Design of Secured Image Transmission Scheme Based on Cryptography in Different Communication Channels

PROJECT REPORT

Submitted in partial fulfillment of the requirements for the award of the Degree of Master of Technology in Department of Electronics & Communication Engineering with specialization in Communication Systems by the A P J Abdul Kalam Technological University

by

ALIN SARA SAM

TKM20ECCS03

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

TKM COLLEGE OF ENGINEERING

KOLLAM 691 005

JULY 2022

Design of Secured Image Transmission Scheme Based on Cryptography in Different Communication Channels

PROJECT REPORT

Submitted in partial fulfillment of the requirements for the award of the Degree of Master of Technology in Department of Electronics & Communication Engineering with specialization in Communication Systems by the A P J Abdul Kalam Technological University

by

ALIN SARA SAM

TKM20ECCS03

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

TKM COLLEGE OF ENGINEERING

KOLLAM 691 005

JULY 2022

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

TKM COLLEGE OF ENGINEERING

KOLLAM 691 005

CERTIFICATE

Certified that this project titled **"Design of Secured Image Transmission Scheme Based on Cryptography in Different Communication Channels"** is a bonafide record of the work done by **ALIN SARA SAM** (Reg. No. TKM20ECCS03) under my supervision, in partial fulfillment of the requirements for the award of the Degree of Master of Technology in Electronics and Communication Engineering with specialization in Communication System by the A P J Abdul Kalam Technological University.

Guide	**Coordinator**	**HoD**
Prof. Najia A	**Dr. Nishanth N**	**Prof. Abid Hussain**
Associate Professor	Associate Professor	Head, Dept. of ECE
Dept. of ECE, TKMCE	Dept. of ECE, TKMCE	Dept. of ECE, TKMCE

Acknowledgement

I take this opportunity to express my heartfelt gratitude to everyone who has been gracious enough to offer their advice and support when needed resulting in the successful completion of this project work.

First of all, I thank Almighty for all of his mercies throughout this project without which it would not have been possible.

It is my privilege and pleasure to convey my profound sense of respect, gratitude, and obligation to Dr. T.A. Shahul Hameed, Principal, TKM College of Engineering, for providing facilities for the successful completion of my project work.

I sincerely thank Prof. Abid Hussain, head of the Department, Department of Electronics and Communication, for his guidance, valuable support and constant encouragement given to me during this work.

I express my profound gratitude to our P G coordinator, Dr. Nishanth N, associate professor, Department of Electronics and Communication, for his prompt assistance constructive criticism, supervision and patience throughout project preparation and presentation.

I am extremely grateful to Prof. Najia A, associate professor Department of Electronics and Communication, for her support, advice, and crucial contributions to the project effort.

Last, but not the least, I wish to acknowledge my parents and friends for giving me moral strength and encouragement throughout this project.

Alin Sara Sam

TKM20ECCS03

ABSTRACT

The need for establishing a network with privacy and security is gaining much attraction in this modern age. Illegal Data access or confidentiality breach is a serious threat that is prevalent in both wireless and wired communication channels. Due to the optic fiber's attributes, such as its high bandwidth, reliability, and immunity to interference, optical fiber networks can offer secure data transmission and are utilised in a variety of sensitive applications over long and small distances. However, there exists several types of fiber optic eavesdropping attacks. Eavesdropping is major physical layer attack occurs on all network, primarily targeting to obtain highly confidential information shared by government authorities, military, financial or pharmaceutical sectors. In this work an efficient solution to eavesdropping attacks during image transmission is proposed. User data or the original image is encrypted using algorithmic cryptography (AES algorithm) and then transmitted over communication channel. In fiber optic channel, Optical CDMA is used to encode the signal Which acts as an additional Encryption layer in the network. Only the authorized user is permitted to retrieve the actual image correctly using matched decoder and correct decryption key in an AES- OCDMA system. The interception time for the eavesdropper will be high as they have to check each optical code and every possible encryption key which will eventually lead to low success rate of interceptor. Further, the encrypted image can also be transmitted over a OFDM to set up a high speed secure network.The encryption quality of images in AES- OFDM scheme transmitted over AWGN channel is obtained with MATLAB and is defined in terms of Histograms and PSNR value. Optical OFDM system secured with crytographic algorithms is worth studying in the future

Keywords: Cryptography, Advanced Encryption Standard (AES), Image encryption, Eavesdropping, Optical CDMA, OFDM

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Communication channel, either wireless or optical are employed in several commercial and military applications were sensitive informations are transmitted. Wireless channel are prone to third party attacks due to the openness of channel. Transmitting datas over a fiber channel or hybrid FSO/fiber channel has great advantages in terms of its flexibility and high-capacity. However, data encryption is critical since the possibility of fiber tapping attacks still exists. Security uplifting techniques are some times applied on the top layers of the open system interconnection (OSI) model. The physical layer, however, plainly transmits the encrypted signal's header information. In this scenario, the adversary can decrypt data at the physical layer. Some optical domain techniques, such as optical key distribution, steganography, Ex-OR scrambling, and optical code division multiplexing (OCDMA) [1-2], can also be utilised to increase the network security. OFDM networks also provides high security along with wider bandwidth application.

Eavesdropping is a common type of passive attack that tries to intercept the data transmitted between between two parties by a malicious third party. Wireless networks have a number of nodes that are free to join and exit the networks. In an optical fiber network, data interception is accomplished by coupling a portion of the light pulse from the network fiber to an eavesdropping fiber or photo detector by fiber bending, optical splitting, evanescent coupling, or scattering. This reduces the quality of physical layer security. Physical layer security approaches such as optical CDMA encoding have lately gained popularity as an extra security layer in transmis-

sion systems [3-8]. An enhanced security network can strengthen the confidentiality of messages over a wireless/optical medium in the presence of intruders.

Key sharing and key agreement encryption schemes and quantum communication can provide positive impact on security, but it cannot ensure absolute security. An intelligent eavesdropper receives transmitted ciphertext or cipher image and when he intercepts a big quantity of ciphertext. Then it will easy to get the key parameters that determines the security of the system. Algorithmic cryptography is a common security scheme based on different algorithms like DES RSA or AES . It is implemented in higher layers in OSI network architecture. Security of such systems is not completely free from threats. The 768-bit RSA cryptosystem, for example, was reported broken in December 2009 [8].

Inorder to elevate the secret nature of the picture transmission system, AES-OCDMA system and AES -OFDM system is proposed. The confidentiality of the system is improved if the image data is first encrypted using any cryptographic algorithm and then transmitting over channel. AES algorithm is used for enciphering the image data with secret nature. Although there some cryptographic algorithm like Rivest- Shamir-Adleman (RSA), Data Encryption Standard (DES), Triple DES etc are present, this work uses AES algorithm because of its large key space and the ability to defend brute-force attack. Corresponding encrypted data is encoded by using Physical layer Encoding Techniques. In this work optical CDMA technique is used to perform physical layer encryption. The advantage of the system is that after the equivalent optical decoding procedure in the receiver, an AES decryption technique is performed to recover the user's data. That is, when using an AES-OCDMA multilayer security system, eavesdropper have to intercept both the code of O-CDMA in physical layer and the provided cryptographic algorithm. AES enciphering technique which is used in this work is a symmetric key encryption block cipher. The hexadecimal key which is used for encryption and decryption stands same. The transmitted image is only intelligible for a legitimate user who has the matched decoder and the correct decryption algorithm. The system reduces the SNR of the eavesdropper make the network secure over a large distance for a long time and thereby improves informa-

tion security. OFDM technique can also be used to transmit encrypted image[13-16]. Applying AES to the OFDM network will improve the secrecy capacity of the network. The advantage of OFDM system is that it is possible to establish a secure high data rate network [17]. Since the subcarriers in OFDM are orthogonal to each other, signal interference will be very less. The receiver can correctly demodulate the data only if it receives the entire signal. These systems can be simulated using Optisystem software and MATLAB.

Chapter 2

Literature Review

The end objective of a secure communication network is to protect the data transmitted from being stolen or compromised.Confidentiality, integrity and availablity, that is also known as CIA triad defines the security of a communication link. Optical code division multiple access (OCDMA), is a sensible choice in maintaining the confidentiality and availability by providing some techniques for data hiding.

T.H Shake *et. al* [1] conducted a quantitative examination on the magnitude and kinds of security that OCDMA encoding may give. According to this study, an intelligently encoded OCDMA signal can force a possible eavesdropper to install a specialized and potentially costly detector in order to breach the user's confidentiality. It is possible to increase the confidentiality of data by changing the code words frequently or using an OCDMA code of large code space. This paper compares different OCDMA code types like time spreading codes, time-spreading/wavelength-hopping codes, spectral amplitude codes, and spectral phase codes and states their degree of security in terms of code space. The most significant eavesdropping strategies in OCDMA are noted as signal tapping or fiber tapping and energy detection (for on-off keyed OCDMA). The ability of the unauthorized party to successfully recognise codeword of the user is highly reliant on the SNR at the intercepting receiver. An intelligent system design that lowers the SNR of the unauthorized third party can be made by rapid reconfiguration of codes, or by increasing the complexity of codes.

