Image Transmission and Hiding Through OFDM System With Different Encrypted Schemes

Krishna Dharavathu
Research Scholar,
Department of ECE
AUCE (A), Andhra University
Visakhapatnam, India
krishnadharavath4u@gmail.com

Dr.M.Satya Anu Radha
Associate Professor
Department of ECE
AUCE (A), Andhra University
Visakhapatnam, India
radhamsa@gmail.com

M. Siva Sankar Nayak
Assistant Professor
Department of CSE
Usha Rama College of Engg & Tech
Vijayawada, India
Sankar5805@gmail.com

Abstract— in this paper, an efficient way for transmission of encrypted images with a Fast Fourier transform (FFT) version of Orthogonal Frequency Division Multiplexing (OFDM) system is studied. A comparison between encrypted images transmitted with FFT-OFDM system by using two famous encryption algorithms (i.e. Data Encryption Standard (DES) and Advanced Encryption Standard (AES)) is presented. The aim of this comparison is to select the most appropriate encryption algorithm for efficient transmission of encrypted images. While performing the simulation experiments, the peak signal-to-ratio (PSNR) at the receiver is considered as an evaluation metric for examining the decrypted image quality. Form simulation results, it has been observed that, DES encryption algorithm is very much efficient in transmitting encrypted images through FFT-OFDM system over wireless radio channel.

Keywords-FFT, OFDM , AES, DES

*****

I. INTRODUCTION

Many factors like high data rate transmission capability, high band width ,high spectral efficiency, less interference from adjacent channels, robustness to multi path delays and fading, ease of system scalability and flexibility, etc, have made OFDM system as a favoured choice for modern digital data transmission over a wireless radio channel. OFDM technology is presently been incorporated in all latest mobile wireless communication systems. Few of them are 802.11 based WLANs, Wi-Fi, Wi-Max, 4G LTE, etc. There are many version of OFDM system. Few noted and popular version are namely, the Fast Fourier Transform OFDM (FFT-OFDM), the Discrete Cosine Transform OFDM (DCT-OFDM) and Discrete Wavelet Transform (DWT-OFDM). Out of all these configurations, the FFT-OFDM version is most widely used. The FFT-OFDM is implemented in several standards such as IEEE HIPERLAN/2,802.11a and 802.16a [1]-[6]. Several studies have also been presented with other two OFDM system version [7].

Very recently, OFDM has been chosen as the digital modulation standard for HDTV. So far, very less intensive work has been carried out on efficient transmission of encrypted images with OFDM system. This motivated to direct research to this issue. The main aim of this paper is to find the best image encryption algorithm that can be used to transmit encrypted images through OFDM system efficiently. Two encryption algorithms namely DES and AES are compared in this paper. Both DES and AES are diffusion based algorithms that can be implemented by using different modes of operation such as the electronic code-book(ECB), the cipher block chaining(CBC),the cipher feedback(CFB),the output feedback(OFB) and the counter(CTR) [8].These selected modes of operations generally governs the relation between blocks during encryption process. In this paper ECB mode of operation is chosen. The added advantage of using this mode is that the encryption and decryption process can be performed on separate blocks of plain-text, which allows performing parallel processing.

The rest of the paper is organized as follows: section II describes about two data encryption algorithms used in this paper, section III presents about the FFT-OFDM system used for encryption image transmission. Section IV discusses the experimental results. The final conclusions are made in section V.

II. DATA ENCRYPTION ALGORITHM

Encryption can be defined as the method of protecting the information from undesirable access or attacks by converting it into a non-recognizable form. It mainly involves in scrambling of data contents such as text, image, audio, video, etc, resulting in new form of data which is unreadable during transmission. Two encryption algorithms namely DES and AES are used in this paper which is described in detail in the following sub-sections as follows:

A. DES (Data Encryption Standard)

The DES algorithm operates on 64-bit blocks of data with a 56-bit key. It is basically a 16-round Feistel cipher i.e. a form of iterated block ciphers, where the cipher text is generated from the plain text by repeating the same transformation. It involves four basic operations namely expansion, permutation, XOR and substitution. The data to be encrypted is firstly divided into 64 bit blocks and fed into an initial permutation(IP) stage, in which each block is divided in to two sub-blocks(i.e. left sub-block and right sub-block); each with 32 bits length. The right sub-block is fed into a Feistel function

(F-function). The F-function operates on half a block of 32 bits at a time and consists of four stages:

- Expansion: The 32-bit half block is expanded to 48-bits using the expansion permutation by duplicating half of the bits. The output consists of eight 6-bit (i.e. 8 x 6 =48 bits) blocks, each containing a copy of four corresponding input bits, plus a copy of the immediately adjacent bit from each of the input blocks to either side.
- Key Mixing: The result is combined with a sub-key using an XOR operation. Sixteen 48-bit sub-keys, one for each round are derived from the main key by using a key schedule mechanism.
- Substitution: After mixing in the sub-key, the block is divided into eight 6-bit blocks before processing by the substitution boxes (S-boxes). Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form a lookup table. The S-boxes provide the core security of DES without them; the cipher would be linear and trivially breakable.
- Permutation: Finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box. This is designed so that, after expansion, each S-box output bits are separated across 6vdifferent S-boxes in the next round.

