JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 09, 2020

Secure image transmission through an OFDM and MIMO OFDM systems with different cryptographic algorithms

Tabish Rao,
Asst. Professor, SOC (School of computing),
GEHU-Dehradun Campus
DOI: 10.48047/jcr.07.09.582

Abstract:

Data security and privacy concerns are now hindering the development of wireless communication networks. The need for a secure and dependable wireless network to transmit digital data (including text, images, and video) between origin and destination is growing. There are two main tiers at which security may be implemented: the data layer and the network layer. Encryption methods are used to ensure the safety of the data itself. They immediately operate on the data to alter its proper format, making interpretation more difficult. However, network-level security entails implementing certain network-related security processes to protect data from unwanted access through the network. Secure data transfer (in the form of pictures) through an air interface is the focus of this work, which focuses on the former type of security in wireless communication systems.

Keywords: wireless communication, text, image, and video, encryption, secure transmission

Introduction

Nowadays, the world becomes a global village due to the advances in technology, primarily Technology for wireless communication. Today, large volumes of digital data are transferred over the wireless digital communication system using standard digital technology and the internet at exceptional speeds. In the blink of an eye, a great deal of information is created and transferred across the wireless communication system in the form of digital multimedia data like picture, audio, and video. The digital communication system offers several benefits over the analog one, including improved quality, more flexibility in editing and duplicating, etc. Numerous unauthorized parties attempt to intercept digital multimedia data as it travels via a wireless communication system before it reaches its intended recipient. Even as the global number of cyberattacks continues to rise dramatically, it must ensure that our data remains secure. Everyone must now think about cyber security. Therefore, several cryptographic systems are utilized to safeguard data from cybercriminals. Encryption is a technique used in cryptography to ensure that only the intended recipient can read the contents of a message by transforming it from its original form (called plaintext data) into an unreadable garbage format (called ciphertext data). Decryption is the process of turning encrypted information back into its original, unencrypted form. In today's crowded and loud digital world, people still expect fast data transfer speeds and robust security. In order to achieve high data transmission rates in a noisy environment, the OFDM system is often implemented as a multi-carrier scheme. In a multipath environment, increasing data speeds may be achieved by using several antennas at both the transmitter and reception ends. By incorporating antenna diversity into the OFDM system, a greater data rate may be attained without the need for any supplementary resources or bandwidth extension. Orthogonal frequency division multiplexing (OFDM) and multiple-input and multiple-output based

orthogonal frequency division multiplexing (MIMO-OFDM) systems are discussed here because of their prevalence in modern digital wireless communication architectures. Both the 2x2 and 4x4 antenna diversity techniques are taken into account in MIMO-OFDM systems. Bit error rate (BER) and peak signal to noise ratio (PSNR) are used to assess the picture quality after recovery under various signal-to-noise (SNR) situations. The primary goal of the paper is to provide a safe method of sending images over the internet. Data and picture security is often provided by cryptographic techniques. Several fundamental procedures are used in the development of cryptographic algorithms. Permutations, rotations, operations involving logic, arithmetic operations, and replacements all fall under this category. The data is redundant due to the use of encryption techniques. A well-designed encryption system will be more difficult to crack and will have fewer security flaws. Crypto wireless communication systems are realized by making small adjustments to the basic-system designs (OFDM and MIMO-OFDM) by adding encryption and decryption devices at the transmitter and receiver ends. In this study, we investigate the safety of sending images using a crypto-system over an AWGN channel. Block ciphers such as the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and the Rubik's Cube are implemented into the aforementioned system for further security. The quality of recovered pictures in crypto-systems is being studied as part of the inquiry. A secondary focus of this study is a statistical performance-based evaluation of the relative resilience of various encryption schemes. Additionally, it places a premium on crypto-system performance analysis rather than basic-system performance study. The whole system has been built using MATLAB. Based on the findings, it is clear that antenna diversity technology and encryption algorithms have been successfully integrated in an effective and secure communication system. It is always necessary to trade up security for better system performance (in terms of BER, PSNR, and the quality of the recovered picture). The Rubik's Cube algorithm is used to create a cryptosystem with performance almost on par with that of the barebones systems (OFDM and MIMO-OFDM). For the same set of channel circumstances, introducing cryptographic techniques has little to no negative effect on performance. The suggested Crypto-MIMO-OFDM systems provide efficient and secure picture transmission at a modest cost to signal-to-noise ratio (SNR). Therefore, the Internet, medical transcription, banking, etc., may be examples of real-time applications that might benefit from using such technologies.