T.H Shake *et. al* [2] proposed a theoretical examination on the level of confiden-

tiality that can be provided by spectral phase encoded Optical CDMA. An intelligent eavesdropper can find out the code and can intercept the information being transmitted until the PN sequence code is changed by the legitimate users. The advancement of energy detection and differential detection technologies has the potential to compromise the innate security of conventional Optical CDMA. Because the high and low energy levels of bit are easily distinguishable and can be easily identified by a receptor in traditional on-off keying (OOK) OCDMA, data bits can be simply recovered by interceptor employing a simple energy detector in the uplink end of a user even in the absence of a decoder. The level of secrecy provided by spectral-phase encoding is undeniably higher than that provided by technologies such as the OOK wavelength division multiplexing signalling utilised in conventional commercial optical networks.

Some authors [3] has a proposed code switching to improve the security of the OCDMA system.In this study, the authors encode information bit one (1) using a modified Pseudo Noise code and information bit zero (0) with a complimentary code sequence. This code-switching data modulation technology increases security over on-off keying by eliminating the vulnerability to eavesdropping.

A Cheriffi. *et. al* [4] has developed a new two dimensional SWZCC Code for spectral/spatial optical CDMA systems featuring zero cross correlation. The suggested system works as follows: user information are encoded with their respective spectral sequences code and thereafter disseminated to receivers via fiber star couplers using the spatial sequences code. After collecting the coded data at the receiver end, data detection is performed utilising Fiber Bragg Grating and Photo detector. Optisystem software is used to simulate and analyse the system. The proposed code has a greater SNR and a BER which is less than an acceptable value of 10^9.

A physical layer security mechanism based on OCDMA is proposed by Y. Tan *et. al* [5] and quantitatively analysed. The seed sequence shared between legitimate communication parties is expanded into a time spreading, wavelength hopping code by using a 5 stage linear feedback shift register. The de-spreading code used in the optical reconfigurable decoder of the intended receiver will also be changed accord-

ingly. The dynamic encoder and decoder employed in this study is a combination of a wavelength selective switch (WSS) that controls the output ports related to distinct wavelength optical signals, an optical tunable delay line (OTDL), and an optical Coupler (OC). OTDL is employed to control the timeslot of the pulse. With the help of simulation data, the authors claim that expanding the number of wavelengths and interference users, as well as selecting the appropriate transmitting optical power, can help to increase system security. The issue of OCDMA codeword capacity, which makes the system vulnerable to brute force search attacks, is addressed by utilising an unique 2-D wavelength-hopping/time-spreading (WH/TS) code with a huge capacity.

To improve data secrecy, Urmila Bhanja *et. al* introduced a new efficient code named multi-diagonal prime hop code (MDPHC) which is a 2D wavelength/time OCDMA code This code with in the novel encryption mechanism is tested using optisystem version 14.0. [6] The two-dimensional MDPHC code is created by merging two one-dimensional codes, such as the multi-diagonal code (MD) and the prime hop code (PC). The suggested solution adds a second layer of security to the OCDMA network, making it more secure.

J.Ji proposed *et. al* [7, 8] a cross layer security network based on Physical layer encryption and algorithmic cryptography is introduced simulated and analysed the performance. OCDMA is used for providing physical layer security while cryptographic algorithms like DES or AES is implemented in higher layers of OSI network architecture. The security of the system has been increased considerably ass the interception time for an eavesdropper is long.

H S Gill *et. al* [9], developed a novel work to improve the security of orthogonal frequency division multiplexing PON using wavelength division multiplexing. An elliptic curve with Diffie-Helman key exchange protocol is used to establish a shared secret key to enable safe communication over an insecure channel. This key can be used as the AES algorithm's encryption key at optical line terminals and optical network equipment. Choose keys that are as strong as possible to avoid brute-force attacks. Finally, without the session key information, recovering the original data for

an unauthorised ONU is difficult. The suggested architecture will help to improve the physical layer security of next-generation PONs.

Recently, the privacy ensured by orthogonal frequency division multiplexing-based passive optical network (OFDM-PON) systems has generated significant interest. A multi- level encryption approach for physical-layer security based on a multiscrolls system is developed and experimentally proved in an OFDM-PON system in this research. The suggested approach uses four-order grid multi-scrolls to produce chaotic sequences for encryption . The proposed approach can achieve a large key space. Additionally, a DFT precoding method can be used to increase the system's PAPR performance. The findings suggest that the proposed strategy can bring out considerable improvement in security and bit error rate (BER) performance of the system. [10]

Q. Zhang *et. al* [11] presented an image encryption system based on the AES algorithm, and implemented the algorithm in MATLAB The various methods for developing the AES algorithm are well discussed. First, the original image is converted into a 2D matrix form that the AES algorithm can use as input. The digital image can then be encrypted after completing certain rounds of operations. The comparison of the histogram analysis and the key analysis revealed that the method can better realise the effect of encryption and decryption.

D. M. Alsaffar *et al* [12]carries out a study to compare the encryption algorithms Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) for picture encryption in terms of encryption quality. According to the histograms obtained, the AES encrypted image has the most uniform histogram, meaning that RSA image encryption is less productive. MATLAB is used to implement both algorithms.

Some authors has investigated how encrypted images are transmitted using various versions of OFDM in [13, 14]. Image transmission through wireless channels like AWGN channel is carried out in these works. The image encryption quality is defined on the basis on peak signal to noise ratio.

Chapter 3

Cryptography

3.1 What is Cryptography

The practice of using codes to secure data and communications so that only the intended audience can decipher them is known as cryptography. It changes the original message's format from readable to unintelligible and vice versa. Cryptography is a science of coding messages secretly while cryptanalysis is a science of breaking codes. Different cryptanalysis types used for obtaining information are the chosen plain text attack,a known plain text cryptanalysis approach, and cipher text only attack. Cryptography is required in data and telecommunications when communicating over any untrusted media, particularly the Internet. Cryptographic encryption can be implemented either with symmetric keys which is a common key only known to the sender and receiver or with asymmetric keys (public keys). A pair of keys is used in an asymmetric key cryptographic system; That is public key- known to everyone and one private key -known only to the owner. For the secure exchange of datas between two parties symmetric-key encryption techniques they need to obtain the same cryptographic keys for enciphering/deciphering operations. Also it is highly essential to keep the key as secret. If an intruder somehow find the secret key, they can easily obtain the data being transmitted. Due to fore mentioned reason, symmetric keys are also known as secret keys. It is more faster than asymmetric systems and challenging to crack if a big key size is used. DES,3 DES and AES are some of the symmetric key Cryptographic algorithms [12]. Data Encryption Standard or DES cipher is used to encrypt data of length 64 bits with a key length of 56 bits. So the possible keys in DES

encryption is 2^{56} which was found too weak because of its limited key combinations and low resistance to brute force attack compared to AES.

3.2 Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a symmetric block cipher or cryptographic algorithm that is used to encrypt (encipher) and decrypt (decipher) any kind of information to eliminate unauthorized use of data. Encryption is a process of converting data into a scrambled form called cipher-text; decryption is the inverse process of encryption which converts the scrambled data back to its original form, called plaintext. Depending on three different key lengths 128, 192, 256 it is referred as AES-128, AES-192, AES-256. It takes 16 byte/128 bits as input block size. In AES enciphering method each whole round is made up of four distinct operations like substitution of every byte, permutation, the arithmetic performed over the finite field, and an exclusive- OR operation with the intial key. In this work the encryption operation AES-128 cipher is used. The units of measurement for data in AES are Bits, Bytes, Words, Blocks and State. The smallest unit is the bit, and other units can be expressed in terms of smaller ones [11]. The various terminologies and their definitions related to AES are

- Bit: A binary digit that can either be 0 or 1.
- Byte: A collection of 8 bits that can be arranged into a [1x8] matrix or an [8x1] matrix which is handled as a single unit.
- Word: A set of 32 bits that can be seen as a single entity and can be expressed as a 4-byte row matrix or a 4-byte column matrix.
- Block: A block in AES is 128 bits.
- State: They are composed of 16 bytes, just like blocks. It is treated as a 4x4 byte matrix.

3.2.1 AES Transformation Functions

1. Substitute Bytes

   The SubBytes/substitute byte transformation, is a table lookup which is of the order 16x16. A Substitution table is used to replace each byte from the input state with another byte (S-box). The resulting matrix is 4x4. The Inverse Substitute Bytes transformation applies the inverse S-box for every byte of the state and is thus the inverse operation of the Substitute Bytes transformation. It is obtained by first performing the inverse of the affine transformation and then performing the multiplicative inverse in GF (2^8).

