



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 1, April 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Secure Image Transmission of an Encrypted Image through a MIMO–OFDM System with Different Encryption Schemes

Mr. Venkatesan¹, P. Akash², M. Bharath³, M.Nandha Kumar⁴, V. Surya⁵

Associate Professor, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering,
Krishnagiri, Tamil Nadu, India ¹

UG Students, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering,
Krishnagiri, Tamil Nadu, India ^{2,3,4,5}

ABSTRACT -The Evolution of the Internet has resulted in many new moments for the creation and delivery of content in digital or analog form. It is very much essential to secure data in financial service, defense, health care, government sector, and share marketing. To ensure the data from eavesdroppers, the physical layer security is one of the best solutions. The security features at this level reduce maintenance, operational, and complexity without damaging the quality of service. Physical layer security with cryptographic technology makes it as well suited for transferring multimedia information through unsecure or potentially risky wireless communication system. To provide security features to an image/data, one needs to protect the transmitted data from unauthorized access. In this project, the proposed system is an efficient cryptosystem for digital image encryption and authentication in medical applications using Generative adversarial networks. Digital watermarking and blurring algorithms are used to protect the multiple data from unauthorized access. GAN using for to provide both security techniques and attack scenarios, in order to detect the systems. The proposed cryptosystem provides high performance of an attacking gains access to server and enhanced security that processes the MRI-ray images and for effective diagnosis of patient diseases.

KEYWORDS: Digital watermarking, Generative adversarial networks.

1. INTRODUCTION

The data breach has spread worldwide all over the world, where the information is stolen or taken from a system without the knowledge of consent authorization of the system's user. With the explosion of information that is mostly in digital, data security is the need of the hour. It is mandatory for us to keep our information safe from the reach of intruders without authorized access, to maintain confidentiality and the integrity between the sender and receiver. Establishing a highly reliable and secure means of wireless communication for the transfer of digital or analog data (in the form of text, image, and video) from sender to receiver is becoming an essential requirement. They construct an image encrypting and editing model for based on homomorphic. The idea of homomorphic computation is to operate on an encrypted ciphertext and the result will be the same as operating on the plaintext. In our implementation we extend Palliser's Homomorphic Encryption (PHE) scheme to operate over images. The Palliser cryptosystem is an additive homomorphic and probabilistic symmetric encryption scheme. It is one of the partially homomorphic and it can add encrypting ciphertexts or multiply an encrypting ciphertext by a plaintext. With the development of computers, electronics, and modern communication technologies, the issue of security and confidentiality of information transmission and storage has become an important field of research. Such data processes are implemented in either a legal or illegal manner, or different approaches are used to hide data such as watermarking, it can be considered as an increasing method that can provide protection to the users or customers of the digital media against digital piracy. Generative adversarial networks (GAN) are used to provide both security advances and attack scenarios, in order to bypass detection systems.

II. OBJECTIVE

The main objective of this system is to encrypt and decrypt the MRI images safely and to obtain data using GAN network and Orthogonal frequency division multiplexing (OFDM). The medical images are pixelated and blurred in order to remove the noise. No additional overhead is added on the wireless frame and Data security is always guaranteed.

III. LITERATURE REVIEW

1. L. P. Feng, L. B. Zheng, P. Cao ADWT-DCT based blind watermarking algorithm for copyright protection.

The proposed a discrete wavelet transform- (DWT-) and discrete cosine transform- (DCT-) based digital image watermarking technique for copyright protection. Here, the watermark image is encrypted using the Arnold transform. system computes the block-based DCT of DWT LL sub band, which provides better visual quality of the image to the human eye.

2. L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, T. Yan A novel image encryption scheme based on non uniform sampling in block compressive sensing.

The idea of these approaches is that compressive sensing operation is performed block-by-block. Based on BCS, the computational complexity of CS is reduced. In order to achieve block secure CS, some image block secure CS schemes have been reported.

3. Priya, C.V.L. Raj, N.R.N Digital watermarking scheme for image authentication.

Changing the content of the data is extremely simple when multimedia editing programs are applied. A digital signature establishes an integral role for the content summary. After that, the signature is changed if any change occurs in the content by indicating a gap to that content.

4. Abd El-Samie, F. E., Ahmed, H. E. H., & Elashry, I. F Image encryption a communication perspective.

It considers two directions for image encryption: permutation-based approaches and substitution-based approaches. It explores number theory-based encryption algorithms such as the Data Encryption Standard, the Advanced Encryption Standard, and the RC6 algorithms.