TABLE I. OFDM SYSTEM PARAMETERS FOR DES ENCRYPTED CASINO IMAGE TRANSMISSION

Parameters	Values
Modulation	QPSK
Modulation Order (M)	4
Bits/Symbol	2
Guard Interval Type	Cyclic Prefix
Cyclic Prefix (CP) Length	32 Samples
Total Number of Sub-Carriers (N)	128
Number Of Data Sub-Carriers	117
Type Of Transmission	FFT-OFDM
Frame Length	234 Samples
Channel Model	AWGN
SNR Range	-10 dB to 10dB
DES-56 Cipher Key	55128DF941BBB8A5

The OFDM System parameters for DES Encrypted casino Image Transmission is as shown in Table-I.Further details regarding DES algorithm and its implementation can be found in [8] - [9] respectively.

B. AES (Advanced Encryption Standard)

The AES algorithm is an iterated block cipher algorithm with fixed block size of 128-bits and variable key size which can be 128 or 192 or 256 bits. The intermediate cipher text is called a state. The number of rounds performed on the intermediate state is related to the key size. For key sizes of 128 or 192 or 256 bits, the number of rounds is 10, 12 and 14 respectively. Each round consists of a fixed sequence of transformations, except the first and last rounds. These transformations are listed as follows:

- Sub Byte: It is a non-linear byte substitution process operating on each of the state bytes, independently. The substitution box(S-box) is a multiplicative inverse in the Galois field (GF) (2^8) followed by applying an affine transform over the GF (2). The inverse of this transformation is obtained by the inverse of the affine transform followed by taking the multiplicative inverse in the GF (2^8).
- Shift row: In this process, the rows of the state matrix are cyclically shifted with different shifts that depend on the block size.
- Mix column: It computes the new state matrix S by left multiplying the current state matrix S by a constant polynomial.
- Add Round Key: In this operation, the round key is applied to the state in a sample bitwise XOR.

TABLE II. OFDM SYSTEM PARAMETERS FOR AES ENCRYPTED CASINO IMAGE TRANSMISSION

Parameters	Values
Modulation	QPSK
Modulation Order (M)	4
Bits/Symbol	2
Guard Interval Type	Cyclic Prefix
Cyclic Prefix (CP) Length	32 Samples
Total Number of Sub-Carriers (N)	128
Number Of Data Sub-Carriers	117
Type Of Transmission	FFT-OFDM
Frame Length	234 Samples
Channel Model	AWGN
SNR Range	-10 dB to 10Db
AES-128 Cipher Key	00010203040506070809 0A0B0C0D0E0F

The OFDM System parameters for AES Encrypted casino Image Transmission is as shown in Table-II.
Further details regarding AES algorithm and its implementation can be found in [8]-[12].

III. FFT-OFDM SYSTEM FOR ENCRYPTED IMAGE TRANSMISSION

The block diagram of a general base band FFT-OFDM system with additional functional blocks, namely the image encryption block at the transmitter side and image decryption block at the receiver side is shown in the fig. At the transmitter end, the encrypted images is generated by using the relation given by (1)

$$C = E(P, K) \qquad (1)$$

Where, P is the original image, E is the encryption algorithm, K is the encryption key and C is the encrypted image. Likewise, at the receiver end, the recovered image is decrypted so as to obtain the original transmitted image by using the relation given by (2)

$$P' = D(C', K') \qquad (2)$$

Where the C' is the possible corrupted cipher image, D is the decryption algorithm, K' is the decryption key, which may be similar to or different from the encryption key K and P' is the recovered original image.

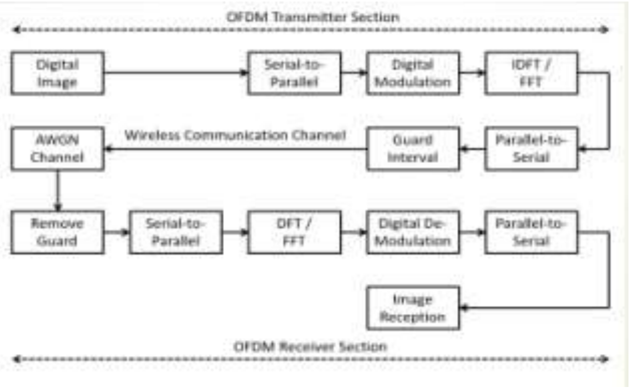

Figure 1. Block Diagram of OFDM System

The OFDM block diagram is as shown in fig 1. The input digital image data which is in the 2D matrix format is initially divided into a number of plain text block is then before encryption. Each individual plain text block is then encrypted with the same cipher key. The encrypted image data is then transformed to a multilevel sequence of complex numbers in one of several possible modulation schemes. The modulated symbols are grouped into blocks, and the inverse Fast Fourier Transform (IFFT) is performed to convert the symbols from frequency domain to time domain. At the end of the transmitter, a guard interval is inserted between symbols with cyclic prefix (CP) to eliminate inter-symbol interference (ISI). The resulting OFDM signal is then transmitted through the modelled Additive White Gaussian Noise (AWGN) channel.