The main goal of this project is to develop an OFDM communication system for the transmission of visual content. Binary phase change keying (BPSK), quadrature phase shifting keying (QPSK), quadrature amplitude modulated (QAM), 16-phase shift keying (PSK), and 16-phase shift keying (QAM) are all used in the construction of an OFDM system for use over an AWGN channel utilizing a rapid Fourier transform. From a communication standpoint, we analyze the system's performance by measuring parameters like PSNR, BER, and the quality of the recovered picture. Wireless communication is the process of exchanging data between nodes via an air interface or radio interface. These days, wideband communication technologies are the norm. Having a reliable wireless interface that can handle very high data rates is essential for a wide variety of radio users. Extremely high data rates, necessitating large bandwidths, will be necessary for future mobile communication systems. There is a restriction on the system's capacity due to the radio interface's features. The next paragraphs will go through a few of the most prominent distinguishing aspects.

Propagation Along Multiple Paths: The strength of a radio frequency (RF) signal increases as it travels away from its source. On its approach to the receiver, a radio frequency (RF) signal is affected by a number of obstacles. When an RF signal reflects off an object, it splits into numerous waves that each go in a different direction. When radio frequency (RF) impulses travel in several directions, a phenomenon known as multipath propagation occurs. Since the reflected RF waves have a longer route to travel and reach later compared to a direct RF

wave, this causes a delay in the signal's overall arrival time. High-rise structures, hills, water features, walls, coated glass, and other metallic or RF-reflective surfaces may all contribute to multipath propagation. Due to the longer transmission distance, more RF energy is lost in the reflected signal compared to the direct route signal. At the receiver, the desired wave joins forces with several reflected waves. A reflected wave in multipath propagation moves away from an unreflected wave. Null points along the course of a signal are formed in a multipath environment and are a function of frequency. It alters the receiving signal's amplitude and phase. Due to the Multipath effect, information symbols overlap and the receiver becomes muddled. Bit errors will arise if the delays are long enough. Changing the antenna's position alters the pattern of reflections, reducing the likelihood and impact of multipath interference. The term "multipath" refers to the addition of the original signal to any reflected waves that have formed intermediate the transmitter and the receiver due to obstructions in the path. Line of sight (LOS) transmission is the most common method above 2 GHz. Therefore, there must be little obstruction between the transmitter and receiver.

When using a communication connection with a high delay spread (m), the symbols will be exposed to intersymbol interference (ISI). As long as the symbol time, T, is greater than the number of carriers, m, a multicarrier modulation may reduce ISI. Slowdown dominoed: The delay spread is the time it takes for all reflected signals to reach their destination after the first main signal has arrived. It is often given in units of nanoseconds.

- Fading: Both the coherence bandwidth and the coherence duration are essential channel characteristics. There are four forms of fading that a wireless channel may impose on a signal, and they all depend on the signal's bandwidth and symbol period. A frequency-flat or flat-fading channel exists when the signal bandwidth is less than the channel's coherence bandwidth. The channel exhibits frequency selectivity if used otherwise. The communication channel is time-invariant if and only if the symbol period is less than the coherence time. The channel exhibits frequency selectivity primarily in high rate of data systems. A signal's amplitude, phase, and latency may all be affected by the many pathways it takes to reach the receiver. Multipath fading, also known as small-scale fading, is a phenomena in which the received signal intensity varies greatly over time as a consequence of interference from several paths. Doppler shift refers to the frequency shifts that occur along a transmission route as a result of a moving item.
- Doppler spread: Doppler spread refers to the fading caused by the contributions of signal components with varying Doppler shifts. Fast fading of the received signal occurs if its Doppler spread is large in relation to the signal's bandwidth. Slow fading occurs when the spared is smaller than the signal's bandwidth.
- Inter Symbol Interference ISI: Inter Symbol Interference (ISI) describes the effect of several reflections of the broadcast signal arriving at the receiver at various times and being combined destructively, resulting in the crashing of the bits hooked on each other. Fading of the signal is also introduced. Frequency-selective channels also produce fading in the signal and are linked to the delay spread, both of which contribute to Inter Symbol Interference (ISI).

