BIT ERROR RATE ANALYSIS FOR IMAGE TRANSMISSION USING OFDM BASED ON CHAOS CRYPTOGRAPHY.

R. Shankari¹, K. Ranjani², S. Sangeetha², U. Vishnupriya²
Asst. professor-I, Dept of ECE, Velammal Engineering College, Chennai, Tamilnadu, India¹
UG students, Dept of ECE, Velammal Engineering college, Chennai, Tamilnadu, India²

Abstract
Chaos coding examines the constitution of wave supported OFDM systems and jointly compare with the interpretation of optical primarily based MIMO OFDM. Wavelet based OFDM has a lot of blessings compared to the optical based OFDM. There is no necessity for periodic prefix, a lot of adjustable and optimal conclusion. Wavelets wish endure fittingly in nearly full areas of wireless communication themes with OFDM that may be a durable soul for next peers of wireless scheme. We have a tendency to area unit mistreatment chaos coding in optical medium so as to serene the data bits and avoid the interference. Finally hacker analysis and licensed analysis conjointly doing for cipher the efficiency.

Keywords: OFDM, Wavelets, Chaos Encryption, Wireless Communication, Bit Error Rate.

INTRODUCTION
Wireless Communication is the rapid growing and most teeming technological areas in the communication field. Generally, in a communication system, information is handover from transmitter to receiver that are placed over a confined distance. Wireless networks are being possible in peculiar areas like education, military, package delivery, and medical emergency care.

One of the foremost syndicate of wireless communication is surety of the data. Since the signals are handover in vacant space, it is probable that a snitcher can capture the signals and imprint piercing information. The foremost objective of encryption is to protect the intimately of digital data stored on computer systems or transmitted through the internet or any other computer network. Generally occupied encryption ruse are not suitable for image encryption. Chaotic based image encryption is widely used.

Chaotic cryptography is the application of the mathematical chaos theory to the preview of the cryptography, the inquisition or techniques used to backstage and securely handover information with the appearance of a third-party or scrappy. If chaotic parameters, as well as cryptographic keys, can be intrigue consonantly or intrigue to produce acceptable and functional output, it will make it subsequent to undoable for an scrappy to find the output without any knowledge of the initial values. With the advent of chaos-based cryptography hundreds of new image encryption algorithms, all with the bourn of ament the security of digital images were proposed. Chaotic image encryption can be evolved by using the properties of chaos including deterministic dynamics, flickery actions and non linear transform. Generally chaotic based cryptography is not qualified for serviceable application. It does not serene algorithm due to reciprocity of initial condition, which can be easy shattered. So in this algorithm victimized by using original input values are multiplied with encrypted values which gives the indistinct value. Then the input value is bit XOR which provide the small ideal value of the pixel. To deal with the specialized challenges of image security technologies are image encryption methodology to provide end to end security.

EXISTING METHODS
The guard bits used in FDMA to prevent interference waste the useful and scarce frequency resources. Maximum bit rate is fixed, so that it will not fit when the date rate is varying as per QOS and priorities. Spectrum planning and networks are bulky and it takes more time. While the station is not performing, the transmitting or receiving operation the spectrum is wasted as the frequency in FDMA are permanently allocated.

TDMA users having the predetermined time slot. Users might be disconnected if the time slots are full while moving from one cell site to other cell site. It also suffered from multiple distortion. TDMA requires more efforts for planning and network. Quality are affected by multipath interference. Call may be dropped while switching from one base station cell to other cell.

In CDMA overall QOS will decrease with the increase of number of users. To retrieve the original baseband signal precision code synchronization is required. In CDMA system, self jamming is occurred due to loss of orthogonality or spread sequence of different subscribers. Near far problem is occurred in CDMA system. In TDMA, CDMA, FDMA collision will occur.
PROPOSED METHODS

The proposed architecture has two main components: one is it uses the OFDM channel for data transmission and the other one is it uses chaos algorithm for encryption technique. Input image is encrypted by chaos encryption. The value of the each pixels in the image are converted into 8 bit binary value. Chaos coefficients have the constant value which are \( u = 3.9999 \) and \( x = 0.40000565 \). Threshold for these values are calculated by calculating the average of the constant values. Then we apply bit Xor for input data and threshold value. This is the process performed for encryption operation at the transmitter side. Then the encrypted image is again converted to data which is transmitted to the OFDM channel. It uses the symmetric encryption mechanism so the encryption and decryption key are same. Then it passes through the OFDM channel.