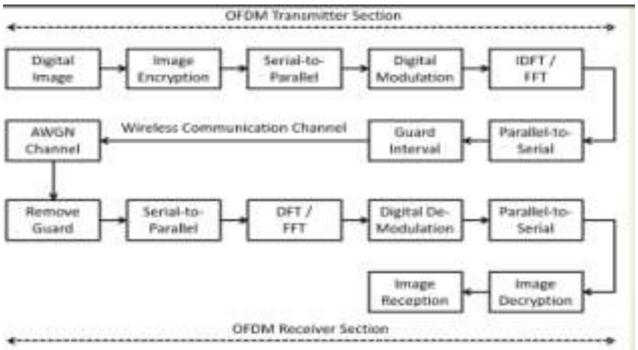

Figure 2. Block Diagram of FFT-OFDM Crypto System Architecture

TABLE III. OFDM SYSTEM PARAMETERS FOR ORIGINAL CASINO IMAGE TRANSMISSION

Parameters	Values
Modulation	QPSK
Modulation Order (M)	4
Bits/Symbol	2
Guard Interval Type	Cyclic Prefix
Cyclic Prefix (CP) Length	32 Samples
Total Number of Sub-Carriers (N)	128
Number Of Data Sub-Carriers	117
Type Of Transmission	FFT-OFDM
Frame Length	234 Samples
Channel Model	AWGN
SNR	-10 dB to 10dB

At the receiver end, an inverse of transmitter section operations are performed. Initially, the cyclic prefix (CP) is removed from the received signal. After that, the received signal is transformed into the frequency domain via FFT. Finally, the demodulation and decryption processes are performed and the recovered image data is reconstructed to obtain the digital image which is used at the transmitter.

Table II and Table III shows the specifications of the modelled FFT-OFDM system used for encrypted used for encrypted image transmission by using DES and AES cryptographic algorithms. The same FFT-OFDM system can also be used for original image transmission without encryption. For this purpose, the two blocks i.e, image encryption block at the transmitter end and image decryption block at the receiver end are removed. In this case, except the cipher key parameters mentioned in the Table I and Table II, the rest of the parameters remain the same.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Simulation experiments have been performed to test the performance of FFT-OFDM system with DES and AES encryption algorithms for efficient transmission of encrypted images. The performance of FFT-OFDM system for encrypted image transmission is in turn compared with the original image transmission as well. For carrying out the simulation experiment, a gray scale Casino image is taken as the reference image.

The performance of an encrypted image transmission system is evaluated based upon set of encryption quality parameters. The encryption quality can be measured by using three important performance metrics namely, Histograms, Deviation and Noise Immunity.

The histogram of an image represents the occurrence probability of each gray level in the image, in the case of encryption algorithms. The histogram is required to be uniform as possible to achieve better security. Uniformity in the histogram of the image indicates that the encryption algorithm is more powerful. Fig 2, Fig 3 and Fig 4 illustrates the original, DES and AES encrypted versions of the casino image along with their corresponding histograms respectively. Fig 5 and Fig 6 are represents Histogram Comparison of Original Image and Its DES and AES Encrypted Version. It is observed that, the tonal distribution (i.e., histogram) is uniform in case of both DES and AES encrypted images thereby indicating that both the encryption algorithms are equally powerful.

