Presenting Channel Estimation Method to Reduce Errors on Encrypted Images based on the Comparative Methods in OFDM Systems

Babak Ehyaee
Department of Communication, Bushehr Branch,
Islamic Azad University Bushehr, Iran.

Navid Daryasafar
Department of Communication, Bushehr Branch,
Islamic Azad University Bushehr, Iran.

ABSTRACT
The AES encryption algorithm is a modern pattern having the characteristics such as high speed and simplicity of software implementation. Despite having all the advantages brought by the encrypted data, they are more sensitive to noise than the normal data. Perhaps, one of the reasons for this to happen is the existence of consecutive cycles during the decrypting operation. Using the error correction coding may be suggested as one suggestion; however, using this method significantly increases the volume of data. In this article, we multiply the received symbols by the adjustment coefficients. In order to find adjustment coefficient we need to estimate the channel. The smallest mean squares algorithm is an appropriate way for estimating the channel. The computer simulation results are good indicators of the superiority of this method to OFDM technique and the other modulations.

Keywords
Encryption, AES algorithm, LMS algorithm, Channel estimation.

1. INTRODUCTION
Data Protection is a serious topic in Telecommunications. Daily we see news about several robberies and attacks on our information resources. So researchers are trying to reduce the effects of the attack to information sources. Encryption methods can be used as an effective solution for protection of the resources used. One of the most popular encryption method is AES. Now this method uses in many communications systems and services such as smart cards, mobile phone, ATM and web. AES's feature causes it different than other methods. Send and receive encrypted data is such as typical data. Information through a communication channel with a technique such as OFDM is sent.[1-2]
OFDM Technique makes information transmission with high data rate and establishment of multimedia services such as sending voice, data and video through wireless networks, possible. This technique is a special mode of multi-carrier systems in which high bit rate data is broke down into parallel lower bit rate groups and each group is modulated by the orthogonal sub-carriers.
In this paper, we will study the effect of noise and channel on the data encrypted by AES method which has been transmitted by OFDM technique. Then, expressing the proposed method, we will try to decrease the effect of channel and noise on the encrypted data. For convenience, we will use data from an image, because the effect of noise and channel is better observed on image data.[3]
This paper is divided to different sections. In section 2, we described the AES algorithm and then we used data from an image, conducted the cryptographic operation on the image and presented the output. In section 3, introducing the OFDM technique, we will put the encrypted image on a communication channel, and then we will decode the image in the receiver. In Section 4, expressing the proposed method, we will try to decrease the effect of channel and noise on the encrypted data.
Further, in the second chapter the AES algorithm is introduced. In the third chapter, the suggested algorithm for fading channel coefficients estimation in OFDM systems will be described and finally, the simulation results will indicate the performance of suggested algorithm.

2. AES ALGORITHM
AES (Rijndael) is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14). The cipher key is similarly a rectangular array with four rows and number of columns equal to the key length divided by 32. The number of rounds is related to the key size, so for key sizes of 128, 192 and 256 the number of rounds are 10, 12 and 14 respectively.These rounds are governed by the following transformations:
Bytesub transformation: Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation. It is a non linear byte substitution, operating on each of the state bytes independently. The substitution table (S-box) is a multiplicative inverse in the GF(2^8) followed by applying by an affine over GF(2). The inverse process is true with the decryption process, which is obtained by the inverse of the affine mapping followed by taking the multiplicative inverse in the GF(2^8) .
Shiftrows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.
Mixcolumns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers. In MixColumn, the columns of the state are considered as polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = (03)x^3 + (01)x^2 + (01)x + (02)$.
Addroundkey transformation: Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

The encryption procedure consists of several steps as shown by Fig. 1.[4-5] After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption. Fig.2 show encrypted image using this method.[6-7]

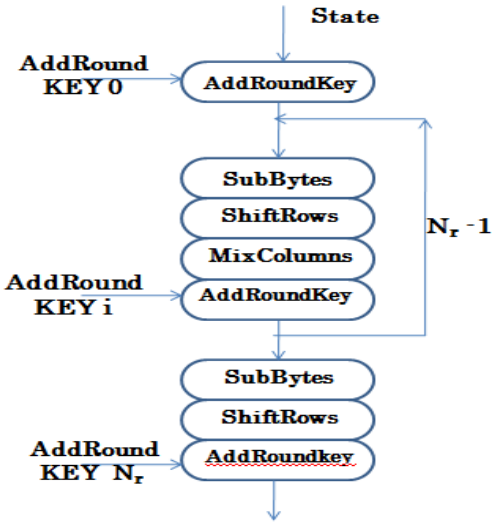


Fig 1: AES algorithm general diagram.

