sub-bands in a pseudo-random fashion, but there are different implementations within this general framework that can deliver better performance.

II. GENERALIZED GRAY 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[1-2]. In data transmission, Gray codes are capable of providing more robust communication and simultaneously play an important role in error detection and correction. Gray codes are also beneficial in Genetic Algorithms due to the property of their code-words to change incrementally. Gray codes can be used as Location Identifiers. Gray Codes can be used for enumeration of Plane Straight-Line Graphs. The application of Space time Trellis Coded Ternary Phase Shift Keying to achieve higher spectral efficiency and coding for mobile communication are discussed in. Gray codes have many application areas of which analog – digital converters of mechanical type is the oldest application. It is essential to use a Gay code to overcome ambiguities that otherwise appear as the code is advanced [3-17]].

ALGORITHM TO GENERATE GENERALIZED GRAY CODES

(n, r) Gray code (radix 'r')

Let an n-bit radix 'r' Gray code be needed. Let (P_1, P_2, P_3 ,…….P_n) be a permutation of (1,2,3,….n). The r^n integers (0,1,2,……(r^n-1))can be arranged in the following doubly indexed indicial sets.

$Q_{j,k} = r^j \{k,k+r,…….k+m\}$

j = 0,1,2,……..…n
k = 1,2,……r-1
Where 'm' is the largest positive integer such that $m \leq r^{n-j-1} - k / r$.
Over the integers (0,1,…..(r-1),0) a new succession order (0,s_1,s_2,……s_i…..s_{r-1},0) is defined where s_1,s_2,….s_{r-1} is a permutation of (1,2,3,…i…(r-1)) so that s_i succeeds s_{i-1} and let s_1 succeed '0' and '0' succeed s_{r-1}. Then, starting with the row of all zeros as a zeroeth row, the i^{th} row is obtained from the $(i-1)^{th}$ row by replacing the p_j^{th} bit by its successor, if it is in $Q_{j-1,k}$.

Binary Gray codes

Let us consider the construction of a 3-bit binary Gray code. All the integers, i.e., {0,1,2,3,…..(2^3 –1)} are arranged in the form of indicial sets as shown below:

$Q_0 = 2^0 \{1, 3, 5,7\} = 1,3,5,7$
$Q_1 = 2^1 \{1, 3\} = 2,6$
$Q_2 = 2^2 \{1\} = 4$

As stated earlier, let (P_1, P_2, P_3 …… P_j ……P_n) be a permutation of (1,2,3,….. j,….n). Since we are considering a 3-bit case, consider the permutation {2,3,1}. Hence, $P_1 = 2$; $P_2 = 3$; $P_3 = 1$. The first code word is (0 0 0) which is the zeroeth row of the code. To obtain 1^{st} row, we have to change P_j^{th} bit if '1' is in Q_{j-1}. Here, 1 is in Q_0. Therefore, P_1 bit is to be changed and P_1=2, hence the code is (0 1 0). Similarly, since '2' is in Q_1, P_2 bit (i.e. 3^{rd} bit) is to be changed, hence the code is (1 1 0). The resulting code obtained by continuing this procedure is tabulated in Table I. All the 3! = 6, 3-bit Cyclic Gray Codes generated using the algorithm in decimal notation in Table II.

Table I
3-bit Cyclic Gray Code for permutation {2, 3, 1}

Sl No.	i^{th} row	P_j	Bit to be changed	3-bit Binary Gray Code 3 2 1
1	0	-	-	0 0 0
2	1	P_1	2	0 1 0
3	2	P_2	3	1 1 0
4	3	P_1	2	1 0 0
5	4	P_3	1	1 0 1
6	5	P_1	2	1 1 1
7	6	P_2	3	0 1 1
8	7	P_1	2	0 0 1

Table II

Sl. no	Permutation	Cyclic Gray code
1	1 2 3	0,1,3,2,6,7,5,4
2	1 3 2	0,1,5,4,6,7,3,2
3	2 1 3	0,2,3,1,5,7,6,4
4	2 3 1	0,2,6,4,5,7,3,1
5	3 1 2	0,4,5,1,3,7,6,2
6	3 2 1	0,4,6,2,3,7,5,1

A total of n! Gray codes can be generated using the above technique for any integer value of 'n' and all these Gray codes are cyclic.