5. Ahmad, J, & Ahmed, F Efficiency analysis and security evaluation of image encryption schemes. International Journal of Video & Image Processing and Network Security.

It presents a framework to evaluate image encryption schemes proposed in the literature. Instead of visual inspection, a number of parameters, for example, correlation coefficient, information entropy, compression friendliness, number of pixel change rate and unified average change intensity etc., are used, to quantify the quality of encrypted images.

6. Eldokany, I., Soliman, N. F., & El-Bendary, M. A. M. Efficient transmission of encrypted images with OFDM in the presence of carrier frequency offset.

The impact of carrier frequency offset (CFO) and CFO compensation on the transmission of encrypted images with different orthogonal frequency division multiplexing (OFDM) versions is studied. A comparison between four encryption algorithms with images transmitted through different OFDM versions is presented.

IV. EXISTING SYSTEM

In the existing systems, input digital image is in the 2D matrix format and converted into plaintext block before encryption block. Each plaintext block is then encrypting with the same secure cipher key.

The data rate of the OFDM system is very low, due to the fading and additive noise in the wireless channel

environment, transferring the high data rate is not easy.

V. PROPOSED SYSTEM

In this system, the MRI images are processed using effective image processing techniques. It has hybrid digital image watermarking and blurring methods to remove the noise in the MRI Images by Gaussian blur algorithm. GAN used to provide both security advances and prevent attack scenarios, in order to bypass detection systems. Also, the system will predict the disease of the patient whose MRI image is being processed. The homomorphic properties of this cryptosystem are demonstrated by applying a brightness adjustment transform over the encrypted image.

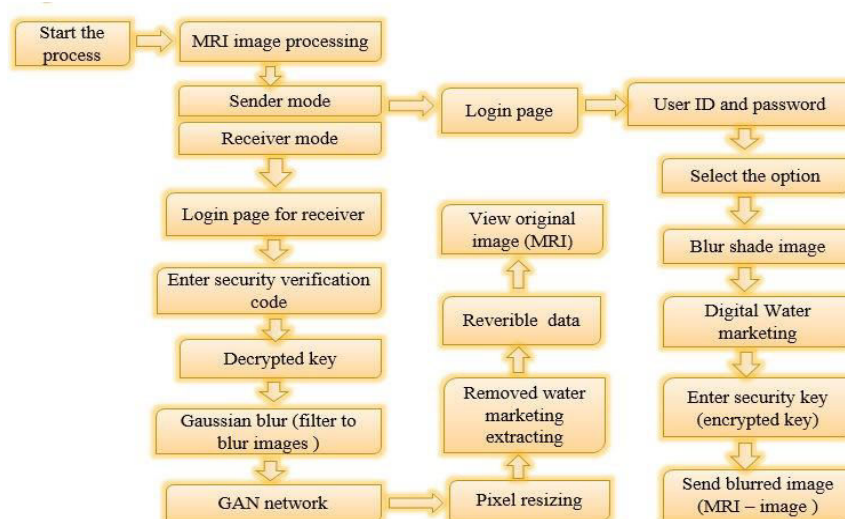


Figure 1: Block Diagram

A. GUASSIAN BLUR ALGORITHM

Gaussian blur is a methodology of blurring a picture by convolving the image with a mathematician operate. Convolution is solely the method of taking a tiny low matrix referred to as the kernel and running it over all the pixels in a picture. At each picture element, it performs some math operation involving within the convolution matrix and also the values of a picture element and its surroundings to see the value for a picture element within the output image. With the assistance of the mathematician operating, $m \times n$ matrix is generated. Victimization of this matrix and also the height of the distribution at that picture element location and also the new RGB values of the blurred image are computed. To dynamic the values within the kernel, the impact on the image may be modified — blurring, sharpening, edge detection, noise reduction, etc.

B. WATERMARKING

A watermark may be a brand, text, or pattern that's designedly superimposed onto another image. Its purpose is to create it tougher for the first image to be derived or used while not permission. Pictured at right is an associate degree example of a watermark applied to a digital image. Generally, partner want to mold the level in order to claim possession of watermark plus. While not watermarks, valuable digital assets may be liable to content larceny or

unauthorized use. Digital Watermarking is the use of a sort of marker covertly embedded in very digital media like audio, video, or image that permits the U.S.A. This system is employed for tracing violations on social media and knowing the genuineness of the notes within the banking industry. The data desires are embedded within the media. The signal that is embedded in the host signal and also the info is termed a digital watermark. The method has 3 main parts:

- 1.Embed –In this, the digital signal is embedding with the digital watermark.
- 2.Attack –The moment once the transmitted media is modified, it becomes a threat associate degree is termed an attack on the watermarking system.
- 3.Protection –The detection of the watermark from the noisy signal which could have altered media (JPEG compression, rotation, cropping, and adding noise) is termed Protection.