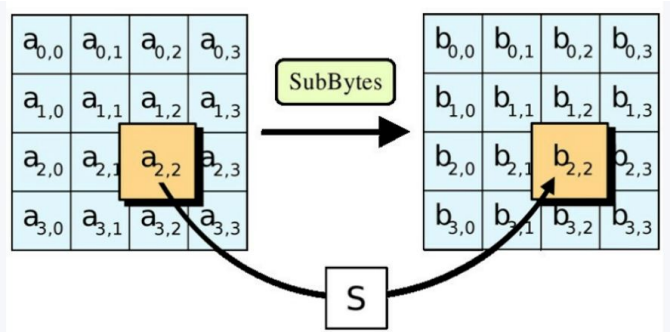

Figure 3.1: Illustration of byte substitution

2. ShiftRows Transformation

   The first row of State is not changed in the forward shift row transformation. Sucessive rows of the state array is shifted. A single byte circular left shift is applied for the second row. On the successive rows(3rd and 4th rows) a 2-byte circular left shift and a 3-byte circular left shift is performed respectively. Just like inverse substitution bytes, inverse Shift rows is also an inverse operation of shiftRows. The first row of the state array stays consistant. Bytes in the second, third, and fourth rows are shifted to the right by one, two, and three bytes, respectively.

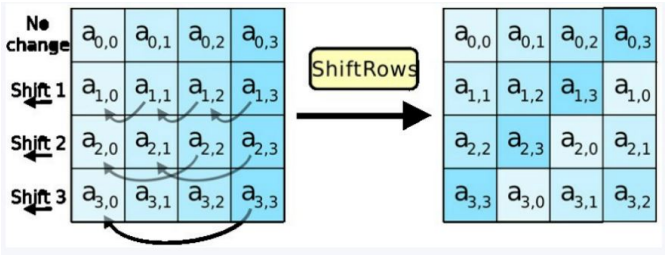

Figure 3.2: Illustration of ShiftRows Transformation

3. MixColumns Transformation

   The forward mix column transformation operates on each column individually. This is actually a matrix multiplication step. Each column is multiplied by a specified matrix, causing the position of each byte in the column to change. In inverse mix columns every column is multiplied with inverse of that specified matrix.

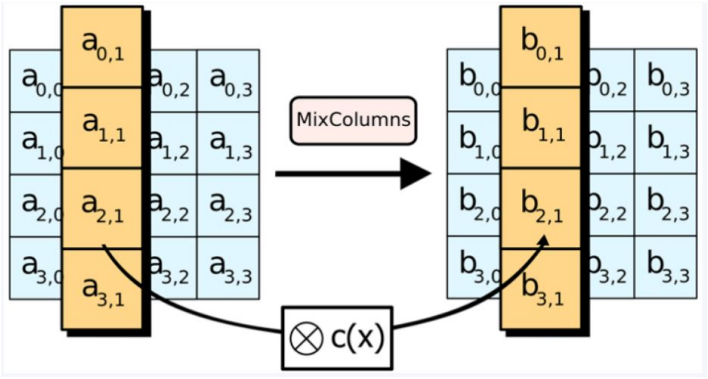

Figure 3.3: Illustration of MixColumns Transformation

4. AddRoundKey Transformation

   The Add Round Key operation is an Exclusive- OR of the 4x4 State and 4x4 round Key. By using the key schedule process, the round Key is derived from the cipher key. The state and round Key are the same size, and an XOR operation is performed per element to obtain the next State.

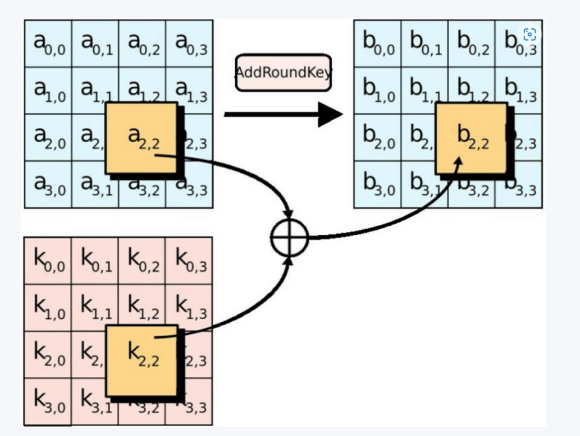

Figure 3.4: Illustration of AddRoundKey Transformation

3.2.2 AES Encryption and Decryption

AES requires input data of length 128 bit and a 128 bit key length for each round, therefore the input key must be enlarged to the necessary word count depending on the number of rounds. The encryption stage of AES cipher can be broadly divided into three phases: the opening round, the principal rounds, and the closing round. Each round uses the output of the preceding round as the input. Initially the add round key operation (XOR operation) is performed between each byte of the input data and the input key. The resulting output will be delivered as the input of the succeeding round [21]. After that he State array is modified by implementing a round function ten times (major rounds), with the last round varying somewhat from the first N-1 rounds. Main Rounds consists of SubBytes, ShiftRows, MixColumns and AddRound-Key whereas the final round consists SubBytes, ShiftRows and AddRoundKey. Then the last State is copied to the output. The round function is governed by a key schedule, which is a one-dimensional array of four-byte words obtained from the Key Expansion procedure.

The scrambled 128 bit data and the same secret key of 128 bits known to both communicating parties is the input to the decryption block.The Cipher functions are inversed and executed in reverse order to generate actual data being transmitted. The individual transformations used in the Inverse Cipher are InvShiftRows, InvSubBytes, AddRoundKey. Here, also a 10 rounds will be carried out and the only difference in

the decryption block is that the result of the KeyExpansion of each round will also be given to the MixColumns operation after which the AddRoundKey transformation should be carried out. In this work, the input to AES Algorithm is an image with secret nature is and the key is in hexa-decimal form. For encryption process first, dividing image and making it 4x4 byte state i.e. matrix format. Then calculate the number of rounds based on length of the key and expand it using our key schedule. The number of round will depend on the key size of the algorithm. Here AES-128 algorithm is used so, the number of round in AES encryption and decryption process is ten. The last round does not consist of mix column transformation in the iteration.