III. FREQUENCY HOPPING SPREAD SPECTRUM

Frequency hopping is a spread spectrum technique that involves partitioning the allocated frequency band, called the *hopping band*, into a large number of smaller *sub-bands*. These sub-bands are also called carrier frequencies, channels, tones, sub-channels, or sub-carriers. Transmission is carried out in short bursts on one sub-band at time, hopping from sub-band to sub-band in a pseudo-random fashion after each burst, as illustrated in Fig. 2.1. The figure illustrates how the total system bandwidth of B_{tot} Hz is divided into K narrow sub-bands, where each sub-band has a bandwidth of $B_{sb} = B_{tot}/K$ Hz. The system uses one sub-band at a time, for a *hop duration* of T_{sb} seconds, before hopping to another sub-band. In this manner all sub-bands are used roughly an equal amount of time, but no sub-band is used continuously for a long time. The rate at which the hops occur, relative to the symbol transmission rate, allows us to categorize the FHSS system as either fast or slow hopping. If the *hop rate*, which is the inverse of the hop duration, is greater than the symbol rate, then the system is characterized as *fast hopping*. In this case each transmitted symbol is divided over multiple sub-bands. *Slow hopping* occurs when the hop rate is less than or equal to the symbol rate, which means that one or more data symbols are transmitted within each hop. The order in which the hopping occurs over the sub-bands is called the *hopping pattern*. This sequence is generated by a secure pseudo-random code generator at the transmitter. The hopping pattern is also known by the intended receiver so it can easily recover the transmitted signal, but other receivers, without this knowledge, are unable to detect the signal, thereby impeding undesirable signal interception and making intentional jamming more difficult. To provide a secure and unpredictable frequency hopping pattern, the pattern should be a random sequence and this sequence should have a large period. The large period prevents the capture and storage of a period of the pattern by a jammer or eavesdropper. Here the unlicensed ISM band 902-928MHz is considered as FHSS frequency band.

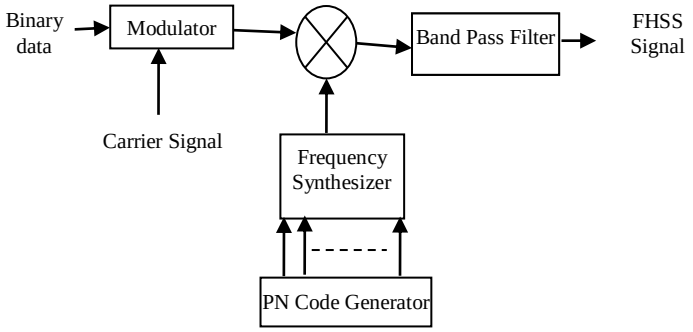

Fig. 1: FHSS Transmitter

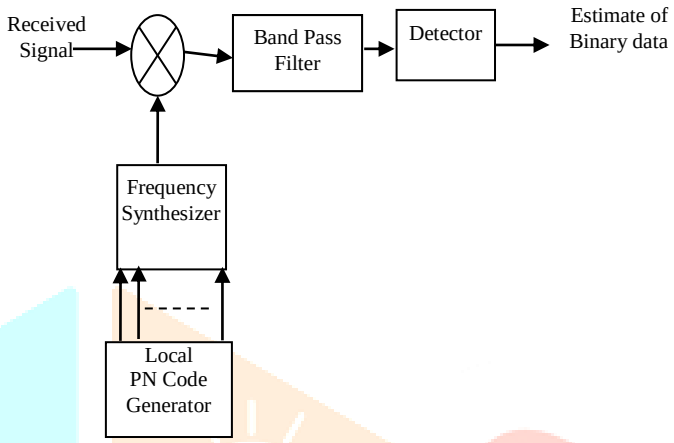

Fig. 2: FHSS Receiver

IV. ENCRYPTED FHSS

In Frequency Hopping Spread Spectrum, the random sequence of carrier frequencies plays an important role and if this sequence is hijacked then all the secured information may leak out. Even and Odd data packets are transmitted and recovered using original and encrypted hopping sequences respectively. The encrypted sequence is obtained from generalized Gray code algorithm. Each permutation of length 'n' input to the algorithm generates a 2^n length Gray coded sequence which is used as an encrypted hopping pattern. The same encrypted hopping sequence can be generated and used for the data recovery at the receiver. A total of n! different permutations provide n! hopping patterns. If n= 4, hopping pattern has 2^4(= 16) carrier frequencies and a total of 4! (= 16) different hopping patterns can be obtained using the generalized Gray code generation algorithm. These hopping patterns by default always start from one frequency. So, to reduce the risk of hostile access that frequency value is discarded and a 15- length hopping pattern is obtained which is used in the encryption process.

V. RESULTS AND DISCUSSION

Figs 3 and 4 display the hopping patterns obtained from the permutations [1 2 3 4] and [2 1 4 3] respectively. As the value of 'n' increases the length of the hopping pattern and total number of possible hopping patterns also increases. In Fig.5, the process of frequency hopping spread spectrum with a 15- frequency hopping pattern along with necessary waveforms. FHSS signal and its Fourier transform are displayed in Fig. 6. The different 15-length frequency hopping patterns obtained using different permutations are tabulated in Table. III.

