TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 6077 - 6082

Secure Transmission of Medical Information by Adopting Blockchain Data Hiding Technique in Channel Coding

Mr. BabuIlluri[1], Dr. Deepa Jose[2], Ms. B. Rammyaa[3], Mr. R. Rajmohan[4]
[1]Research Scholar, Department of Electronics and Communication Engineering, KCG College of Technology, Karapakkam,
Chennai-600097
[2] Head Research & Associate Professor, Department of Electronics and Communication Engineering, KCG College of Technology, Karapakkam, Chennai-600097
[3]Assistant Professor, Department of Electronics and Communication Engineering, KCG College of Technology, Karapakkam,
Chennai-600097
[4] Associate Professor, Department of Computer Science and Engineering, IFET College of Engineering.

Article Info
Volume 82
Page Number: 6077 - 6082
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 29 January 2020*

Abstract:
Telemedicine is growing at a very rapid pace, where the doctor monitors the patient from a remote distance and provides medical assistance. This can be achieved using a wireless medium, which is prone to hacking, the patient information could be hacked through the wireless channel. To overcome this problem, we need to use the concept of blockchain into data hiding technique for medical images. The proposed blockchain data hiding scheme depends on the LSB (Least Segment Bit) steganographyand the data hiding capacity of medical image is analyzed by using Matlab tool.According to the simulation results, we observe that the BER of secret data is allowable and the data hiding capacity has been increased 0.029(hiding ratio).

Keywords: *MIMO, OFDM, channel-coding, Blockchain, BER*

I. Introduction

Now a days, the major issue in transferring a medical data through wireless communication channel, is the security of the data that is transferred.Wireless transmission these days is not as safe as it used be, due to hacking. Recent survey quotes that 13millions of sensitive information arestolen [1], which shows that hackers are equally good in extracting the data that are protected by the traditional mathematical encryption algorithms. So we intend to confuse the hackers by adopting a data hiding scheme for transmitting any sensitive information. Now data hiding scheme has become popular in security research field, changing the statistical properties of all kinds of sensitive information like audio, text, images and video that are transmitted through wireless channel.

II. Literature Survey

Hooshmand et al. [1] proposed anencoding process having polar and adopted a secret consecutive decoding algorithm, that enhances secure and coherence communication, and reduced the size of the key for polar based coding channel.

Hooshmand, Aref et al. [2] presented the quality and safe channel coding method based on the LDLC (Latin Square low-density lattice codes). Here the author also aims to reduce the key size, and created an order matrix of parity check inserted into LDLC scheme as secret key.

Esmaeil et al. [3] presented the random deletes and inserted the number of bits in a code word for

January - February 2020
ISSN: 0193 - 4120 Page No. 6077 - 6082

a QC-LDPC, based on scrambling and permutation reduced the key size.Valkilian et al. [4] presented the MIMO-OFDM system by adding block coding scheme to enhance the diversity improvement over fading (slow) wireless channel.Chen et al. [5] presents the data hiding in channel coding as a part of noise, analyzing the error correction capability and hiding capacity also.

III. Channel Coding

The basic block diagram of channel coding is shown in Figure.1 [3].

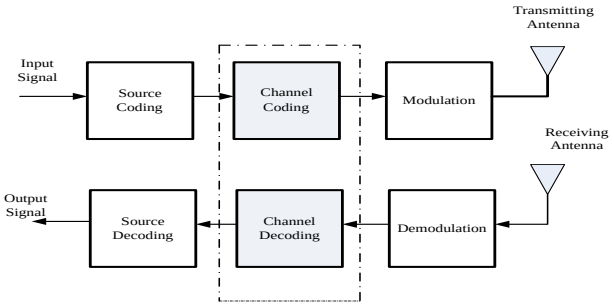

Figure.1 Channel Coding (Encoding & Decoding)

The figure.1 shows, how the information is passed through the channel coding block. The space time coding can increase the wireless spectrum efficiency

We implemented data hiding scheme by using a Multi input multi output-Orthogonal frequency division multiplexing System. The modules of a MIMO-OFDM system are; carrier data, coding channel (Space time coding) and embedded data and secret data passing through the blockchain encryption process.The encryption data and channel coding data are embedded and sent through the OFDM module. At the receiving side the image data passing through the OFDM, eliminates the first Cyclic Prefix of received signal, Channel coding and extracted the secret image data by using extraction algorithm. By combining the data hiding and cryptography process, the secret data is let into the blockchain encryption block. The channel coding can improve the reliability of transmitted information by adding redundancy [6-9]. So we have proposed a data hiding scheme that depends on the channel coding method in the MIMO-OFDM System along with space-time coding technique.