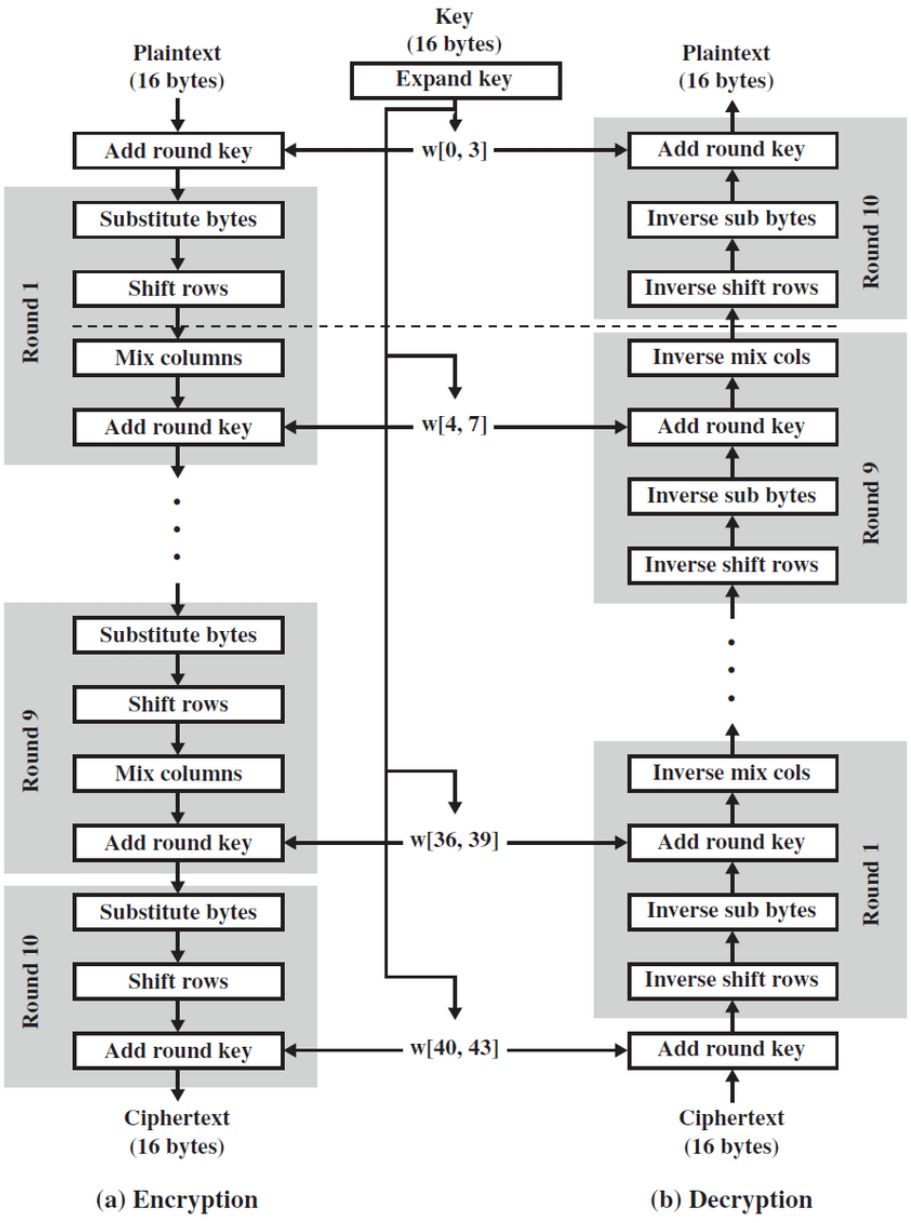

Figure 3.5: Encryption and Decryption process of AES

Chapter 4

Proposed Methodology

Optical/wireless networks are susceptible to a range of security attacks that try to obstruct service or gain unauthorised access to data being transmitted. Security flaws could cause clients to lose money or their privacy, and network-wide service interruptions could cause significant data and revenue losses. These attacks typically result in service interruption or eavesdropping as their type of damage. Signal insertion, signal splitting, and physical infrastructure attacks are only a few examples of security assaults on optical networks.Here,in this work, for the secure image transmission the encrypted image is transmitted through Optical CDMA network and then through FFT OFDM system. The advantage of the system is that encryption of data takes initially using AES enciphering. An additional security is provided when we transmit the signal using O-CDMA technology. Since it is a spread spectrum technology the encrypted signals stays hidden within the noise. The spreading process makes the interception process difficult for the eavesdropper. Thus the system acts as an improved security system. In orthogonal frequency Division Multiplexing, each subcarriers are orthogonal to each other and there wont be any signal interference. The encrypted signal signal transmitted can the recovered only at the lega ONU who receives the whole signal.

4.1 Image Transmission

The encrypted image is transmitted over two different channels, a fiber optic channel and wireless channel that is Additive White Gaussian noise Channel. The former channel make use of optical CDMA technology while the latter uses OFDM technique. Before transmitting over the channels the encrypted image is first converted into binary by using MATLAB tool.

4.1.1 Optical CDMA

Code-division multiple-access (CDMA) is a spread spectrum technique that is well known for its jam-resistant properties. This technique allows a large no. of users to share the same transmission bandwidth. In case of CDMA, the resources allocated per channel is power instead of bandwidth or time (codes are assigned to each user in the form of 0's and 1's). In CDMA technology the input signal is multiplied by the pseudo-random code generated with a multistage shift registers, to give the spread spectrum (SS) signal, spreading out the signal energy over a huge bandwidth. Therefore, the energy or power density stays in a lower level than the channel noise making the signal look like random noise. A photo detector can identify and decode the signal only when it knows the original pseudo random code with which the signal was encoded. Thus the pseudo random code performs the similar function as that of key for recovering the original information. Previously CDMA technology was applied to radio frequency communications systems, and eventually extended to optical domain.

Optical CDMA is technology that combines the flexibility of CDMA and the large bandwidth of the optical fiber. An optical signature sequence, or codeword, can be formed by sending a brief optical pulse during specific chip intervals but not others. Each user on the O-CDMA system has a unique signature sequence. The encoder of each transmitter represents each 1 bit by sending the signature sequence; A binary 0 bit, on the other hand, is not encoded and is represented as an all-zero sequence. Because each bit is represented by a pattern of illuminated and unilluminated chips, the data stream's bandwidth is increased. On an OCDMA system, adding a new client is as simple as allocating a new code, given that the extra (unutilized) codes

were provisioned when the network was deployed. In the absence of free codes, the system might be modified to handle more users by increasing the amount of time- or wavelength-domain spreading. Various types of codes proposed for Optical CDMA technology are 1-D codes, 2-d codes (time-spreading-wavelength-hopping codes) and 3-D codes.Orthogonal Optical Codes (OOC), Prime Sequence codes (PS). are some of the 1–D codes. The main disadvantage of 1–D code is that the temporal length.They have small code space for a given code length and is prone to brute force search attacks.To remove this drawback, 2–D and 3–D OCDMA codes are used.

Security in Communication networks are explained on the basis of confidentiality integrity and availability.O-CDMA provides both confidentiality and availability protection noise. Without knowing the code being used, it is complicated for an eavesdropper to successfully demodulate the O-CDMA signal, especially if numerous users are transmitting on various codes at the same time. So it is promising sensible choice in encrypting optical transmission links at the physical layer, which can improve the security of communication system against fibre-optic eavesdropping attacks. Physical-Layer Security by Optical CDMA Systems are based on the parameters like the type of code words, length of code words etc.

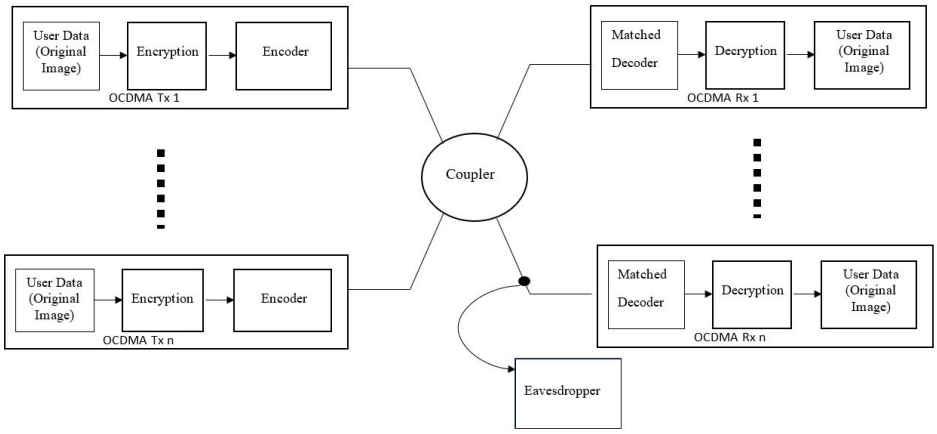

Figure 4.1: System model of AES- OCDMA security network.

Fig. 4.1 shows the system model enhanced security system based on OCDMA and AES. In the block diagram legal users uses a Legitimate channel for transmission and

Eavesdropper (unauthorized third party) tries to obtain the data sends between them. Cryptanalyst uses known-plaintext attack to eavesdrop information using a a wiretap channel. In the transmitter, the user's data is first encrypted by Advanced encryption Standard.This work mainly deals with the secure transmission of image data. So the original image is processed so that it can be used as input to the encryption algorithm.

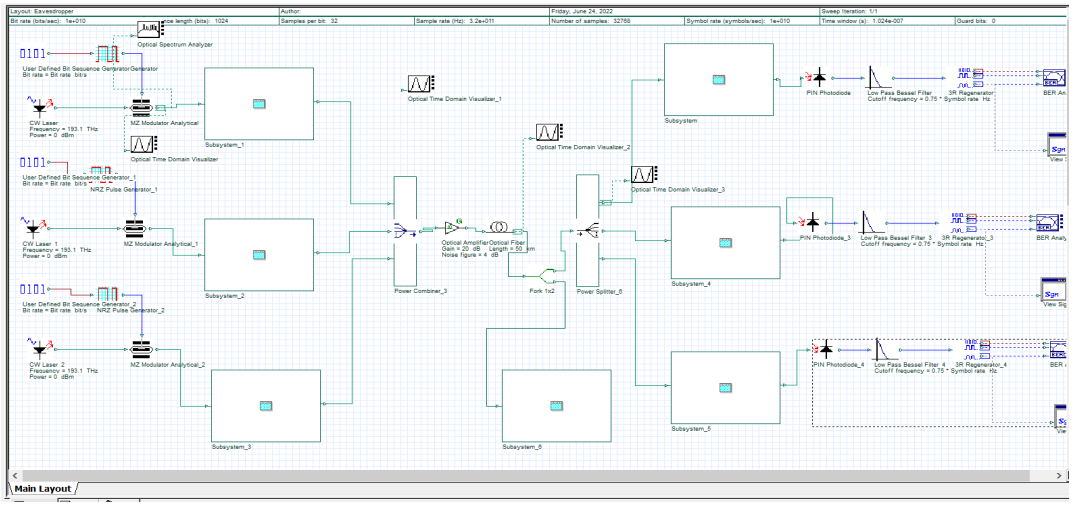

Figure 4.2: Simulation Diagram of AES- OCDMA security network.