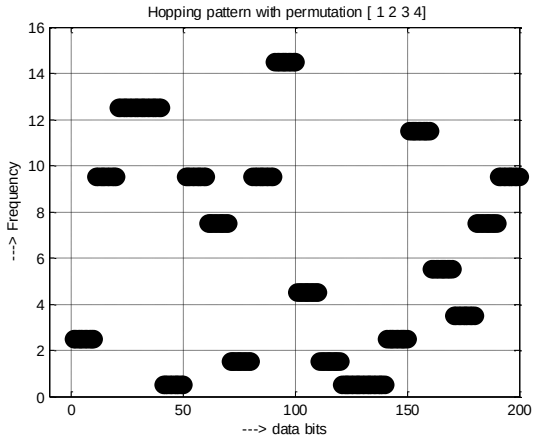

Fig. 3: Frequency Hopping pattern observed with permutation [1 2 3 4]

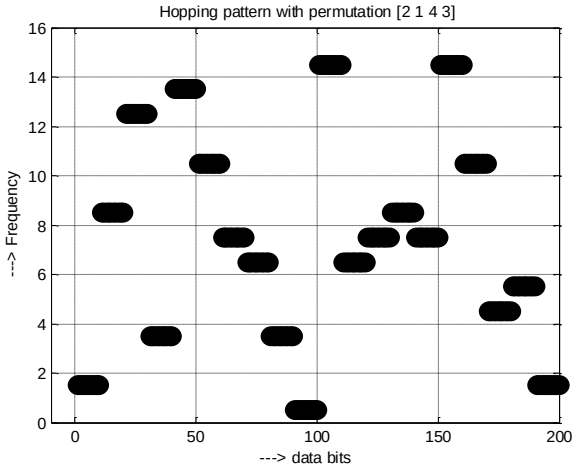

Fig. 4: Frequency Hopping pattern observed with permutation [2 1 4 3]

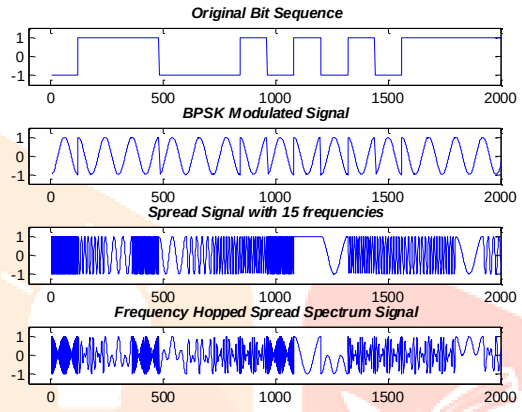

Fig. 5: Original binary data sequence, BPSK modulated signal, Spread Spectrum Signal an encrypted FHSS signal

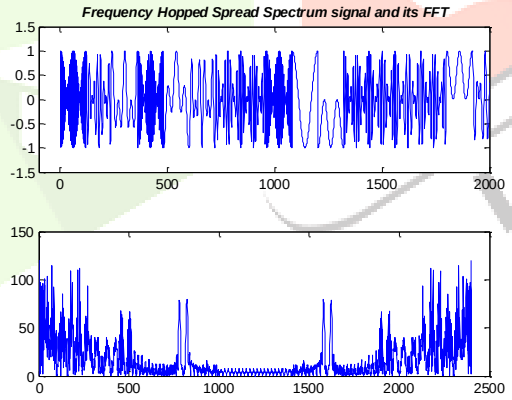

Fig. 6: Time and frequency domain representation of encrypted FHSS signal

TABLE III PERMUTATIONS AND FREQUENCY HOPPING PATTERNS

Permutation	Frequency Hopping Sequence
1 2 3 4	F_8 F_{12} F_4 F_6 F_{14} F_{10} F_2 F_3 F_{11} F_{15} F_7 F_5 F_{13} F_9 F_1
3 1 2 4	F_8 F_{10} F_2 F_3 F_{11} F_9 F_1 F_5 F_{13} F_{15} F_7 F_6 F_{14} F_{12} F_4
1 2 4 3	F_4 F_{12} F_8 F_{10} F_{14} F_6 F_2 F_3 F_7 F_{15} F_{11} F_9 F_{13} F_5 F_1
4 2 1 3	F_4 F_5 F_1 F_3 F_7 F_6 F_2 F_{10} F_{14} F_{15} F_{11} F_9 F_{13} F_{12} F_8
2 3 1 4	F_8 F_9 F_1 F_5 F_{13} F_{12} F_4 F_6 F_{14} F_{15} F_7 F_3 F_{11} F_{10} F_2

IV. CONCLUSION

In a multiple access system which includes more number of users and each user's data is to be transmitted in a secured system the number of hopping patterns required are also more. In a Frequency Hopping Multiple Access (FHMA) system each user's data is divided into bursts of uniform size and a unique hopping pattern is assigned to every user. In such cases security can be improved by using two hopping sequences per user.