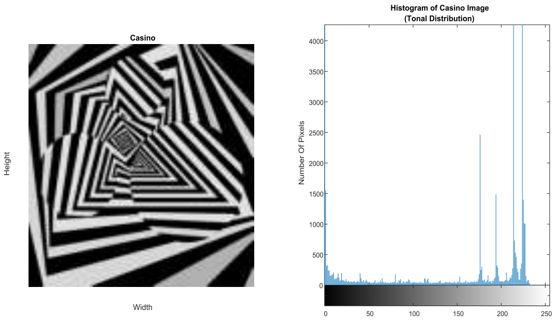

Figure 3. Casino Image and its Histogram

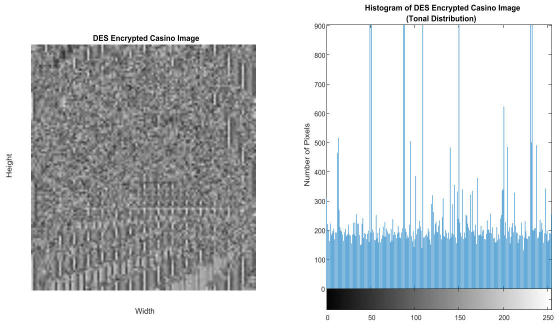

Figure 4. DES Encrypted Image and its Histogram

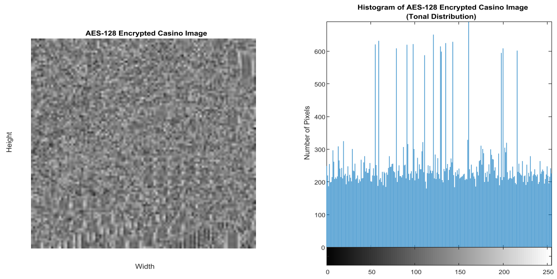

Figure 5. AES Encrypted Image and its Histogram

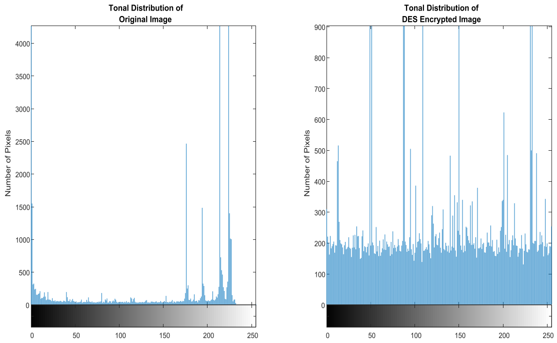

Figure 6. Histogram Comparison of Original Image and Its DES Encrypted Version

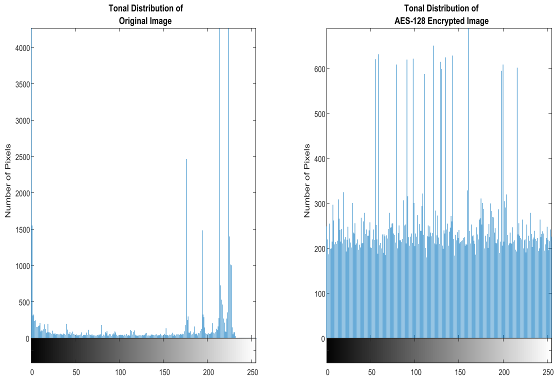

Figure 7. Histogram Comparison of Original Image and Its AES Encrypted Version

The deviation is another metric, used to evaluate the encryption quality. Mathematically, the deviation between the original image and the encrypted image is expressed as shown in (3).

$$D=\sum_{i=0}^{gxg}| I_i - J_i | \qquad (3)$$

Where I_i is the ith pixel of the original image and J_i is the ith pixel of the encrypted image. As the value of deviation increases, the degree of security is enhanced. Table IV shows the tabulated deviation values for the DES and AES encrypted casino images respectively. From this table, it is very much clear that the both algorithms are preferred from the deviation point of view due to their diffusion property which enhances security [13].

TABLE IV. DEVIATION VALUES FOR THE ENCRYPTED CASINO IMAGE

Encryption Technique	Deviation
Data Encryption standard (DES)	73.9264
Advance Encryption standard (AES)	73.8094

Another requirement for encryption algorithm is to achieve good noise immunity in addition to security. The noise immunity describes the ability of the image crypto-system to tolerate noise. For testing the noise immunity, error patterns with different bit error rates (BER) are simulated with the encrypted image and then its effect is observed at the receiver by using decryption algorithm. If the decrypted image has a close resemblance with the original image, then the crypto-system is said to be immune to noise. The same noise immunity validation of FFT-OFDM system is also performed on the original image transmission and its performance is compared with the DES and AES encrypted images. Table V, shows the SNR, Bit Error Rate (BER) and Errors for Original FFT-OFDM System and Table VI Shows the Comparison of SNR, Bit Error Rate (BER) and Errors for DES and AES Encrypted algorithms.

Fig 7 shows the variation of decrypted image PSNR with simulated BER. From this figure, two valid observations can be drawn. Firstly, the FFT-OFDM system with the original image transmission is having better performance when compared with FFT-OFDM system for encrypted image transmission. The recovered original image at the receiver is having relatively high PSNR values even at high BERs when compared with the PSNR values of the decrypted images. Secondly, among crypto-systems the performance of DES crypto FFT-OFDM system is better than the AES crypto FFT-OFDM system. The DES decrypted image achieved good PSNR values at both high and low BERs when compared with AES decrypted image. Finally from this figure, it is clear that DES encryption algorithm achieves the best PSNR values in presence of errors.

Fig 8 illustrates the variation of PSNR with SNR. From this figure, two valid observations can be drawn. Firstly, the FFT-OFDM system with original image transmission is having better performance when compared with FFT-OFDM system for encrypted image transmission. The recovered original image at the receiver is having relatively high PSNR values even at low SNRs when compared with the PSNR values of the decrypted images. Secondly, among crypto-systems, the performance of DES crypto FFT-OFDM system is better than the AES crypto FFT-OFDM system. The DES decrypted image achieved good PSNR values at both low and high SNRs when compared with AES decrypted image. Finally from this figure, it is clear that the DES encryption algorithm achieves the best PSNR values at the low SNRs.