The proposed system is expressed as

$$X = HY + N$$

Here X=Received signal,
H=Channel Matrix,
Y=Transmitted signal,

A. Proposed Method

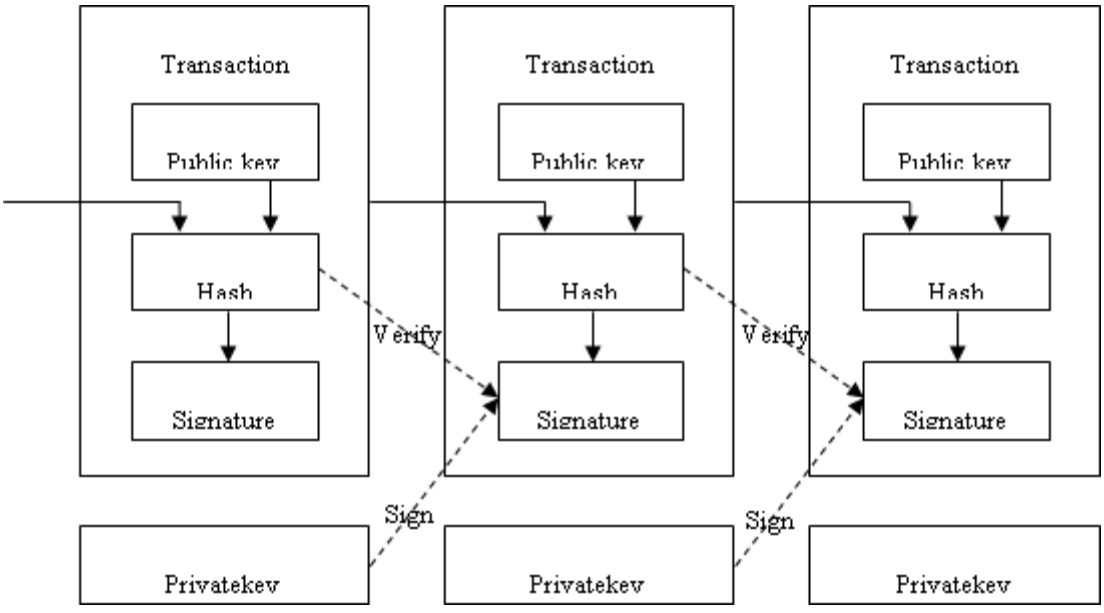

Figure.2 Functional structure of block chain encryption. [13]

January - February 2020
ISSN: 0193 - 4120 Page No. 6077 - 6082

BlockChain Encryption:

Here, the n block of image is used as input

a. Inputs are Image pixels rows
b. Hash
c. Signature

a. Inputs (Consider 64x64)

Transaction_1 →
Transaction_35 →
Transaction_64 →

65	95	95	98	94	94	94	92	83	· · ·
48	72	91	93	90	92	86	82	·	· ·
50	54	62	80	85	75	65	.	·	· ·
75	65	78	85	90	68		·	·	·
.	.	.	.	.	.		.	.	.
.	.	.	.	.	.		.	.	.
.	.	.	.	.	.		.	.	.
66	88	107	107	60	85		.	.	.

We need to generate public (p_b) and Private (n_b) keys using ECC (Elliptical Curve Cryptography) algorithm of each transaction

Example: p_b = {735162270093215432149989210}

n_b = {213104231967314321497271090}

b. We need to generate for hash values for each transaction along with previous transaction hash values also, then after it will creates a block.

By using blokchain techniques into medical image transmission in terms of image pixel values which would be converted into a binary format, and each binary values of particular image pixel values will be generate hash values by using SHA-512. By adopting block chain concept into image pixel values, we restrict the hacking of the original medical image.

This is s due to the fact that each and every transaction needs a previous hash value, which is not that much easy and hence retrieval of the sensitive information is prohibited.