B. GENERATIVE ADVERSARIAL NETWORK

A generative adversarial network (GAN) is a machine learning model within which two neural networks vie with one another to become a lot of correct in their predictions. The two networks a GAN are called the generator and the discriminator. Generator: The Model that is used to generate new plausible examples from the problem domain. Discriminator: The Model that is used to classify examples as genuine (from the domain) or spurious (generated). The generator update supported whether or not the generated samples fooled the discriminator. The generative model's square measure is able to generate new examples from the sample that don't seem to be solely almost like examples however square measure is indistinguishable similarly. It analyses the distribution of the information in such the simplest way that once the coaching section the chance of the distributor creating a slip maximizes. On the opposite hand, supported by the model can estimate the chance that the sample is coming back from the information or not from the generator.

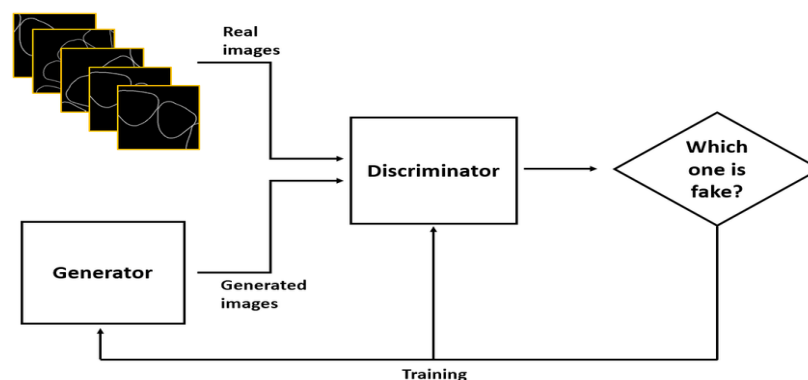


Figure 2: Architecture of Generative Adversarial Network

D. MIMO (Multiple-input, multiple-output)-OFDM (Orthogonal Frequency Division Multiplexing)

Multiple-input&output orthogonal frequency-division multiplexing (MIMO-OFDM) is the dominant air interacting for 4G and 5G broadcasting wireless communications. It combines multiple-input, multiple-output (MIMO) technology, which multiplies capability by transmission totally different signals over multiple antennas, and orthogonal frequency-division multiplexing (OFDM), which divides a radio channel into an outsized range of closely spaced sub-channels to produce a lot of reliable communications at high speeds. Analysis conducted throughout the mid-1990s showed that whereas MIMO may be used with alternative common air interfaces like time-division multiple access (TDMA) and

code-division multiple access (CDMA), the mix of MIMO and OFDM is most sensible at higher information rates. In orthogonal frequency division multiplexing, the sub channels are closely spaced, not only there is no guard band between them but they are overlapped. With the same available bandwidth, OFDM would allow more data transmission than frequency division multiplexing (FDM). Orthogonal means two or more multiple objects act independently, any neighbor signals in OFDM operate without dependence or interference with one another. The signals are multiplexed in a way that the peak of one signal occurs at the null of other neighbor signals. At the receiving end, the demultiplexer would separate them based on this orthogonal feature. OFDM utilizes the available bandwidth better, thus offering higher data transmission rate than frequency division multiplexing (FDM). In MIMO, due to fluctuation in channel quality independent fading channels are added (more antennas) at both sender and receiver side to increase the reliability of transmission link. In OFDM where different frequency sub channels carry different parts of modulated data. In spatial multiplexing, independent channels are created in the small allocated bandwidth. A considerable amount of signal processing is required to recover the transmitted data stream at the receiver. MIMO system decoder must estimate the individual channel transfer characteristics to determine the channel transfer matrix. Once all of this has been estimated, then the matrix can be produced and transmitted data stream can be reconstructed by multiplying the received vector with the inverse of the transfer matrix.