The input image is converted is converted into two dimensional matrix and perform AES encryption. The encrypted image is converted into binary values. The binary values are loaded into User defined bit sequence generator component in optisystem. Then the data is OOK modulated by Mach-Zehnder modulator. The data is transmitted at transmission rate 10 Gbit/s, transmission power is 0 dBm and at wavelength 1550 nm. After that, encoding is ensured by optical encoder so that the data is hidden to others. Then, the signal is amplified by an Erbium Doped Fiber Amplifier (EDFA) and transmits. Bob employs the decryption method to recover data at the receiver following the associated optical decoding operation. The system can be accomplished using any optical code and encoder.

Inorder to increase the complexity of the system we can use a complex codes, so the corresponding encoder can be modified according the type of the encoder/decoder using. If time-spreading code is employed, an optical encoder is created by connecting Optical Delay lines (ODLs) of varying lengths to separate coupler ports. The delay of each port at the decoder is complementary to the delay of the associated en-

coder port. A time spreading Wavelength hopping code can be by using wavelength selective Switches and ODLs. This is a re configurable encoder in which each port of WSS corresponds to different wavelengths to realize wavelength-domain encoding. Different ports connect different lengths of ODL. At the decoding end, the matched decoder is realized by controlling the wavelength setting of WSS. Similarly, the delay of each port of the decoder is complementary to the delay of the corresponding port of the encoder. If Eavesdropper uses linear cryptanalysis method to attack the AES of cross-layer security system, he/she has to intercept the OCDMA code to get the output ciphertexts. The whole system can be simulated using MATLAB and Optisystem. The eye diagram obtained from the legitimate channel as well the Eavesdropping wiretap channel is obtained. The Q factor and the BER obtained gives the performance of the system.

4.1.2 Orthogonal Frequency Division Multiplexing (OFDM)

The goal of Orthogonal Frequency Division Multiplexing (OFDM) technique is to divide a high data rate stream into low rate streams that are delivered simultaneously over a number of orthogonal sub carriers. That is Instead of a single Wide band channel frequency, orthogonal frequency-division multiplexing divides a single information stream among numerous narrow band sub channel frequencies with close spacing. It is most commonly used in wireless data transmission, but it can also be used in wired and fibre optic communication. Each Sub-streams are orthogonal to each other. Signals that are perpendicular to each other are referred to as orthogonal signals. The fact that orthogonal signals do not interfere with each other is a key property of OFDM. When a signal is modified by the sender, its side bands extend out on either side. Only if the entire signal is received can a receiver correctly demodulate the data. Guard bands are used in OFDM to prevent signal interference and cross-talk. However, because orthogonal signals are used in OFDM, there is no interference between the signals even if their side bands overlap.Due to this property OFDM is said to be secure technique.The carrier spacing should be the reciprocal of the symbol period.

OFDM can tolerate significant channel disturbances (interference, frequency fading, multi-path propagation). To achieve excellent spectral efficiency and simple chan-

nel equalisation, OFDM employs the Fast Fourier Transform (FFT). For these reasons, optical OFDM has emerged as an appealing alternative for optical long-distance transmission, owing to its reduced signal bandwidth and straightforward digital equalisation of chromatic dispersion. Several performance parameters can measure the sharpness of an image after reception, including the Peak Signal to Noise Ratio (PSNR).Most often, ODFM is used to evaluate the quality of a reconstructed image.

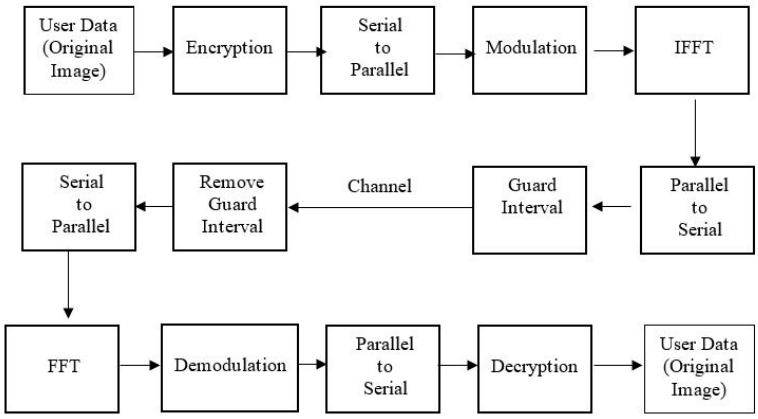

Figure 4.3: Transmission of encrypted image over OFDM

Figure 4.2 shows a block diagram FFT-OFDM system incorporated with an image encryption block on the transmitter part and an image decryption block on the reception part based on Advanced Encryption Standard. The encrypted image generated at the transmitter end which is an function of key and the actual image is given by a relation C = E (P;K), where P represents the original image, E represents the Cryptographic algorithm (here AES symmetric block cipher), K represents the encryption key, and C represents the encrypted image. Similarly, at the receiver end, the demodulated image is is subjected to AES decryption to obtain the original sent image. In this work, the input digital image data is converted to a 2D matrix format and again it is initially divided into a smaller matrices (blocks) for the encryption process. Each individual block is then encrypted with the same cipher key. The encrypted image data is subsequently converted to a multi-level complex number sequence using one of several modulation techniques. Quadrature Phase Shift Keying (QPSK) modulation is employed because of characteristics such as greater noise immunity, higher

transmission rate, and efficient bandwidth use. The modulated signals are grouped into blocks before being converted from frequency domain to time domain using the Inverse Fast Fourier Transform (IFFT). A guard interval is placed at the end of the transmitter between symbols with cyclic prefix (CP) to eliminate inter-symbol interference (ISI). The generated OFDM signal is then sent via a Additive White Gaussian Noise (AWGN) Channel. The inverse of the transmitter section actions are carried out at the reception end. The CP is initially eliminated from the receiving signal. The received signal is then converted into the frequency domain using FFT. Finally, the demodulation and decryption steps are performed to retrieve the original image.

4.2 Software Tools

4.2.1 Optisystem

Optisystem 19.0 is the software design suite introduced by Optiwave that is utilised for simulation of optical CDMA. It is a simulation tool for optical communication systems that enables for the design and test any type of optical link. The project files in optisystem are saved as .osd files. The Graphical User Interface (GUI) is in charge of the optical element layout and netlist, as well as component models and presentation illustrations. The OptiSystem Component Library contains so many components, all of which have been rigorously proven to give results comparable to real-world applications. Each component's parameters can be adjusted by the user by using its attributes or by adding additional datasets to the component. The user can select any component port and record the data, which is subsequently monitored when the simulation is completed. In addition, an arbitrary number of visualizers can be connected to the monitor at the same port. It can work in co simulation with MATLAB, simulink, python etc for simulating user defined optical systems. In the Component Library, OptiSystem accommodates mixed signal formats for optical and electrical signals. In order to anticipate system performance, OptiSystem calculates parameters such as BER and Q Factor.

4.2.2 MATLAB

MATLAB, or Matrix Laboratory, is a tool used for algorithm development, data collecting, modelling, simulation, and experimentation, along with many other purposes. It helps to obtain solutions of numerous technical computing challenges. MATLAB's several toolboxes enable users to learn and use particular technology. Toolboxes are large sets of MATLAB functions (M-files) that supplement the MATLAB platform to tackle specific tasks. Signal processing, image processing control systems, neural networks, simulation are of the toolboxes. It is a high-level matrix/array language with functions, data structures, and other capabilities that enables for the creation of both short throw-away programmes and big complicated application programmes. The MATLAB Graphic User Interface includes the command window, workspace browser, current directory and command history window, editor, and figure windows. The editor window is used to code and model systems, the command window displays command outputs, the current Directory tab displays the contents of the current directory, and the figure window is displayed only when there is a graphic output.

Chapter 5

Simulation Results

5.1 AES-OCDMA Security System

AES-OCDMA is simulated using Optisystem software.The user can correctly decode the image only if they poses both the OCDMA unique signature code and the same AES Encryption key that we used for encryption. Different delays are used in the encoders of different users. Delay used in the encoder are 0.003 ns, 0.018 ns, 0.033 ps, 0.0517 ns, 0.068 ns. Their corresponding decoders uses complementary delays of the encoder. The Encrypted image is transmitted at a transmission rate 10 Gbps and transmission power 0 dBm. The eye diagram obtained for the legal user has a better eye opening than that of illegal user. The standard measure of success for digital communication links is the bit error rate. It can be defined as the percent of bits with mistakes in comparison to the total number of bits gathered in a transmission. It describes how information should be resent when a communication channel has been distorted when noise, interference, or bit synchronisation issues have occurred. The typical error rate for optical communication systems falls between $10^{-9}$and 10^{-15}. If the error rate is 10^{-9}, it indicates on an average one error occurs for every one billion pulses send BER is defined as $BER = \frac{1}{2}erfc(Q/2)$.