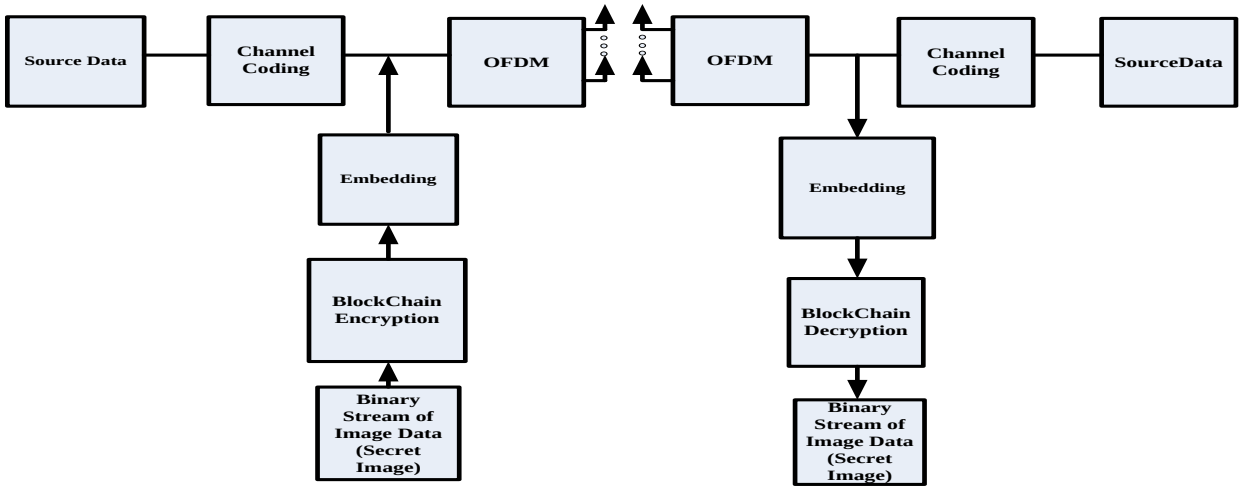

Figure.2 Hiding the Data as adopted Blockchain Methodin

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 6077 - 6082

MIMO-OFDM System

The capacity of data hiding depends upon the SNR value and the structure of OFDM frame and coding channel. Assuming that the SNR value is 20dB then the size of the given carrier data having 9,500 bits after passing through the channel coding and encoded cover data has 21,256 pixels per image bits[7]. And carrier data is based on ECC channel coding and secret data use error correction coding. The channel model has a 2 rays Rayleigh channel and QAM modulation used.

Algorithm steps: Encryption

Input: secret image & source image	
Output: encrypted image(cipher form)	
1	Procedure :Source coding
2	Coding Channel
3	Secret data(image)
4	Go to adopt blockchain encryption process
5	Embedding: channel coding-embedding data output
6	Go to OFDM
7	From OFDM to Antenna

Decryption process

Input: encrypted image(cipher form)	
Output: Decrypted image(original form)	
1	Procedure :Antenna to OFDM
2	Coding Channel
3	Secret data(image)
4	Embedding: channel coding-embedding data output
5	Go to adopt blockchain Decryption process
6	Retrieve the original medical image
7	|| Source Data

B. Simulation Analysis

Figure 3 represents the performance of BER of a carrier signal data of medical image and the source (host)signal data that are processed through a adopt blockchain encryption block in terms of channel coding method, and 2x2 MIMO-OFDM system used. As per the Figure, 30dB SNR (Signal to Noise Ratio) value occurs and BER (Bit Error Rate) is of the range of 10^{-2} level for carrier signal and10^{-4} level of source signal.

Hiding capacity equation [5]

$$=\frac{\text{the lengt h of extracted secret data}}{\text{the lengt h of encoded cover data}}$$

Embedding the secret data along with the host image data, analysis of the Peak signal to noise ratio (PSNR) is given below.