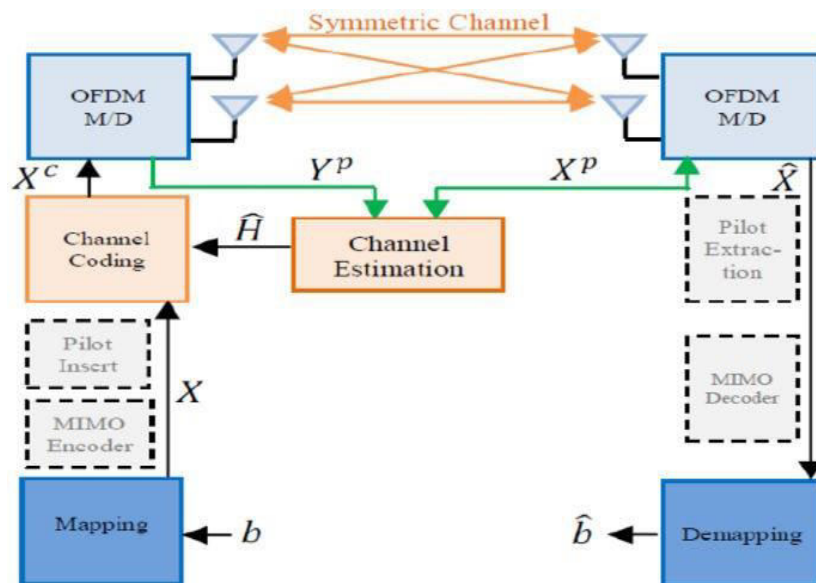


Figure3:MIMO-OFDMdiagram

VI. IMPLEMENTATION

The MRI images are processed using secure image processing technique. This technology has two modes sender and receiver transmitting mode. The sender will log in with a user ID and positive identification. The patient tomography image is blurred and watermarked then enter the cipher key for the blurred pictures. The blurred watermarking image is sent to receiver mode. Within the receiver aspect, the receiver additionally has a login page for login, when a receiver enters the debonair key for that encrypted tomography image. Then the receiver decrypts the image and take away the opaqueness watermarking extraction. Here, the GAN network takes samples and generates a sample of knowledge and when this is the person network decides whether the info is generated or taken from the sample through binary classification. We implement PHE and then extend it for images. To generate secure keys, we require large primes. In

our implementation we use the Rabin-Miller primality test to generate probabilistic primes of a given bit length with the assistance of a sigmoid perform that provides output within to vary of zero to one. Its sigmoid activating function to perform, wherever it estimates the chance that the sample is returning from the samples of information or the generator, this provides each security and safety to write and decode the info effectively. The Gaussian blur rule is employed to blur the images and take away the noise. When the removal of watermarking information is reversible and consider the first tomography pictures & graph and predict the wellness of the patient whose tomography image is being processed. Digital image watermarking and blurring are ways to get rid of the noise within the MRI-Images. During these processes GAN ensures security and safe to encrypt and decrypt the info effectively.