Quality factor is defined as $Q = \frac{|\mu 1 - \mu 2|}{(\sigma 1 - \sigma 2)}$
Where $|\mu 1 - \mu 2|$ is the difference between high and low intensity levels, and $|\sigma 1 - \sigma 2|$ is the standard deviations sum of intensities around the upper and lower intensity levels. From Fig. 5.1 and 5.2 it is clear that the quality factor obtained from the eye diagram

of the legal user is 11.57 and BER is 2.572 e^{-31}. For illegal user the the quality factor is 4.38 and BER is 5.7452e^{-6}. The large vertical and horizontal eye openings indicate the signal's quality. This Shows that the legal user who has keys only gets the image data without much distortions than the interceptor who tries to obtain the image data.

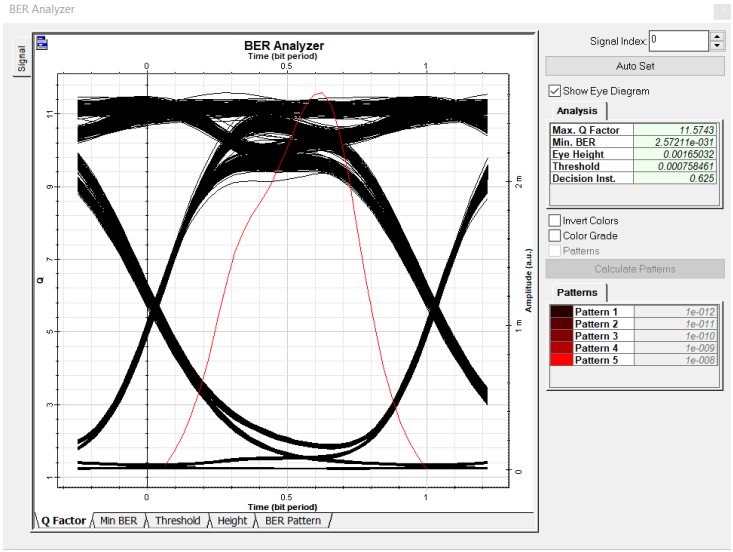

Figure 5.1: Eye Diagram obtained from the legitimate user

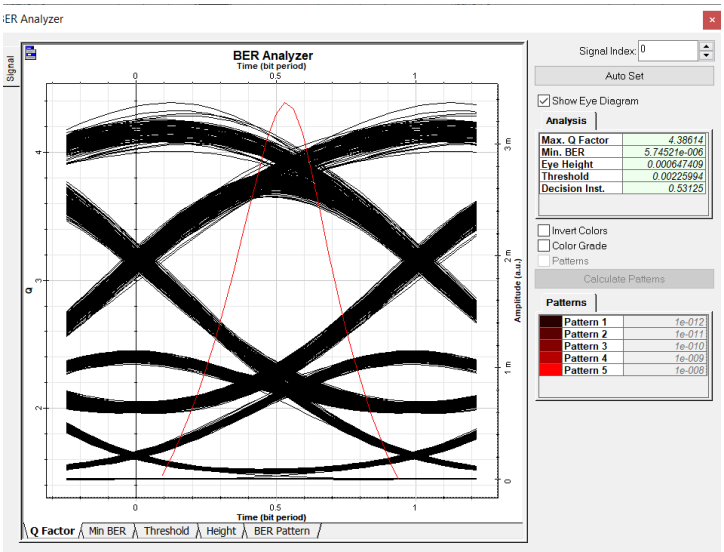

Figure 5.2: Eye Diagram Obtained from the illegal user

5.2 AES-OFDM Security System

Security performance of the proposed system are investigated by carrying out simulation experiments in MATLAB. The system allows the user to select the image the wish to send.Then it check whether the image is RGB or Gray. In the case where an RGB image is chosen, first it is converted to Gray scale and then AES encryption is carried out. The quality of encryption can be measured on the basis of parameters like noise immunity, histograms etc. A picture's histogram illustrates the probability of the occurrence of each grey level in the image. It plots the number of pixels for each tonal value. The ciphertext image histogram analysis is one of the simplest ways for demonstrating image encryption quality. A decent picture encryption algorithm encrypts a plaintext image into an unintelligible form.As a result, a successful image encrypting approach yields an encrypted image with a histogram of evenly distributed intensity. The grey level intensities run from 0 to 255 on the histogram's X axis, with a 50-point gap while Y axis shows the number of pixels. Fig 5.3 show the original image and its histogram while figure 5.4 show the encrypted image and its histogram. The evenness in the histogram of encrypted image shows that the AES- OFDM system is a good quality security network.

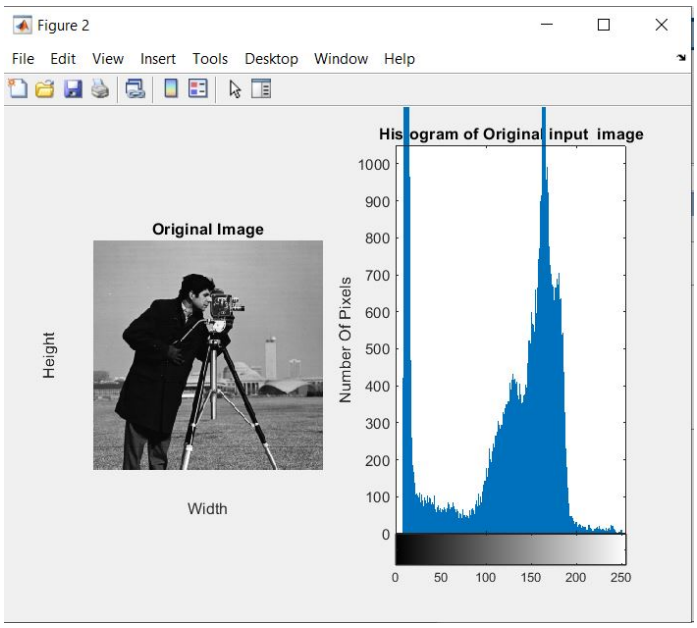

Figure 5.3: Input image and histogram

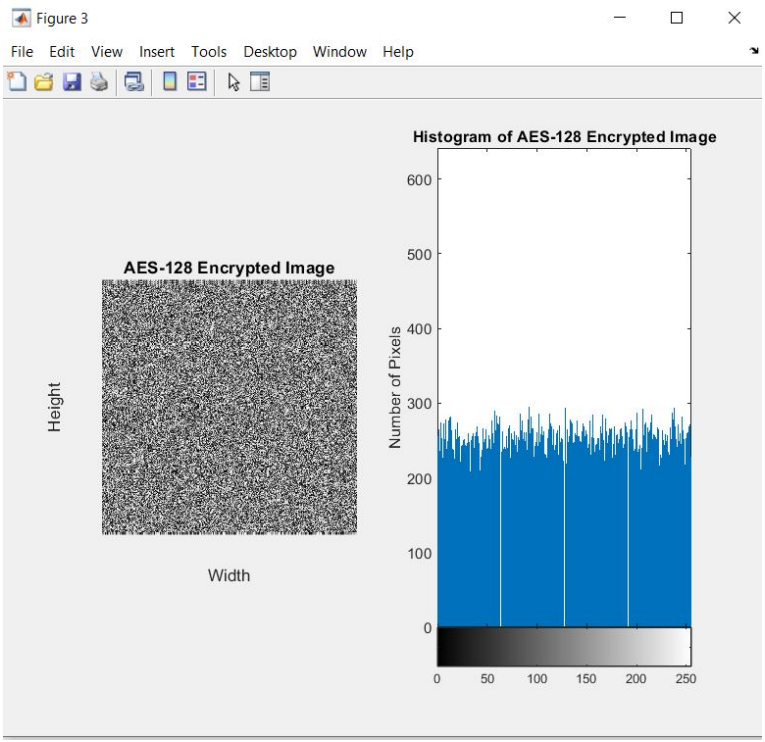

Figure 5.4: Cipher image and histogram

Figure 5.5 depicts the histograms of both the encrypted and original images. The number of pixels for each tonal value is plotted in the histogram of the original image before encryption. The intensities of the enciphered image is almost same everywhere makes it unintelligible to the unauthorized user.