TABLE V. SNR, BIT ERROR RATE AND ERRORS FOR ORIGINAL FFT-OFDM SYSTEM CASINO IMAGE TRANSMISSION

S. No	SNR	BER	ERRORS
1	-10	0.3244	170096
2	-9	0.3148	330143
3	-8	0.2945	308908
4	-7	0.2721	285330
5	-6	0.2485	260662
6	-5	0.2232	234056
7	-4	0.1963	205869
8	-3	0.1692	177389
9	-2	0.1414	148280
10	-1	0.1140	119561
11	0	0.0882	92515
12	1	0.0650	68202
13	2	0.0448	47003
14	3	0.0283	29709
15	4	0.0162	16990
16	5	0.0081	8597
17	6	0.0035	3768
18	7	0.0013	1455
19	8	4.2725e-04	448
20	9	1.0777e-04	113
21	10	1.8120e-05	19

The significance of the plots shown in Fig. 7 and Fig. 8 can be understood more clearly though visual inspection of the quality of recovered images at the FFT-OFDM receiver corresponding to different SNRs. Fig. 9, Fig. 10 and Fig. 11 shows the recovered casino images, DES decrypted images and AES decrypted images at FFT-OFDM receiver corresponding to different SNRs respectively. From Fig.8, it is observed that the quality of the received image is not degraded much at very low SNR values. By comparing Fig. 10 and Fig. 11 and it is observed that, the DES encryption algorithm is more immune to noise than compared with AES encryption algorithm. The visual perceptual quality of AES decrypted images is high only at high SNRs. Even at high SNR (say about 10 dB), the corresponding PSNR value of AES decrypted image is relatively less than DES decrypted image. In the other words, at low SNR (say about 1 dB), though the visual perceptual quality of both DES and AES decrypted images are somewhat similar but the corresponding PSNR value of DES decrypted image is relatively more than AES decrypted image. However this does not help in recognizing the true image transmitted by the FFT-OFDM transmitter.

TABLE VI. COMPARISON TABLE FOR SNR, BIT ERROR RATE AND ERRORS FOR AES-128 AND DES ENCRYPTED CASINO IMAGE TRANSMISSION BY OFDM

S.NO	SNR	BER		ERRORS	
		AES	DES	AES	DES
1	-10	0.3285	0.3268	172215	171339
2	-9	0.3188	0.3165	334335	331869
3	-8	0.2983	0.2963	312787	310641
4	-7	0.2760	0.2746	289429	287989
5	-6	0.2522	0.2509	264430	263107
6	-5	0.2266	0.2255	237642	236488
7	-4	0.2005	0.1991	210219	208749
8	-3	0.1734	0.1719	181835	180282
9	-2	0.1457	0.1441	152749	151055
10	-1	0.1181	0.1168	123812	122463
11	0	0.0917	0.0904	96131	94806
12	1	0.0680	0.0666	71277	69838
13	2	0.0475	0.0464	49774	48620
14	3	0.0305	0.0295	32015	30975
15	4	0.0179	0.0172	18803	18068
16	5	0.0095	0.0091	9923	3557
17	6	0.0043	0.0041	4495	4260
18	7	0.0017	0.0015	1760	1572
19	8	5.1689e-04	4.6730e-04	542	490
20	9	1.2875e-04	1.1730e-04	135	123
21	10	2.0027e-05	2.0981e-05	21	22

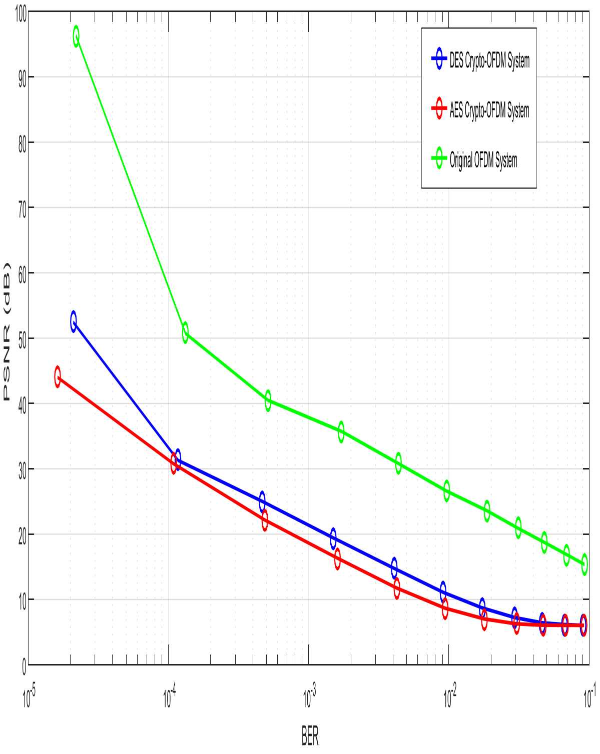

Figure 8. PSNR vs. BER Comparison Plots for Transmitted Original, DES and AES Encrypted Casino Images