VII. RESULT

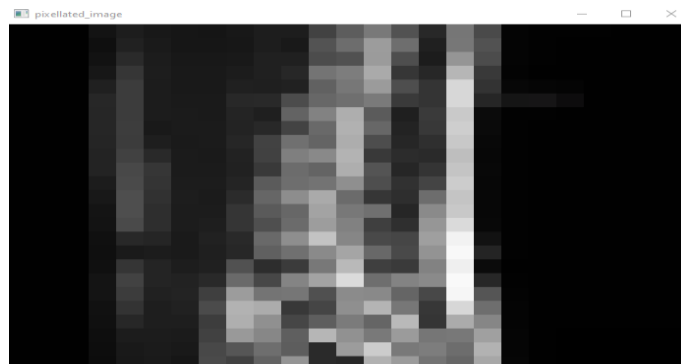


Figure4:BlurredImage

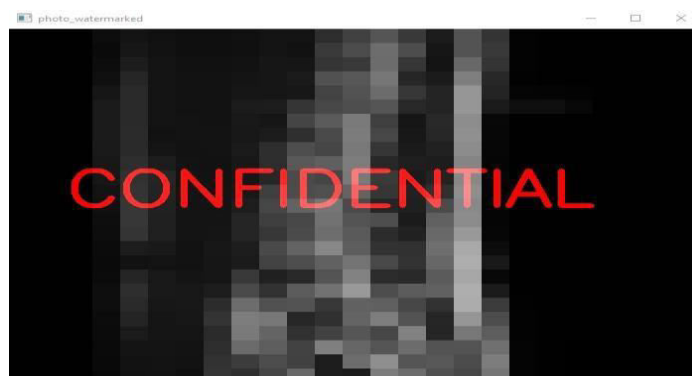


Figure 5: Watermarked Image

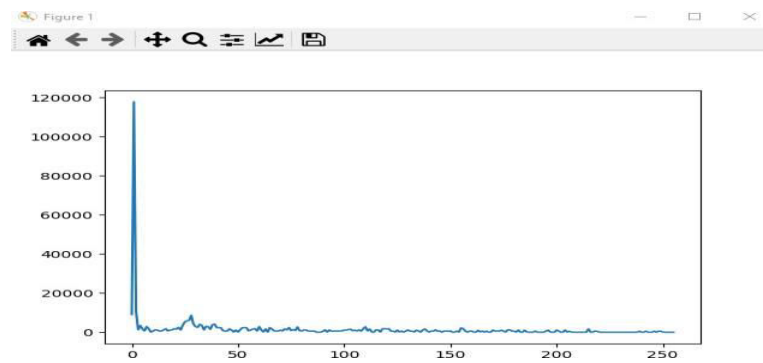


Figure 6: OFDM Output



Figure 7: Decrypted Image

The figures 4 and 5 shows the processed photographs of the input tomography images. The input image is blurred using Gaussian blur rule, then the image is watermarked. Figure ten represents the graph of the blurred images passing through the MIMO-OFDM (orthogonal frequency division multiplexing) system. Various MIMO-OFDM systems have been modeled in the PyCharm excitation setting. Figure 7 shows the decrypted pictures received by the receiver while removing the opacity and watermarking within the image and additionally by passing through the generative adversarial network.

VIII. CONCLUSION

In this conclusion, a demonstration of watermarked medical image transmission supported by the GAN network is completed. This projected system is in a position to protect visual information on plain images, and tomography images by digital watermarking techniques. Since the project theme uses GANs, there is no need to manage encoding keys. During this experiment, the effectiveness of the predicted subject is evaluated in terms of classification accuracy and the disease prediction patient tomography is characterized safely and securely. The experimental results confirmed that the predicted subject allows maintaining high classification accuracy with the pixel-based technology.

REFERENCES

- [1] X. Huang and G. Ye, "an image encryption algorithm based on hyper chaos and DNA sequence," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 57–70, Sep. 2017.
- [2] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the meristem hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.

- [3]J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "an image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," Commun. Nonlinear Sci. Numeri. Simul. vol. 23, nos. 1–3, pp. 294–310, Jun. 2018.
- [4]Y.-Q. Zhang and X.-Y. Wang, "Analysis and improvement of a chaosbased symmetric image encryption scheme using a bit-level permutation," Nonlinear Dyn., vol. 77, no. 3, pp. 687–698, Mar. 2017.
- [5]Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Inf. Sci., vol. 181, no. 6, pp. 1171–1186, 2019.
- [6]W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," Commun. Nonlinear Sci. numeri. Simul. vol. 18, no. 3, pp. 584–600, Mar. 2018.
- [7]A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," Nonlinear Dyn., vol. 87, no. 1, pp. 337–361, Jan. 2017.
- [8]I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "an efficient approach for the construction of LFT S- boxes using chaotic logistic map," Nonlinear Dyn., vol. 71, nos. 1–2, pp. 133–140, Jan. 2018.
- [9]I. I. Cisse, H. Kim, and T. Ha, "A rule of seven in Watson-Crick basepairing of mismatched sequences," Nature Struct. Mol. Biol., vol. 19, no. 6, pp. 623–627, Jun. 2017.
- [10]H. Liu and X. Wang, "Triple-image encryption scheme based on one-time key stream generated by chaos and plain images," J. Syst. Softw., vol. 86, no. 3, pp. 826–834, Mar. 2018.

BIOGRAPHY



Mr. M. Venkatesan,
Associate Professor,
Electronics and Communication
Engineering Department,
Adhiyamaan college of Engineering,
Hosur



Surya. V,
Bachelor of engineering(student),
Adhiyamaan college of Engineering,
Hosur



Akash. P,
Bachelor of engineering(student),
Adhiyamaan college of Engineering,
Hosur.

International Journal of Innovative Research in Science, Engineering and Technology*An ISO 3297: 2007 Certified Organization**Volume 12, Special Issue 1, April 2023***10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPPS '23)****5th -6th April 2023****Organized by****Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India**

Bharath. M,
Bachelor of engineering(student),
Adhiyamaan college of Engineering,
Hosur.



Nandha Kumar. M
Bachelor of engineering(student),
Adhiyamaan college of Engineering,
Hosur.



SJIF: 8.423



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INTERNATIONAL CENTRE



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details