Multi-Carrier Systems

The whole of the available bandwidth of a single carrier system is allocated to a single data stream. Single carrier systems are basic and straightforward to deploy. Problems with intersymbol interference (ISI) arise in wideband applications that employ single-carrier modulation methods, which need short symbol durations. In order to counteract ISI, it is

required to use robust equalization at the receivers, which in turn increases the computational receiver complexity. Wideband single-carrier systems benefit from various multiplexing strategies that increase their spectral efficiency. By allocating distinct time slots to each information stream, time-division multiplexing (TDM) is the most popular method for transmitting several signals over a single transmission medium. Only one source's signal is broadcast during each time slot, thus data from other sources doesn't mix. Because of this, TDM may be considered orthogonal. Sub-band multiplexing is another applicable approach, which involves splitting the available bandwidth into smaller channels before sending them out. Frequency division multiplexing (FDM) is another name for these setups, along with multitone and multi-carrier. In the 1960s, the idea of using frequency division multiplexing and parallel data transmission was presented. To broadcast numerous data streams simultaneously, the multi-carrier technique divides the available radio channel into a large number of sub-channels. As a result, multipath effects may be reduced by lowering the symbol rate on each subcarrier. The available carriers determine which sub-bands will be used for which data streams, or occasionally a single stream may be split into many streams. Narrowband sub-channels have a very stable frequency response, reducing the impact of signal fluctuations due to frequency shifts. When compared to a single carrier system operating at the same bandwidth, this greatly simplifies equalization. Inter-carrier interference (ICI) and cross talk may be mitigated with the use of wider sub-band spacing. The multi-carrier system's spectral efficiency suffers as a result. Reducing the subcarrier spacing through ISI or/and ICI increases the spectral efficiency of a multi-carrier system. To do this, carriers with an orthogonal relationship to one another should be chosen. Orthogonal frequency division multiplexing is the technical term for this method. Most FDM systems are orthogonal in the continuous frequency domain because the transmission signals are orthogonally spaced in frequency. OFDM is a special instance of frequency-division multiplexing.

Literature Review

Avuthu Yuvaraja Reddy et.al.,(2020) In today's information age, it's crucial that data be sent in whatever way possible. One of the main difficulties in communication is ensuring the error-free transmission of these many types of data using present technology, given the constraints of limited bandwidth. We explain the results of a performance analysis of OFDM using ML detection applied to the transmission of picture, text, and audio digital data. Under the assumption of an AWGN channel model, we compare PSK to 4, 16, 32, and 64 QAM with a signal-to-noise ratio (SNR) of 0-30 dB. Analysis based on Mean Square Error as well as Bit Error Rate is performed for verification. Based on the findings, OFDM with ML classification is the most effective mode for transmitting text among those considered in the research.

Jay Patel et.al.,(2020) OFDM, or orthogonal frequency-division multiplexing, is a method of digital communication that uses several carriers to combat issues unique to digital transmissions, such as intersymbol interference (ISI), insufficient data rates, and interference between carriers. Multiple low-rate carriers are used to create a high-rate network for transmitting data. The extended symbol durations of each low data rate carrier are sufficient to completely do away with ISI. With orthogonality, the carrier frequencies may overlap one another closely without inducing intercarrier interference (ICI). This paper's contribution is an evaluation of the feasibility of real-time OFDM RF communications. A lightweight CPU, web camera, and software-defined radio were embedded and integrated utilizing the Mathworks MATLAB environment to do this. The transmission of real-time video feeds for surveillance and monitoring is facilitated by this method. Live pictures were sent from the

webcam at a steady frame rate to the SDR, which then relayed the data to a second SDR located at a different location.

Zhongpeng Wang et.al.,(2019) In this research, we present a technique for picture data transmission over OFDM systems that combines compression encryption with symbol scrambling. The simulation results demonstrate the effectiveness of the proposed technique in achieving both secure transmission in the physical layer as well as efficient secure block compressive sensing. Together, compression-encryption and symbol scrambling strengthen the privacy of the transmitted picture data.