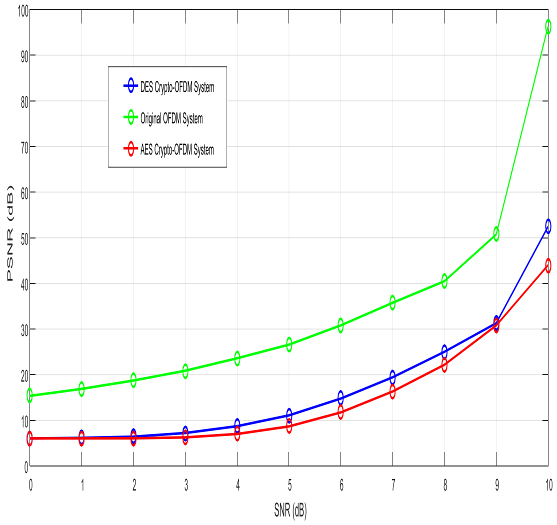

Figure 9. PSNR vs. SNR Comparison Plots for Transmitted Original, DES and AES Encrypted Casino Images

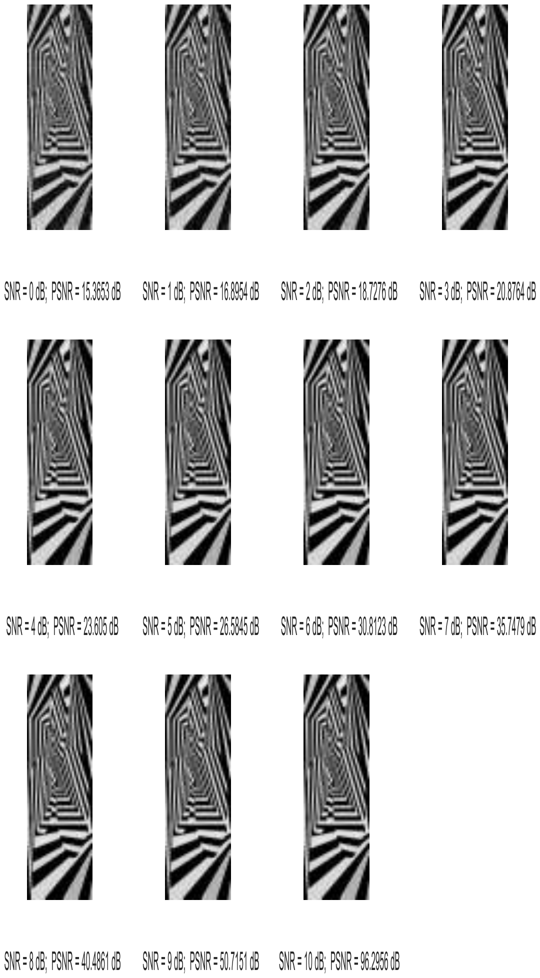
SNR = 0 dB; PSNR = 15.3653 dB
SNR = 1 dB; PSNR = 16.8954 dB
SNR = 2 dB; PSNR = 18.7276 dB
SNR = 3 dB; PSNR = 20.8764 dB
SNR = 4 dB; PSNR = 23.605 dB
SNR = 5 dB; PSNR = 26.5845 dB
SNR = 6 dB; PSNR = 30.8123 dB
SNR = 7 dB; PSNR = 35.7479 dB
SNR = 8 dB; PSNR = 40.4861 dB
SNR = 9 dB; PSNR = 50.7151 dB
SNR = 10 dB; PSNR = 96.2956 dB