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

Mean Square Error between x and x`

$$MSE=\frac{1}{MXN}\sum_{a=0}^{M}\sum_{b=0}^{N}(x(a,b)-x'(a,b)^2$$

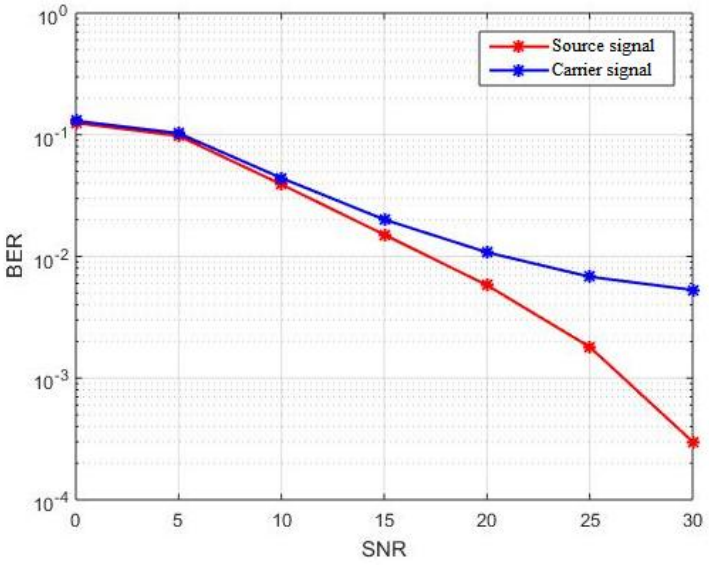

Figure 3 BER performance

January - February 2020
ISSN: 0193 - 4120 Page No. 01 - 11

x(a,b) =host image pixel values and x'(a,b) cover image pixel values. M and N are height and width of the image. Figure 4 show the Matlab simulation results

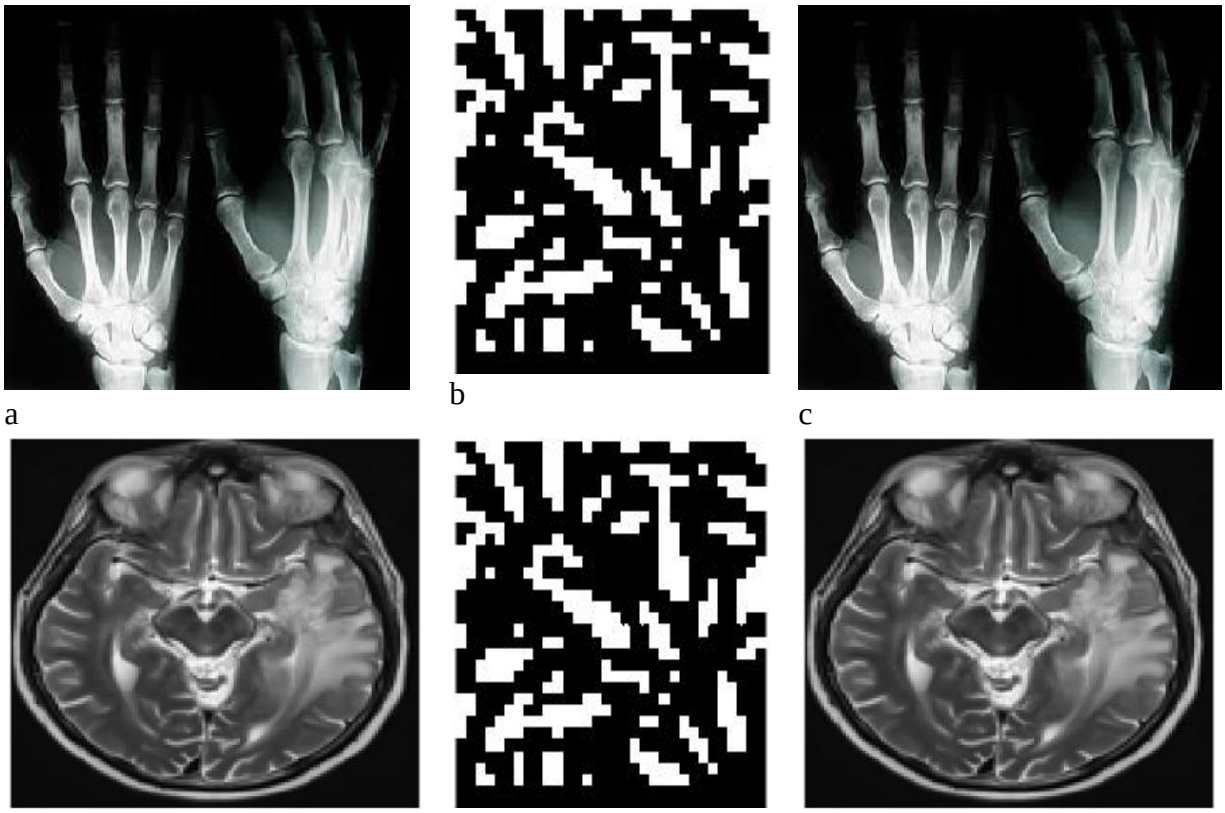

Figure 4 a. Medical Image b. Encrypted Image by using adopted Blockchain concept c. Retrieve the original Medical image