Libertario Demi et.al (2018) Both multi line transmissions (MLT) and orthogonal frequency division multiplexing, or (OFDM) have been used independently to speed up the pace at which ultrasound images may be acquired. Generating several beams during the broadcast phase degrades picture quality for both modalities. In particular, image errors arise from interbeam cross-talk, the strength of which grows in proportion to the number of beams transmitted simultaneously. Here, we conducted experimental research to see whether and how MLT and OFDM may be utilized together to increase the quantity of parallel beams while simultaneously decreasing cross-talk. Different configurations, i.e. with 2 to 6 beams broadcast in parallel, have been used to capture and interpret ultrasound pictures of wire target and of a tissue-mimicking phantom. Contrast ratio, contrast-to-noise ratio, axial resolution, etc interbeam cross-talk are only few of the imaging properties that have been tested. Overall, combining MLT with OFDM is beneficial for increasing the data collection rate while decreasing the amount of cross-talk and improving the CNR, at the expense of some axial resolution and a minor drop in CR.

Block Diagram of OFDM System

Orthogonal frequency division multiplexing (OFDM) is a novel modulation technology for use in wireless communication systems that has a number of improvements over previous methods (see Figure 1). Below, we covered the fundamental steps required to put the OFDM system into action. Since most images are captured in just two dimensions, preprocessing is required before they can be used in any analytical software. This digital information is then modulated using one of many techniques (BPSK, QPSK, QAM, 16-PSK, or 16-QAM) into a multilevel series of complex numbers. Using a serial-to-parallel converter, these modulation symbols are organized into FFT-sized chunks.

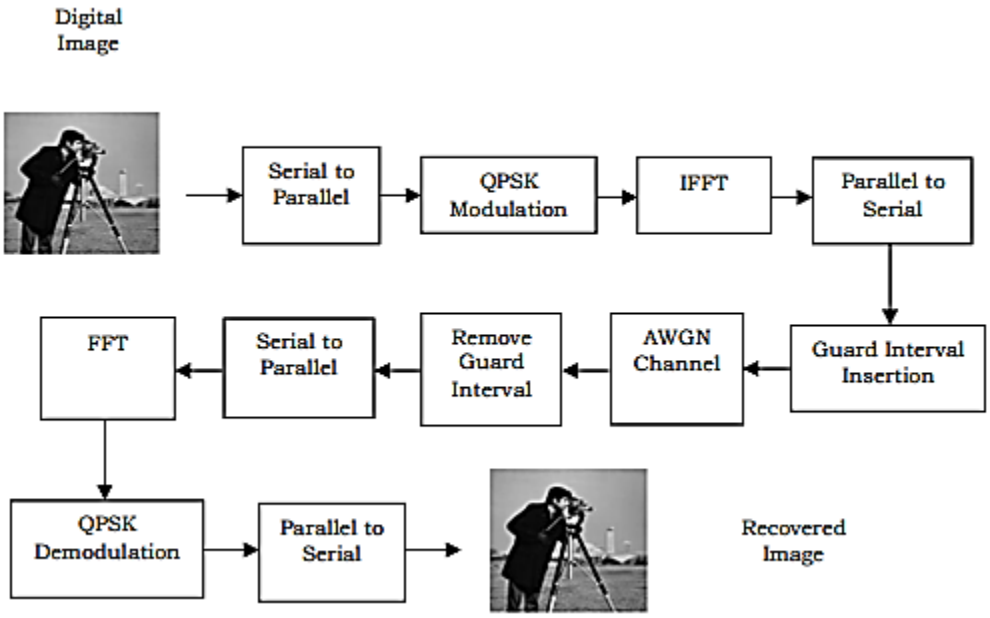

Figure 1: Block diagram of OFDM system

Database

The efficiency of the OFDM system is measured using three test pictures from the MATLAB database. You can get to them if you know the names cameraman, checkerboard, and MRI. Figure 2 depicts some of the potential test images used in this study. These pictures are of 256x256px or other such sizes and may be found in Tagged Image File Format (.TIF), Joint Photographic Experts Group (.JPG), and Graphics Interchange Format (.GIF) formats. When referring to grayscale, a pixel value of 0000 0000 represents perfect black. A pixel value of 1111 1111 represents a perfectly white image. These pictures are not initially in a format that can be sent directly through the OFDM system. It requires some preprocessing to transform the 2D picture, which is currently accessible as a matrix or two-dimensional in nature signal, into a 1D signal before it can be sent. This signal is almost ready to be sent. Finally, the vector data must be converted into a form that is compatible with the modulation method that was employed.