Figure 10. Recovered Casino Image at FFT-OFDM Receiver

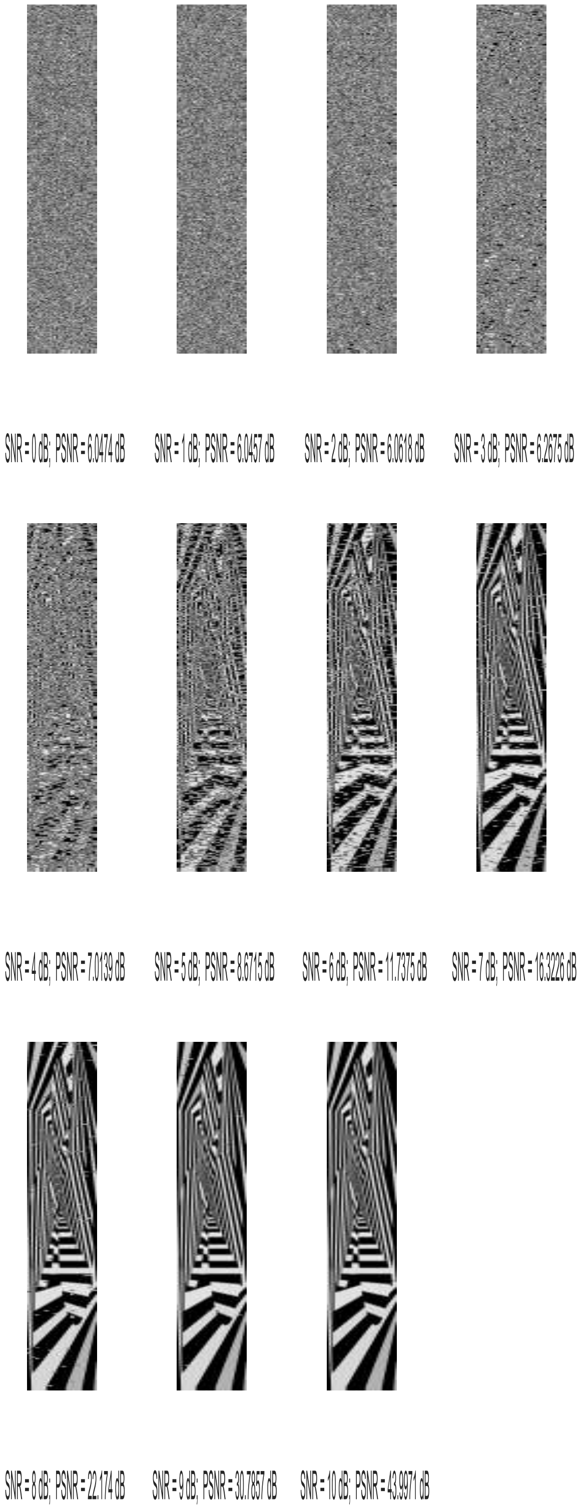
SNR = 0 dB; PSNR = 6.0474 dB
SNR = 1 dB; PSNR = 6.0457 dB
SNR = 2 dB; PSNR = 6.0618 dB
SNR = 3 dB; PSNR = 6.2675 dB
SNR = 4 dB; PSNR = 7.0139 dB
SNR = 5 dB; PSNR = 8.6715 dB
SNR = 6 dB; PSNR = 11.7375 dB
SNR = 7 dB; PSNR = 16.3226 dB
SNR = 8 dB; PSNR = 22.174 dB
SNR = 9 dB; PSNR = 30.7857 dB
SNR = 10 dB; PSNR = 43.9971 dB

Figure 11. AES Decrypted Casino image at FFT-OFDM Receiver

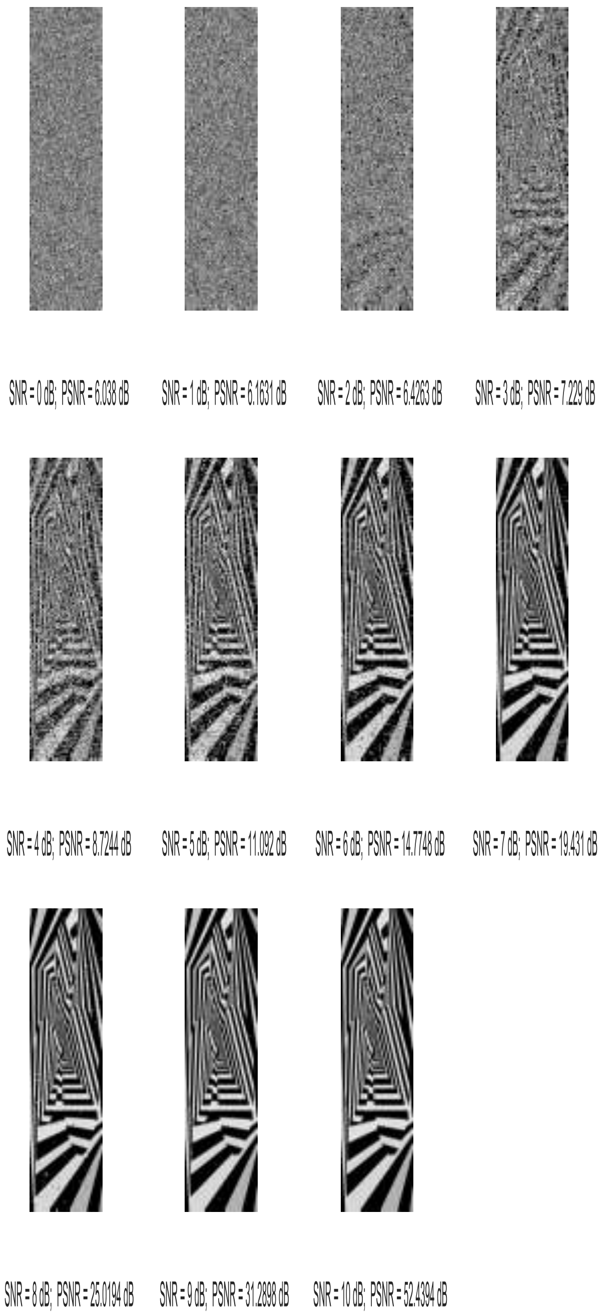
SNR = 0 dB; PSNR = 6.038 dB
SNR = 1 dB; PSNR = 6.1631 dB
SNR = 2 dB; PSNR = 6.4263 dB
SNR = 3 dB; PSNR = 7.229 dB
SNR = 4 dB; PSNR = 8.7244 dB
SNR = 5 dB; PSNR = 11.092 dB
SNR = 6 dB; PSNR = 14.7748 dB
SNR = 7 dB; PSNR = 19.431 dB
SNR = 8 dB; PSNR = 25.0194 dB
SNR = 9 dB; PSNR = 31.2898 dB
SNR = 10 dB; PSNR = 52.4394 dB