The length of the hopping sequence can be increased to any power of 2. The total number of hopping patterns available is also going to increase drastically as the length of permutation 'n' increases. The data recovery is done by applying the same hopping patterns at the receiver. The generation of required hopping patterns at the receiver using the same permutation is very simple using the Gray code generation algorithm.

REFERENCES

[1] F. Gray, 1953. Pulse Code Communication, U.S. Patent No. 2632058.

[2] K. J. Sankar, V.M. Pandharipande and P.S. Moharir, 2004. Generalized Gray Codes, Intelligent Signal Processing and Communication Systems (ISPACS'04), pp. 654-659.

[3] A. Ebrahimzadeh and A. Falahati, 2013. Frequency Hopping Spread Spectrum Security Improvement with Encrypted Spreading Codes in a Partial Band Jamming Environment, Journal of Information Security, 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., 2014. Improved Jamming-Resistant Frequency Hopped Spread Spectrum System, Ph.D Thesis, Carleton University, Ottawa.

[6] Jonathan Min, 1996. Analysis and Design of Frequency Hopped Spread Spectrum Transceiver for Wireless Personal Communications, Final Report, University of California.

[7] K. Fazel and S. Kaiser, 2003. Multi Carrier and Spread Spectrum system, John Wiley and Sons.

[8] M. K. Simon, J. K. Omura, R. A. Scholtz and B.K.Levitt, 2004. Spread Spectrum Communications Handbook, McGrawHill.

[9] Usha K. and Jaya Sankar K., "Generation of Walsh Codes in Four Different Orderings using 3-bit Gray codes", International Journal of Applied Engineering Research (IJAER), ISSN 0973-4562, Vol. 6, no. 21, pp. 2475- 2484, December 2011.

[10] Usha K. and Jaya Sankar K., "A Technique for the construction of Inverse Gray Codes", International Journal of Emerging Trends in Engineering and Development (IJETED), ISSN 2249-6149, Vol.2, Issue 2, March 2012.

[11] Usha K. and Jaya Sankar K., "Generation of Walsh Codes in Two Different Orderings using 4-bit Gray and Inverse Gray codes", Indian Journal of Science and Technology (IJST), ISSN 0974-6846,Vol.5, No.3, pp 2341-2345, 2012.

[12] Usha K. and Jaya Sankar K., "Binary Orthogonal Code Generation for Multiuser communication using n-bit Gray and Inverse Gray codes", International Journal of Electronics and Communication Engineering (IJECE), ISSN 0974-2166, Vol.5, No. 2, pp. 165-174, 2012.

[13] Usha K. and Jaya Sankar K., "Partial generation of 2^n-length Walsh codes using n-bit Gray and Inverse Gray codes", International Journal of Electronics and Communication Engineering and Technology (IJECET), ISSN 0976-6464, Vol.4, Issue 4, pp. 232- 239, July-August 2013.

[14] Usha K. and Jaya Sankar K., "New Multi level Spreading Codes for DS CDMA Communication," World Conference on Advances in Communication and Control systems, CACCS 2013, 6-8th April 2013, DIT University, Dehradun, Uttarakhand, India.

[15] Usha K. and Jaya Sankar K., "Performance Analysis of New Binary User Codes for DS CDMA Communication over Rayleigh fading channel," Proc. Of International Conference on Microelectronics, Communications and Renewable energy, IEEE ICMiCR 2013, ISBN 978-1-4673- 5150-8, pp. 1-5, 4-6th June 2013, AJCE, Kanjirapally, Kerala, India.

[16] Usha K. and Jaya Sankar K., "Performance evaluation of new multi level spreading codes for synchronous DS CDMA communication," Proc. Of International Conference on VLSI, Communication, Advanced devices, Signals & systems and Networking, VCASAN 2013, ISBN 978-81-322-1524-0_22, pp. 159-167, 17-19th July, 2013, BNMIT, Benguluru, Karnataka, India.

[17] K. Usha, *et al*., "Performance evaluation of new multi level spreading codes for DS CDMA Communication over Rayleigh fading channel", Proc. Of Second IEEE International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013, ISBN 978-1-4673-6217-7/13, pp. 649-654, 22-25th August 2013, SJCE, Mysore, India.

[18] Kamle Usha & Kottareddygari 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, Volume 97 Number 1, J. Inst. Eng. India Ser. B (2016) 97:61-67, DOI 10.1007/s40031-014-0163-3