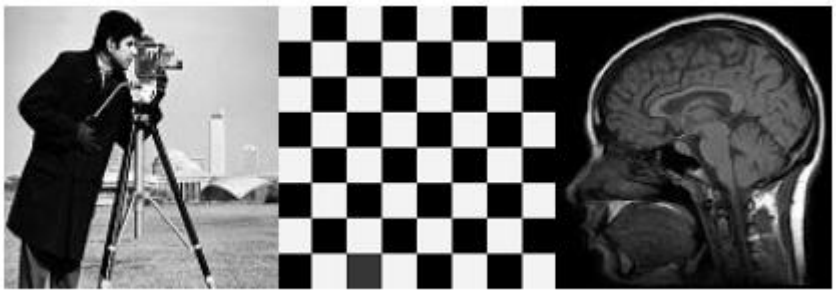

Figure 2. (a) Cameraman (b) Checkerboard (c) MRI

In the case of BPSK modulation, for instance, the vector information must be encoded as binary (consisting of only two signaling bits, or 0s and 1s). In order to perform QPSK modulation, the vector information must be converted to binary (four signaling items, 00, 01, 10, and 11). The OFDM transmitter takes this information as its "source data" or "image signal input." Once the digital bits are recovered at the receiver, the original picture may be rebuilt by a series of inverse operations.

Simulation Results and Discussions

BPSK, QPSK, QAM, 16-PSK, and 16-QAM are all investigated for transmission of cameraman, checkerboard, and MRI test pictures across an AWGN channel in an OFDM system. The PSNR and BER under varying signal-to-noise ratios are used to evaluate the operation of the OFDM system. Table 1 provides a summary of the design parameters for the OFDM system.

Parameters	Values
Modulation	BPSK, QPSK, QAM, 16-PSK 16-QAM
Modulation Order (M)	2, 4, 16
Bits/Symbol	1, 2, 4
Guard Interval Type	Cyclic Prefix
Cyclic Prefix (CP) Length	32 Samples
Total Number of Sub-Carriers (N)	256, 128, 32
Number Of Data Sub-Carriers	118
Number of pilot sub-carriers	11
Type Of Transmission	FFT-OFDM
Frame Length	234 Samples
Channel Model	AWGN
SNR	0 dB to 25dB
Image Dimension for Transmission	256x256
Total Data	256*256*8 = 5,24,288

Table 1: OFDM System Parameters

The BER comparisons for the three test pictures sent through the OFDM system using the various modulation techniques are shown in Table 1 below. Figures 3, 4 show the same thing. It was found that when SNR levels were increased, bit errors in the recovered pictures were reduced. Modulation-wise, BPSK provides better BER values than other modulation techniques for the structure under consideration. BER graphs for several pictures show that when SNR improves, BER correspondingly improves. Increasing the SNR always results in better performance.