Table.1 Capacity hiding of medical image

Medical Image	PSNR(dB)	Capacity(Hiding)[5]		Capacity(Hiding) Proposed method	
		Per bits	Ratio	Per bits	Ratio
X-Ray	36.46	197502	0.0942	197502	0.0953
CT Scan	36.67	197438	0.0941	197438	0.0951
CT Scan Tumor	37.07	197435	0.0941	197435	0.0945
MRI Scan	35.82	196628	0.0942	196628	0.0958
Head CT Scan	38.3	197873	0.0943	20,147	0.0972

IV. Conclusion

This proposed work results in increased data hiding capacity while passing through the MIMO-OFDM system by incorporating blockchain concept in channel coding method. By adding blockchain concept into a channel coding method, the medical image is found to be transmitted more securely compared to the traditional encryption process. The future work of this paper is to adopt

January - February 2020
ISSN: 0193 - 4120 Page No. 01 - 11

this encryption technique in defense applications, communicating securely to the destination without any loss.

Reference

1. R. Hooshmand andM.Aref,"Polar code-based secure channel coding scheme with small key size" IET Communication,Vol.11,no.15,pp.2357-2361,2017.
2. R. Hooshmand andM.Aref,"Efficient secure channel coding scheme based on low-density Lattice codes"IET Communications,Vol.10 No.11,pp.1365-1373,2016
3. BabuIlluri, Deepa Jose, "Countermeasure to protect sensitive information stealthily in remote interchanges using steganography in educational environments", International Journal of Electrical Engineering & Education, doi.no:10.1177/0020720918825239
4. D. R. DenslinBrabinEmailauthorJ. Raja Paul PerinbamD. Meganathan,"A Block Based Reversible Data Hiding Scheme for Digital Images Using Optimal Value Computation", Wireless Personal Communications-Springer,June 2017, Volume 94, Issue 4, pp 2583–2596.
5. [5]L. Chen, Z. Fan and J. Huang, "Data hiding capacity of spatial domain bit replacement steganography in an MIMO-OFDM coding channel", AEU - International Journal of Electronics and Communications, vol. 70, no. 9, pp. 1295-1303, 2016.
6. J. Park and T. Ogunfunmi, "Efficient FPGA-Based Implementations of MIMO-OFDM Physical Layer", Circuits, Systems, and Signal Processing, vol. 31, no. 4, pp. 1487-1511, 2012.
7. G. Sworo, K. Dandekar and M. Kam, "Reconfigurable antennas and link adaptation algorithms for MIMO-OFDM wireless systems", EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, 2015.
8. S. Faraji, A. Salari and S. Sheikhaei, "Fixed-point implementation of interpolation-based MMSE MIMO detector in joint transmission scenario for LTE-A wireless standard", AEU - International Journal of Electronics and Communications, vol. 70, no. 11, pp. 1506-1514, 2016.
9. M. Wu, C. Dick, J. Cavallaro and C. Studer, "High-Throughput Data Detection for Massive MU-MIMO-OFDM Using Coordinate Descent", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 63, no. 12, pp. 2357-2367, 2016.
10. P. Wang, C. Li and Z. Xu, "A Cost-Efficient Real-Time 25 Mb/s System for LED-UOWC: Design, Channel Coding, FPGA Implementation, and Characterization", Journal of Lightwave Technology, vol. 36, no. 13, pp. 2627-2637, 2018.
11. N. Kirubanandasarathy and K. Karthikeyan, "Design of pipeline R2MDC FFT for implementation of MIMO OFDM transceivers using FPGA", Telecommunication Systems, vol. 63, no. 3, pp. 465-471, 2016.
12. Y. Sakakibara, K. Nakamura and H. Matsutani, "An FPGA NIC Based Hardware Caching for Blockchain", Proceedings of the 8th International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies - HEART2017, 2017.
13. https://bitcoin.org/bitcoin.pdf