Figure 12. DES Decrypted Casino image at FFT-OFDM Receiver

V.CONCLUSION

In this paper, the performance of FFT-OFDM system for transmission of encrypted images using DES and AES encryption algorithms have been investigated. The simulation results showed that the performance of FFT-OFDM system with DES encryption algorithm is best as compared with that of AES encryption algorithm.

REFERENCES

[1] Salwa M. Serag Eldin, “Optimized OFDM Transmission of Encrypted Image Over Fading Channel,” Springer, sens Imaging, 2014. Avilable: http://doi.org/10.1007/s11220-014-0099-3/

[2] D. Krishna, Dr. M.Satya Anuradha, “Image Transmission Through OFDM System Under the Influence of AWGN channel,” IOP Conference Series: Materials Science and Engineering 225 (ICMAEM-2017) 012217. Avilable: http://doi.org/10.1088/1757/-899X/225/1/012217

[3] N.S.Sai Srinivas, “OFDM System Implementation,Channel Estimation and Performance comparison of OFDM Signal”, in IEEE International Conference on ElectroMagnetic Interference compatability (INCEMIC), Visakhapatnam, India,Jul 2015, pp.461-466

[4] P.Tan and N.C.Beaulieu, “ A Comparison of DCT-Based OFDM and DFT-Based OFDM in Frequency Offset and Fading Channels”, IEEE Transctions on communications, vol.54, no. 11, pp.2113-2125, Nov 2006. Available: http://ieeexplore.ieee.org/document/4012512/

[5] F.Gao, T. Cui, A.. Nallanthan, and C. Tellambura, “Maximum likelihood based Estimation of Frequency and Phase Offset in DCT-OFDM Systems under Non-Circular Transmission: Algorithms, Analysis and Comparisons”, IEEE Transctions on Communications, vol. 56,no. 9,pp. 1425-1429, September 2008. [online]. Avilable: http://ieeexplore.ieee.org/document/4623796/

[6] R. Merched. On OFDM and Single-Carrier Frequency-Domain Systems based on trignometric transforms”, IEEE Signal Processing Letters, vol. 13, no. 8, pp.473-476, Aug 2006. [online]. Avilable: http://ieeexplore.ieee.org/document/1658060/

[7] P. Tan and N. C. Beaulieu, Precise bit error probability analysis of DCT-OFDM in the presence of carrier frequency offset on AWGN channels”, in GLOBECOM ’05. IEEE Global Telecommunications Conference, 2005, vol. 3, Nov 2005, pp. 6 pp-[online]. Avilable: http://ieeexplore.ieee.org/document/1577887/

[8] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed, Upper Saddle River, NJ, USA: Prentice Hall Press, 2010

[9] I. Eidokany, E.S.M. EI-Rabaie, S. M. Elhalafawy, M. A. Z ein Eldin, M. H. Shahieen, N. F. Soliman, M. A. M. EL-Bendry, M. A. EL-Naby, F. S. Al-Kamali, I. F. Elashry, and F. E. Abd El-Samie, “Efficient transmission of encrypted images with OFDM in the presence of carrier frequency offset”, Wireless Personal Communications, vol.84, no.1,pp. 475-521, Sep 2015. [online]. Avilable: http:/doi.org/10.1007/s11277015-2645-2

[10] J. Daemen and V. Rijmen, The Design of Rijnadael. Secaucus, NJ, USA: Spriger-Verlag New York, Inc., 2002

[11] AES (Advanced Encryption Standard), FIPS-197 (Federal Information Processing Standard),” November 2001. [online]. Avilable: http://csrc.nist.gov/publications/fips 197/fips-197.pdf

[12] N.S. Sai Srinivas and MD. Akramuddin, “FPGA based hardware implementation of AES Rijndael Algorithm for Encryption and Decryption,” in 2016 International Conference on Electrical, Electronics, and Optimization techniques (ICEEOT), Chennai, India, March 2016, pp. 1769-1776. [online]. Avilable: http://ieeexplore.ieee.org/document/7754990/

[13] J. Daemen and V. Rijmen, The bloch cipher Rijnadael. Berlin Heidelberg: Springer Berlin Heidelberg, 2000, pp. 277-284. [online]. Avilable: http://doi.org/10.1007/10721064_26