In Orthogonal Frequency Division Multiplexing (OFDM), all the subcarriers are interleaved so that guard bits space becomes very small in order to achieve high data rate. OFDM splits high rate data stream into parallel streams which are then transmitted by modulating N distinct carriers, each subcarrier is orthogonal to each other. The projection of one basis vector on the other basis vector is zero. OFDM is a multiple carrier which encodes the digital data on several number of carrier frequencies. To reduce crosstalk and interference single data stream is divided into multiple narrowband channels at various frequency. Here the data are modulated and the wavelet is applied on it. Wavelet means it split into lower data and higher data. Then the ifft and the cyclic prefix operation are performed which are briefly described as follows:

In serial to parallel converter input data streams are formatted into required word size for transmission serially and converted into parallel format. During transmission each word is assigned to one carrier parallely. In parallel to serial converter process in which all the received stream of data elements is converted and send as a stream of data at one bit at a time. Cyclic prefix means the data at the end is repeated to avoid data loss at the receiver side. However cyclic prefix is eliminated in the receiver side.

IFFT is used to convert the signal from time domain to frequency domain. The conventional approach of OFDM requires a set subcarriers which is generated by the carrier bank. Bit combination decides how each was modulated with a constellation, but this approach made system voluminous and expensive. So IFFT is used to make system digital, simple, cheap, and efficient. FFT is used to convert the signal from frequency domain to time domain.

In information theory the basic noise model is additive white Gaussian noise which minimize the effect of many random processes which occurs in nature. Additive means because of an information system any noise added might be intrinsic and white means refuse to the frequency band that will have uniform power for an information system. Gaussian means the time domain has a normal distribution with a zero average value of time domain.

In serial to parallel converter input data streams are formatted into required word size for transmission serially and converted into parallel format. During transmission each word is assigned to one carrier parallely. In parallel to serial converter process in which all the received stream of data elements is converted and send as a stream of data at one bit at a time. Cyclic prefix means the data at the end is repeated to avoid data loss at the receiver side. However cyclic prefix is eliminated in the receiver side.

IFFT is used to convert the signal from time domain to frequency domain. The conventional approach of OFDM requires a set subcarriers which is generated by the carrier bank. Bit combination decides how each was modulated with a constellation, but this approach made system voluminous and expensive. So IFFT is used to make system digital, simple, cheap, and efficient. FFT is used to convert the signal from frequency domain to time domain.

In information theory the basic noise model is additive white Gaussian noise which minimize the effect of many random processes which occurs in nature. Additive means because of an information system any noise added might be intrinsic and white means refuse to the frequency band that will have uniform power for an information system. Gaussian means the time domain has a normal distribution with a zero average value of time domain.

Data is given to the mapper. Mapper QAM/PSK is used to compare the results of different receivers. By analyzing the performance of the different receivers by utilizing different sized QAM so as to set in order to observe the difference in the effective minimum distance from the different receivers while using different signal sets corresponding to index codes of increasing length. QAM transmission is valid for any general index coding issues. The advantage of mapper is providing higher coding gain for a longer index code when compared with the binary transmission. To evaluate the mean and variance of received symbols, demapper is used.
Encryption key is produced by the logistic map. A smart hacker can easily predict the encryption key because the logistic map is periodic in nature. To overcome this problem, a non-linear equation is used in the logistic map and the periodicity is also removed. From the OFDM channel, the data is transmitted through the Zig-Bee transmitter (hardware) at one end and received by the receiver Zig-Bee (hardware) at the other end. Zig-Bee RFm75/Cc2500 is used in this project. Then, from the receiver, decryption process is started, which is the inverse process of encryption. Image is decrypted using the same key used for encryption. Images are showed with different SNR values as below.

![Input Image](image1)

**Fig. 4 Input image**

![Encrypted Image](image2)

**Fig. 5 Encrypted Image**

![Decrypted Image](image3)

**Fig. 6 Decrypted image at various SNR level.**

![Zigbee Connection](image4)

**Fig. 7 Zigbee Connection**

![Signal to noise ratio](image5)

**Fig. 8 Signal to noise ratio**

![Mean Square Error](image6)

**Fig. 9 Mean Square Error**

![BER vs SNR](image7)

**Fig. 10 BER vs SNR**
This shows that using Chaos algorithm we can increase the security and collision is avoided due to OFDM channel. It reduces the significant amount of data loss and also increase the signal to noise ratio.

CONCLUSION:
In this paper highly secured chaos encryption is used for image encryption. The secured binary data obtained from chaos encryption technique is passed over OFDM channel to the Zigbee transmitter which send the data to receiver Zigbee and then it is received at the OFDM channel receiver end without any significant loss or collision. The comparative results for Rc7 algorithm and chaos algorithm is shown as test results. Moreover the primary image is unaltered while encryption which is proved by receiving the decrypted image as same as that of original image.

REFERENCES: