DIU Journal of Science and Technology Volume 12, Issue 1, January 2017

2017-01

Effect of Different Block Cipher Modes of Operation for Secured Data Transmission in Convolutional Encoded Dwt Based Mimo Mc-Cdma System

Shams, Rifat Ara

Daffodil International University

EFFECT OF DIFFERENT BLOCK CIPHER MODES OF OPERATION FOR SECURED DATA TRANSMISSION IN CONVOLUTIONAL ENCODED DWT BASED MIMO MC-CDMA SYSTEM

Rifat Ara Shams

Department of Computer Science and Engineering
Daffodil International University

Email: rifat.cse@diu.edu.bd

Abstract: *In this proposed model, performance of different block cipher Modes of operation over ZF channel equalization technique and BPSK modulation scheme in DWT based MIMO Multi-Carrier Code Division Multiple Access (MC-CDMA) system has been analyzed for security issues through simulation. This system is proposed using convolutional coding scheme over AWGN and Rayleigh fading channel with Walsh Hadamard code as orthogonal spreading code. In this research paper, the performance of Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode, Output Feedback (OFB) mode and Counter (CTR) mode is compared as cryptographic algorithms to encrypt the actual data and decrypt its original form.*

Keywords : *ECB, CBC, CFB, OFB, CTR*

1. Introduction

Nowadays we are depending on technology and without it we cannot even imagine to continue a single day. High quality communication without distortion and low cost is the most expected requirement of most of the users [4]. It may sound absurd, but with the development of science and technology, we are facing many troubles regarding security. Security is now the biggest challenge and burning issue in every sector. Paying attention on this issue, several cryptographic algorithms have been developed to provide secured environment.

In previous research [4], performance of different equalization schemes on convolutional encoded Discrete Wavelet Transform (DWT) based MIMO Multi-Carrier Code Division Multiple Access (MC-CDMA) wireless communication system has been measured. In this research work, a model of MIMO MC-CDMA wireless communication system is proposed, where different block cipher modes of operation are compared on text data for intense security of data transmission. My attempt is to find out the best as well as the most secured cryptographic algorithm which suits best with the MIMO MC-CDMA system.

2. Different Block Cipher Modes of Operations

A block cipher mode of operation is a cryptographic algorithm that uses a block cipher to ensure confidentiality and authenticity [1]. It is named “block cipher” because this is the simplest way where plaintext is divided into several 64 bit blocks and encryption is done for each block using the same key. The last block should be padded to 64 bit if it is shorter. In case of encrypting identical plaintext blocks with same secret key results identical cipher text blocks. It is a very hazardous situation for the users as an intruder would be able to guess what the message is by observing the identical cipher text blocks though he/she has no idea of what the original message is. Therefore, to improve this situation and to get different output cipher text blocks from identical input plaintext blocks, different block cipher modes of operations have been launched where the plaintext blocks are mixed with the cipher text blocks and then the result is used as the cipher input [2]. In this research, five different block cipher modes of operations have been used.

Date of submission : 15.03.2017 Date of acceptance : 25.06.2017

2.1 Electronic Codebook (ECB) Mode

In Electronic Codebook (ECB) Mode, all the same sized plaintext blocks are encrypted with the same key to produce the corresponding cipher text blocks. This algorithm is not much protected because identical plaintext blocks produce identical cipher text blocks as it uses the same secret key for every block. Moreover, if the plaintext blocks are encrypted two times under the same key, it produces the same cipher text blocks as encrypted one.