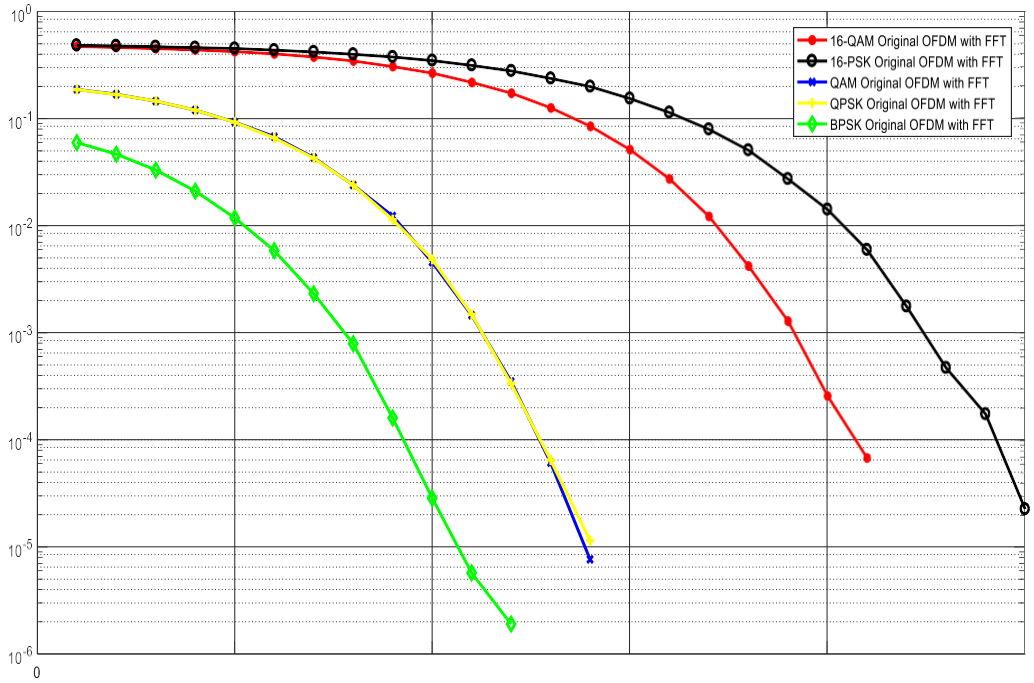

Figure 3: Variations of BER vs. E_b/N_0 for Cameraman imag

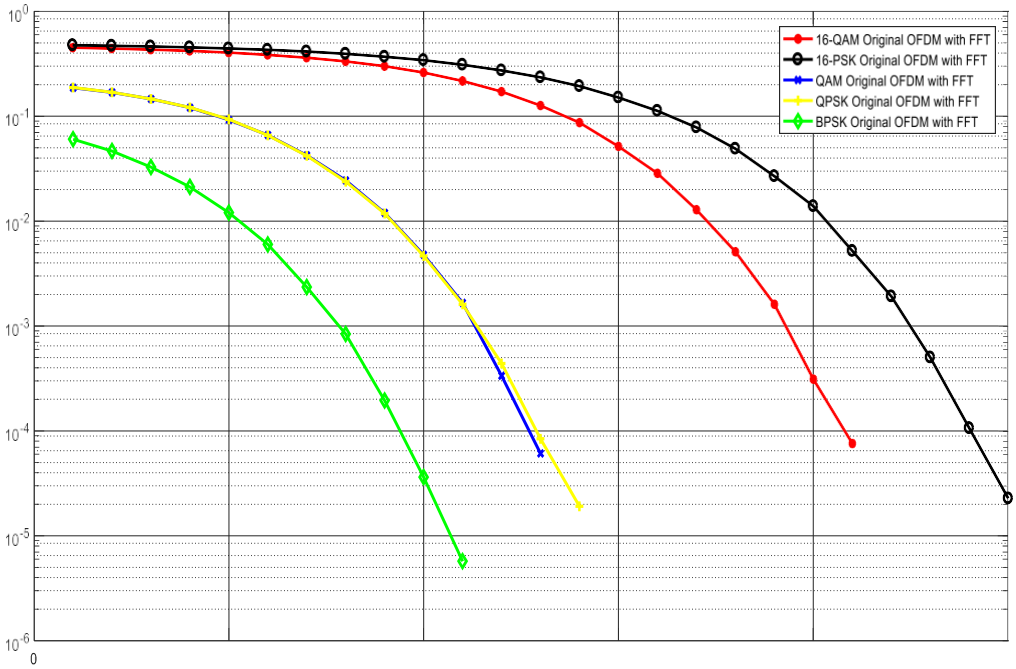

Figure 3: Variations of BER vs. E_b/N_0 for Checkerboard image

Conclusion

In this study, we investigated an OFDM system's capabilities by sending test pictures over an AWGN transmission channel using BPSK, QPSK, QAM, and 16-PSK/16-QAM modulation methods. The simulation findings show that for all three test pictures, the PSNR improves and the BER reduces in tandem with an increase in SNR. The greater the PSNR, the clearer the picture after recovery. The PSNR improves as the number of bit errors decreases. All the systems behave similarly when the SNR is low, with increased bit errors and correspondingly low PSNR values suggesting subpar reconstructed picture quality. When compared to QPSK/QAM/16-PSK/16-QAM systems, BPSK modulation is superior at recovering the original picture at low SNRs (12dB). Because the distance between constellation sites is decreased in higher modulation schemes, BER also decreases.

References

1. Y. Reddy, B. L. Reddy, A. S. Naga Veera Sai, A. K and P. S. S, "MSE and BER Analysis of Text, Audio and Image Transmission Using ML Based OFDM," *2020 IEEE International Conference for Innovation in Technology (INOCON)*, Bangluru, India, 2020, pp. 1-3, doi: 10.1109/INOCON50539.2020.9298204.

2. J. Patel and M. Seto, "Live RF Image Transmission using OFDM with RPi and PlutoSDR," *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, London, ON, Canada, 2020, pp. 1-5, doi: 10.1109/CCECE47787.2020.9255670.
3. K.Ingole "Design And Analysis Of 5g Communication System In Multi-Channel OFDM"2020 *Journal Of Control System And Control Instrumentation*

4. Z. Wang, "Secure Image Transmission in Wireless OFDM Systems Using Secure Block Compression-Encryption and Symbol Scrambling," in *IEEE Access*, vol. 7, pp. 126985-126997, 2019, doi: 10.1109/ACCESS.2019.2939266.

5. L. Demi, A. Ramalli, E. Boni and J. D'hooge, "Orthogonal Frequency Division Multiplexing Combined with Multi Line Transmission for Ultrafast Ultrasound Imaging: Experimental Findings," *2018 IEEE International Ultrasonics Symposium (IUS)*, Kobe, Japan, 2018, pp. 1-4, doi: 10.1109/ULTSYM.2018.8580107.

6. Uzma, J. A. Sheikh, S. A. Parah, G. M. Bhat and Safeena-al-Nisa, "Energy efficient image transmission through orthogonal frequency division multiplexing (OFDM) based multiple input multiple output (MIMO) systems," 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, India, 2017, pp. 1-6, doi: 10.1109/ICIIP.2017.8313794.
7. B. V. Naik, N. L. K. Sai and C. M. Kumar, "Efficient transmission of encrypted images with OFDM system," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 2383-2388, doi: 10.1109/ICPCSI.2017.8392144.
8. S. K. Pulayikodi, N. Tarhuni, A. Ahmed and F. B. Shiginah, "OFDM Based Robust Digital Image Watermarking Resistant to Multipath Spatial Shifts," *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, Manama, Bahrain, 2017, pp. 1-5, doi: 10.1109/IEEEGCC.2017.8448022.

9. A. Ben Abdallah, A. Zribi, A. Dziri, F. Tlili and M. Terré, "Adaptive UWB AV PHY IEEE 802.15.3c for compressed SPIHT image transmission," *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, 2017, pp. 1818-1823, doi: 10.1109/IWCMC.2017.7986560.
10. J. Zhang, Y. Zheng, X. Hong and C. Guo, "Increase in Capacity of an IM/DD OFDM-PON Using Super-Nyquist Image-Induced Aliasing and Simplified Nonlinear Equalization," in *Journal of Lightwave Technology*, vol. 35, no. 19, pp. 4105-4113, 1 Oct.1, 2017, doi: 10.1109/JLT.2017.2734814.
11. M. Chandra, D. Agarwal and A. Bansal, "Performance analysis of image transmission through Rayleigh channel," *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2017, pp. 1-5, doi: 10.1109/ICCCNT.2017.8204188.
12. A. S. Yami and H. Hadizadeh, "Visual attention-driven wireless multicasting of images using adaptive compressed sensing," *2017 Artificial Intelligence and Signal Processing Conference (AISP)*, Shiraz, Iran, 2017, pp. 37-42, doi: 10.1109/AISP.2017.8324103.
13. A. M. Atallah, H. S. Ali and M. I. Abdallah, "An integrated system for underwater wireless image transmission," *2016 28th International Conference on Microelectronics (ICM)*, Giza, Egypt, 2016, pp. 169-172, doi: 10.1109/ICM.2016.7847936.
14. S. Laksir and A. Tamtaoui, "Reduction of the effect of impulsive noise on image transmission in OFDM-based power line communications," *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, Fez, Morocco, 2016, pp. 1-6, doi: 10.1109/IT4OD.2016.7479318.
15. N. Tazin and M. R. H. Mondal, "Optimal biased spatial OFDM for peak power limited optical wireless channels," *2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Surfers Paradise, QLD, Australia, 2016, pp. 1-6, doi: 10.1109/ICSPCS.2016.7843304.
16. S. Gökceli, S. T. Başaran and G. K. Kurt, "A testbed for image transmission over a network coded cooperation system," *2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2016, pp. 1-5, doi: 10.1109/SOFTCOM.2016.7772113