Fig 2: The image decrypted using the AES method

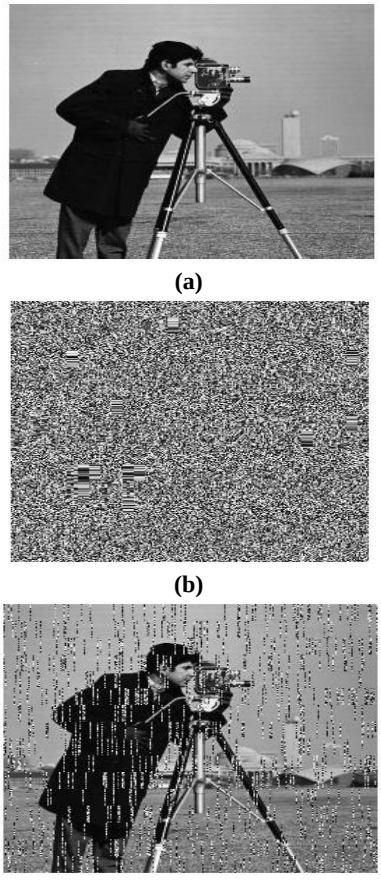
3. OFDM TECHNIQUE

Sending information on perpendicular carriers based on data transmission on multi-carrier systems. In the idea of conventional multi-carrier transmission such as FDMA, the transmitted signal bandwidth is divided into several sub-bands each of which is allocated to a sub-carrier and the information is sent by this sub-carriers. Unlike the conventional multi-carrier transmission systems in which the spectrum subcarriers have no overlap with each other and a protective frequency is considered between every two sub-carrier adjacent to the band. In OFDM system, the distances between sub-carriers are chosen in a way that the sub-carriers are mathematically orthogonal to each other. The spectrum of each sub-carrier in this case can overlap with each other. The overlapping property of the spectrums causes the OFDM system to be more efficient than FDMA in terms of saving the bandwidth.

In order to produce OFDM symbols, first, the sequences of binary data are generated for which the encrypted image data can be used, and they are written as spots in the system space, or so to say, the binary sequences become symbols. These symbols can be QAM and PSK symbols in normal mode or other symbols in other modulations. The symbols can be transmitted in a communication channel in the wireless network by the transmitter. An OFDM symbol is generally consists of N sub-channels that can be shown as the equation 1.[8-9]

$$x(t) = \sum_{k=0}^{N-1} X_k e^{\frac{j2\pi kt}{T}} \qquad 0 \le t < T \qquad (1)$$

The channel effect can be added to the transmitted symbols. The results of simulation of the decrypted image are shown in figure 3.



(a) **(b)** **(c)**

Fig 3: (a) Initial image (b) Encrypted image (c) Decrypted image in receiver

In can be seen that the effect of noise and channel caused the partial loss of the image information. This phenomenon can be stated in this way that due to existence of successive rounds in decoding operations, the additional noise is also located in this cycle, affects the other data of the state matrix and causes the loss of 16 bytes of information.

4.PROPOSED METHOD

One of the applications of adaptive filtering in general subjects, that describes the hypothetical relationship between the input and output, is the system identification. Figure 4, illustrates the overall structure of system identification. It this diagram, the system inside the dash lines is an unknown system.

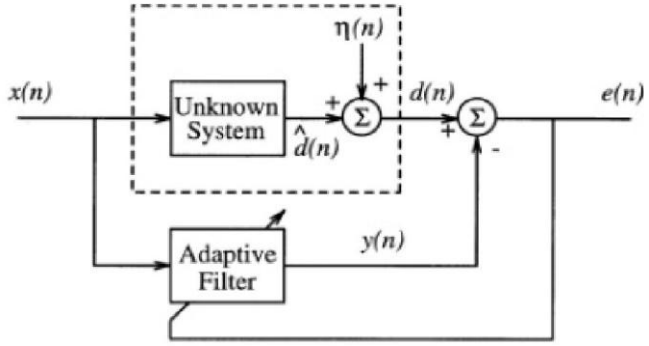


Fig 4: System identification structure

Weiner filter is an optimal linear filter so that it can, to some extent, bring the output signal closer to the desired one. Although this type of filter, is often not used due to the computational complexity, but it is being studied as a reference body for linear filtering of random signals that can be compared with other algorithms.

The algorithm of the smallest square means LMS based on descending steep random algorithm that modifies the filter weights approaching the minimum square mean error (MSE). This algorithm is easily implemented in practice and its performance is also clear and predictable. The incoming symbols belonging to each sub-carrier are multiplied in modulator coefficients or filter weights. The modulator coefficients can be obtained based on the least square errors of MMSE. To calculate modulator coefficients or filter weights for each sub-carrier, the channel estimation is needed. In most cases, in order to be able to estimate the channel, the transmitter sends training symbols which are known as guidance symbols and are recognized by the receiver.