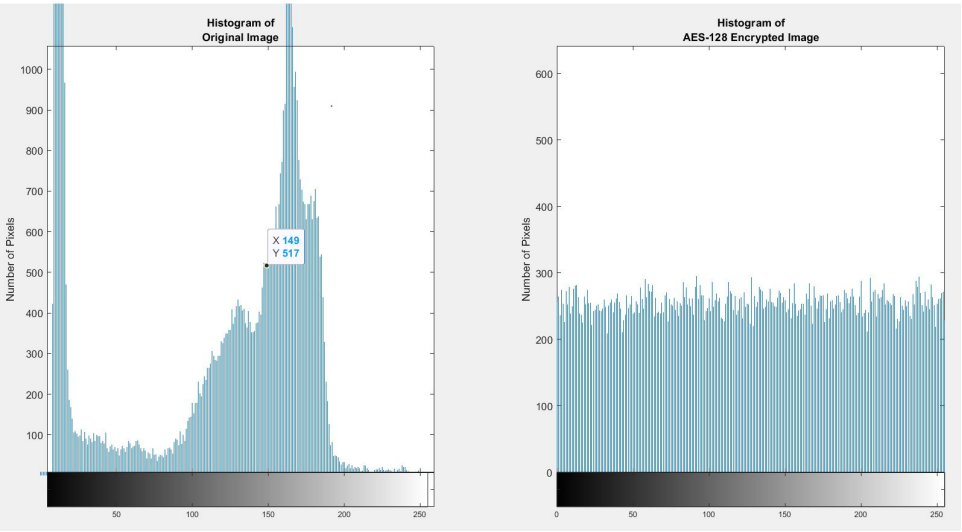

Figure 5.5: Comparison of histogram of Original and cipher image

The encrypted image is transmitted over FFT-OFDM system. FFT treats the input as a time domain component and turns it into a frequency domain component.The OFDM system parameters is defined in table 5.1. In contrast to its counterpart, IFFT, which treats the input as a frequency domain component and transforms it into time domain. IFFT is applied on the transmitter side.

Table 5.1: OFDM system parameters

Parameter	**Value**
Modulation Type	QPSK
Modulation Order (M)	4
Guard Intervel	Cyclic Prefix
OFDM Cyclic Prefix Length	32
Range of SNR	-10 to +10 dB

figure 5.6 shows BER Vs. SNR for AES Encrypted Image Transmission using OFDM System with QPSK Modulation in AWGN Channel. The signal to noise ratio (SNR) is a typical metric used to assess the quality of a communication link.The range of SNR for the proposed system is extends from -10 to +10 dB. The obtained curve shows that the signal to noise ratio is inversely proportional to Bit Error Rate(BER).

A higher SNR signifies a lower error rate and better performance.

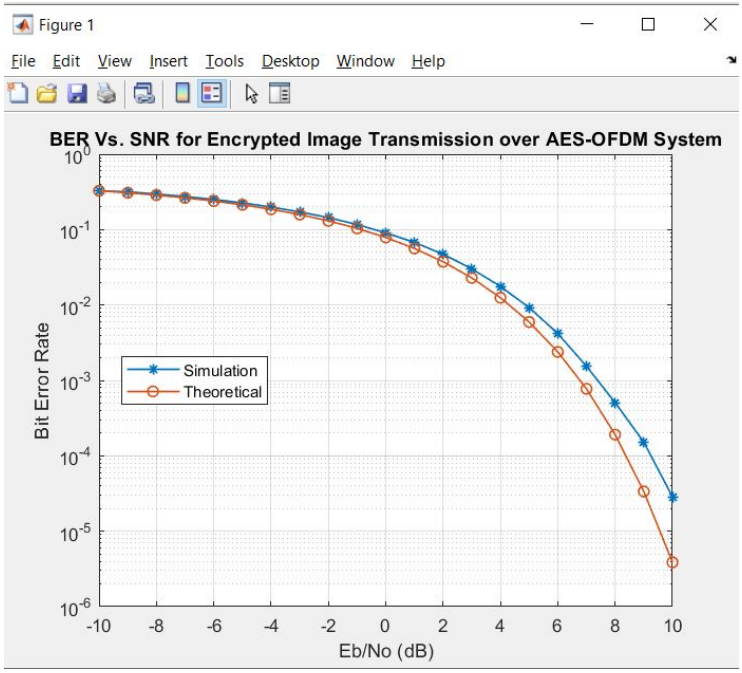

Figure 5.6: BER Vs. SNR for Encrypted Image Transmission over AES-OFDM System

The peak signal to noise ratio (PSNR), which is computed by comparing the actual image and the encrypted image, is used to assess the quality of the decrypted images at the receiver. PSNR is measured in decibels. The elevated PSNR indicates that the encrypted image is more accurate. Fig 5.7 shows AES decrypted image at FFT OFDM Receiver. When the signal to noise ratio is 9 dB and 10 dB, the retrieved image exhibits high quality.

$PSNR = 10log_{10}(\frac{255^2}{MSE})$

The PSNR values of the decrypted image is obtained at different different SNR values. It is observed that PSNR values are low when SNR is zero. As the signal to noise ratio increases, the encryption quality of the image increases as shown in figure 5.8 The variation of decrypted picture PSNR with simulated BER is shown in Fig. 5.9. This graph shows that the AES encryption technique achieves acceptable PSNR values even in the presence of errors.

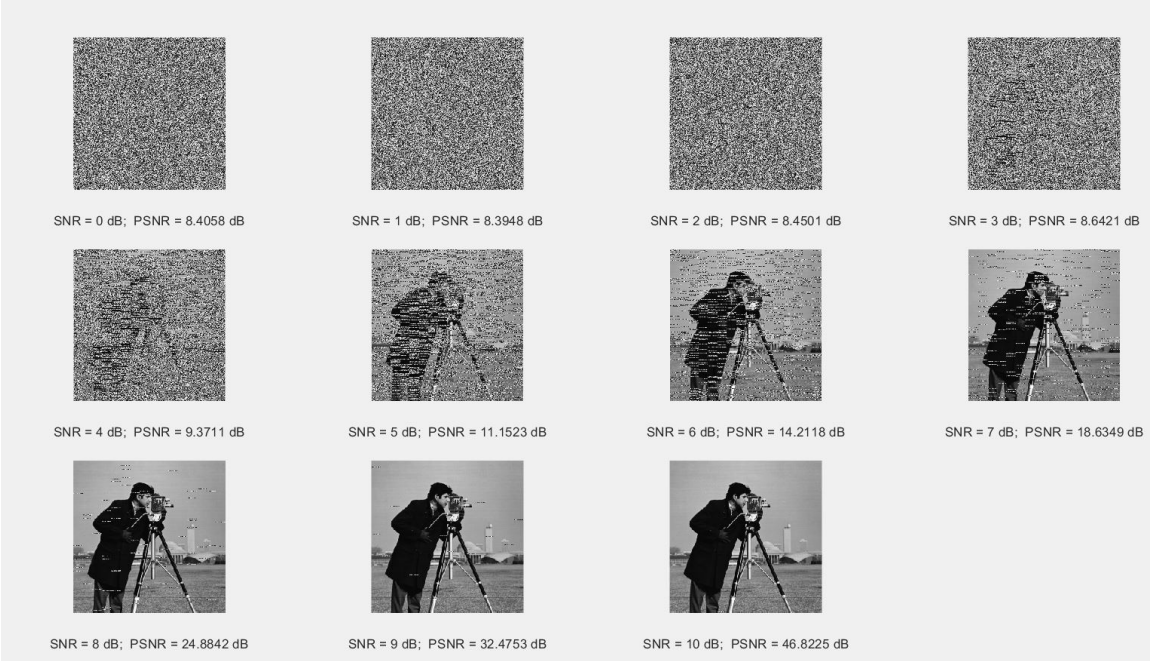

Figure 5.7: AES Decrypted Image at OFDM Receiver for different SNR

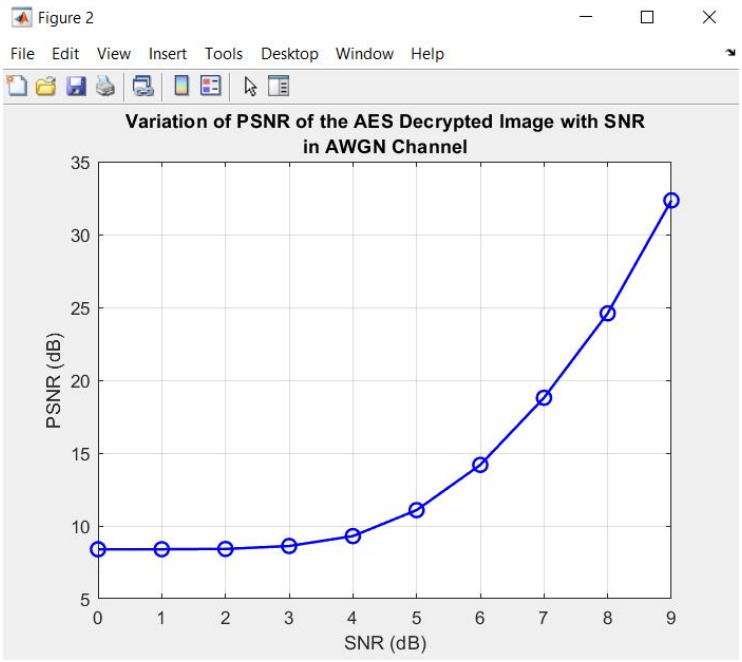

Figure 5.8: Variation of PSNR of the AES Decrypted Image with SNR in AWGN Channel