The LMS algorithm is suggested for solving the Wiener-Holf equation in which the use of statistical information of the channel and data for better performance is required. The necessary steps to estimate channel by LMS method are as follows:[10-11]

1- First, the channel is estimated using LSE. $\hat{H}_{LS}[n]$ is obtained.
2- After obtaining the coefficients, the channel is estimated:

$$\hat{H}_{LMS}[n] = \hat{W}^{H}[n]\,\hat{H}_{LS}[n] \qquad (2)$$

That,

$$\hat{H}_{LS}[n] = [\,\hat{H}_{LS}[n]\hat{H}_{LS}[n-1] \ldots \hat{H}_{LS}[n-1+M]] \qquad (3)$$

That M is the length of LMS filter.

3- Error in n times repeating

$$E[N] = \hat{H}_{LS}[n] - \hat{H}_{LMS}[n] \qquad (4)$$

4- The effective coefficients are changing regularly according to the equation 5:

$$\hat{W}[n+1] = \hat{W}[n] + \mu\hat{H}_{LS}[n]E^{*}[n] \qquad (5)$$

μ is an adjustable parameter.

5- Errors caused by the weight vector:

$$\epsilon[n] = W[n] - \hat{W}[n] \qquad (6)$$

Figure 5 shows the simulation results of the decrypted image using the channel estimation technique by the least square error LMS algorithm. As is clear, the encrypted image is less disturbed than the previous mode. The cause can be explained that, as per the elimination of an added noise, 16 pixels of the image data stay away from the destructive effect of noise.

Fig 5: Decrypted image with proposed method.

The diagram in figure 6 shows the relationship between error and SNR. As is clear, using OFDM technique along with channel estimation method have better results than other methods.

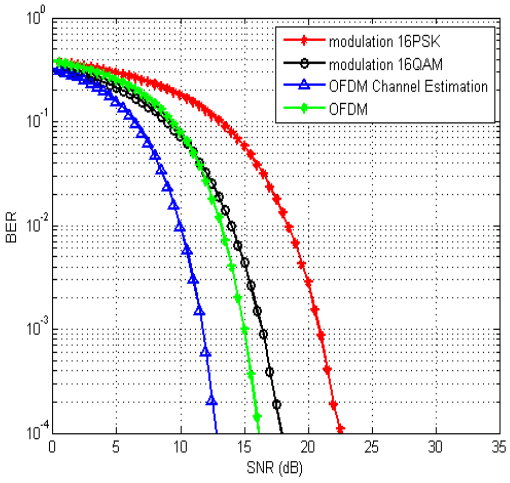


Fig 6: Relationship between error and SNR

4.CONCLUSION

It is possible to make use of matching filters in order to reduce the trace of error in the received symbols. In fact, the matching filters estimate error's level in the output by sending the guide symbols and multiply the received symbols by the weights of filter. Using LMS channel estimation algorithm is an appropriate method used for reducing the channel's effect on the encrypted data. Simulation of the decrypted images indicates the fact that the output results are much better than the state at which the channel estimation has not been used.

5.REFERENCES

[1] NIST. Announcing the advanced Encryption standard(AES), FIPS 197, Technical report, *National Institute of Standards and Technology*, November 2001.

[2] J. Daemen, V. Rijmen , "The Rijndael Block Cipher",AES Proposal:Rijndael, Document version 2, Date: 03/09/99.

[3] M. Yang , N. Bourbaki s , S. Li , " Data - Image –Video Encryption ",*IEEE POTENTIALS*, 2004.

[4] Chi-Wu Huang, " The AES Application in Image Using Different Operation Modes", 5th *IEEE Conference on Industrial Electronics and Application*,pp-393-398, 2010.

[5] Chi-Wu Huang, " The Five Modes AES Application in Sound and Images",*IEEE Sixth International Conference on Information Assurance and Security*,pp-28-31, 2010.

[6] M.Zeghid, " A Modified AES Based Algorithm for Image Encryption", *World Academy of Science Engineering and Technology*,pp-206-211, 2007.

[7] De Wang, " Image Encryption Algorithm Based on S-Boxes Substitution and Chaos Random Sequence",*IEEE International Conference on Computer Modeling and Simulation*,pp-110-113,2009.

[8] M.Hilmey, " Efficient Transmission of Chaotic and AES Encrypted Images with OFDM over an AWGN Channel", *IEEE Conference*, 2009.

[9] Henrik Schulze, Christian Luders, " Theory and Applications of OFDM and CDMA: Wideband Wireless Communications", Wiley, 2005.

[10] Saqib Saleem, Qamar-ul-Islam, " Optimization of LSE and LMMSE Channel Estimation Algorithms based on CIR Samples and Channel Taps", *IJCSI International Journal of Computer Science Issues* Vol. 8 Issue.01,pp-437-443,January 2011.

[11] Mona Nasseri and, Hamidreza Bakhshi, "Iterative Channel Estimation Algorithm in Multiple Input Multiple Output Orthogonal Frequency Division Multiplexing Systems", *Journal of Computer Science*, 2010.