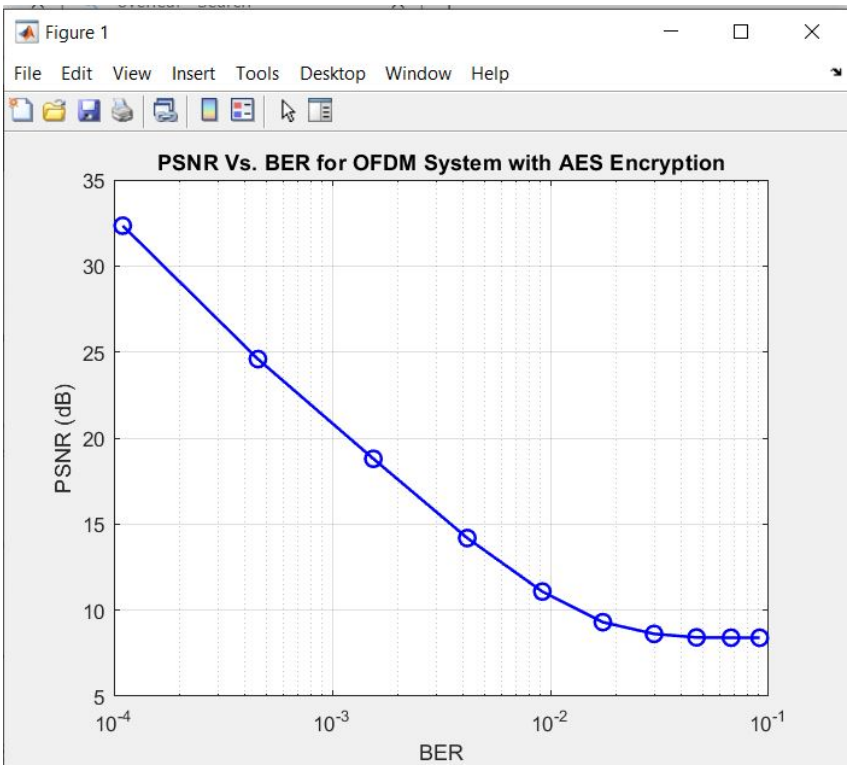

Figure 5.9: PSNR Vs. BER for OFDM System with AES Encryption

Chapter 6

Conclusion & Future Scope

A more secured data transferring method to maintain data hiding which is mix of cryptography and optical encoding is proposed in our system. The data encrypted using AES algorithm is again subjected to optical encoding using OCDMA. That is, interceptor can retrieve images only when the matched decoder and the correct encryption key are employed together. The evaluation on degree of confidentiality offered by the system is carried out and also it is simulated using optisystem software. Inorder to improve the security on the system more complex code that that is difficult to break and any PSK modulation can be used. It is difficult for the interceptor to detect the signal passing through the channel. An interceptor tries a random decoder to decode the transmitted signal. Corresponding data obtained is cipher data. The intruder will be able to obtain an intelligible information only when they break the encryption key also. The Bit Error Rate and Q- factor of the legitimate channel and eavesdropping channel indicates that the legal user end receives the transmitted data accurately than the eavesdropping channel that uses a random decoder and random key. But the requirement of people to transmit a huge amount of data with high data rate and without losing performance and efficiency is a challenge. OFDM is the one of the brightest technique to overcome the challenge. So a communication link using an OFDM modulation technique is established and secured it using the AES cipher. The encryption quality is measured on the basis of PSNR value and histograms. The uniformity of the obtained histogram indicates the quality of encryption and the encrypted image transmitted over AWGN channel is decrypted with correct key to obtain the original image.

As WDM allows for a massive increase in capacity, Wavelength Division Multiplexed Passive Optic Network will be the future technology capable of meeting all bandwidth demands for future generations. Cryptographic alogorithms like AES implemented wavelength division multiplexed OFDM PON is worth studying in future to realize a secured, high datarate network with improved spectral efficiency.

References

[1] T. Shake, "Security performance of optical cdma against eavesdropping," *Journal of Lightwave Technology*, vol. 23, no. 2, pp. 655–670, 2005.

[2] T. H. T.Shake, "Confidentiality performance of spectral-phase-encoded optical cdma," *Journal of lightwave technology*, vol. 23, no. 4, p. 1652, 2005.

[3] V. Jyoti and R. Kaler, "Security enhancement of ocdma system against eavesdropping using code-switching scheme," *Optik*, vol. 122, no. 9, pp. 787–791, 2011.

[4] A. Cherifi, N. Jellali, M. Najjar, S. A. Aljunid, and B. S. Bouazza, "Development of a novel two-dimensional-swzcc – code for spectral/spatial optical cdma system," *Optics & Laser Technology*, 2019.

[5] Y. Tan, T. Pu, H. Zhou, J. Zheng, G. Su, and J. Liu, "Design and performance analysis of a novel secure communication system based on optical code division multiple access technology," *Optical Fiber Technology*, vol. 58, p. 102254, 2020.

[6] U. Bhanja and S. Singhdeo, "Novel encryption technique for security enhancement in optical code division multiple access," *Photonic Network Communications*, vol. 39, pp. 195–222, 2020.

[7] W. Li, J. Ji, G. Zhang, and W. Zhang, "Cross-layer security based on optical cdma and algorithmic cryptography," in *2016 IEEE Optoelectronics Global Conference (OGC)*. IEEE, 2016, pp. 1–2.

[8] J. Ji, W. Li, B. Wu, K. Wang, M. Xu, and L. Sun, "Design and investigation on image transmission in multi-user cross-layer security network," *IEEE Access*, vol. 7, pp. 132 066–132 073, 2019.

[9] H. S. Gill, S. S. Gill, and K. S. Bhatia, "A novel approach for physical layer security in future-generation passive optical networks," *Photonic Network Communications*, vol. 35, no. 2, pp. 141–150, 2018.

[10] Y. Xiao, Z. Wang, J. Cao, C. Long, Y. Chen, R. Deng, J. Shi, Y. Liu, and J. He, "Two-level encryption for physical-layer security in ofdm-pon based on multi-scrolls system," *Optics Communications*, vol. 440, pp. 126–131, 2019.

[11] Q. Zhang and Q. Ding, "Digital image encryption based on advanced encryption standard (aes)," in *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 2015, pp. 1218–1221.

[12] D. M. Alsaffar, A. S. Almutiri, B. Alqahtani, R. M. Alamri, H. F. Alqahtani, N. N. Alqahtani, A. A. Ali *et al.*, "Image encryption based on aes and rsa algorithms," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2020, pp. 1–5.

[13] K. Dharavathu and S. A. Mosa, "Efficient transmission of an encrypted image through a mimo–ofdm system with different encryption schemes," *Sensing and Imaging*, vol. 21, no. 1, pp. 1–31, 2020.

[14] I. Eldokany, E.-S. M. El-Rabaie, S. M. Elhalafawy, M. A. Zein Eldin, M. H. Shahieen, N. F. Soliman, M. A. El-Bendary, M. A. El-Naby, F. S. Al-Kamali, I. F. Elashry *et al.*, "Efficient transmission of encrypted images with ofdm in the presence of carrier frequency offset," *Wireless Personal Communications*, vol. 84, no. 1, pp. 475–521, 2015.

[15] A. Sultan, X. Yang, S. B. Hussain, and W. Hu, "Physical-layer data encryption using chaotic constellation rotation in ofdm-pon," in *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. IEEE, 2018, pp. 446–448.

[16] B. V. Naik, N. L. K. Sai, and C. M. Kumar, "Efficient transmission of encrypted images with ofdm system," in *2017 IEEE International Conference on Power,*

Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 2383–2388.

[17] N. S. S. Srinivas, "Ofdm system implementation, channel estimation and performance comparison of ofdm signal," in *2015 13th International Conference on Electromagnetic Interference and Compatibility (INCEMIC)*, 2015, pp. 212–219.

[18] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 110–117, 2016.

[19] J. Yu and N. Chi, *Digital Signal Processing in High-Speed Optical Fiber Communication Principle and Application*. Springer Nature, 2020.

[20] S. Komeylian and S. Komeylian, "Deploying an ofdm physical layer security with high rate data for 5g wireless networks," in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2020, pp. 1–7.

[21] J. Kaur, S. Lamba, and P. Saini, "Advanced encryption standard: Attacks and current research trends," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 112–116.