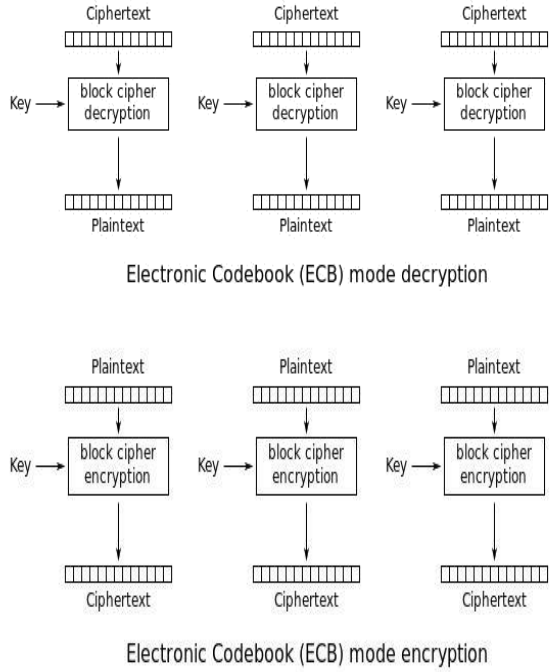

Figure 1: Process of Encryption and Decryption of Electronic Codebook (ECB) Mode [1]

2.2 Cipher Block Chaining (CBC) Mode

Cipher Block Chaining (CBC) mode builds a sequential chain where each plaintext block is XORed with the previous cipher text block except the first plaintext. The first plaintext is XORed with an initialization vector to produce unique output. It produces different cipher text for identical plaintext. If a single bit of a plaintext is changed, all subsequent cipher text blocks are damaged as these are connected like a chain and it is not possible to decrypt the cipher text which was received from this plaintext [2].

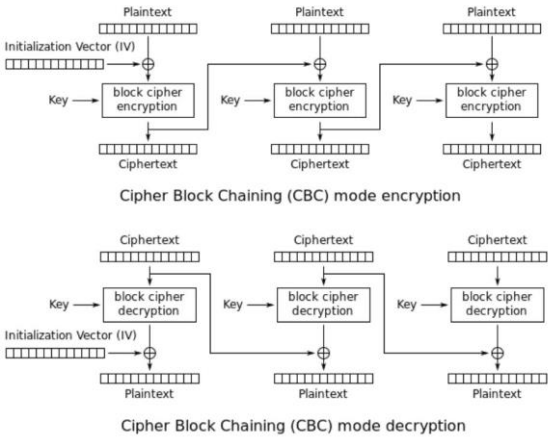

Figure 2: Process of Encryption and Decryption of Cipher Block Chaining (CBC) Mode [1]

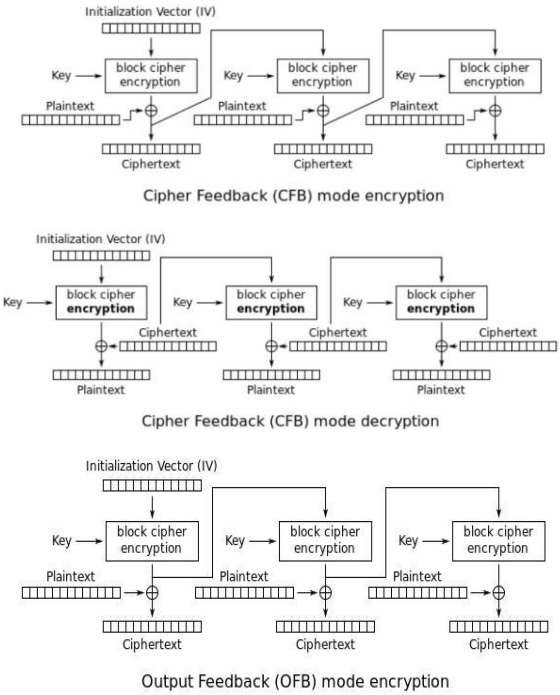

Figure 3: Process of Encryption and Decryption of Cipher Feedback (CFB) Mode [1]

2.3 Cipher Feedback (CFB) Mode

Cipher Feedback (CFB) mode is just like as CBC. The main difference is that, here at first the cipher text block of previous stage is encrypted by a secret key and then it is XORed with the plain text and finally the required cipher text block is achieved. If any bit is missing from cipher text block while decrypting, the whole plain text block is not affected; only few portion is affected.

2.4 Output Feedback (OFB) Mode

In Output Feedback (OFB) mode, block cipher in previous stage acts as input of the current stage like key-stream generator [3]. Then this stream cipher block is XORed with the plaintext to produce the corresponding cipher text block. If one bit of cipher text is changed during decryption, only the same bit of plain text is changed not to affect the other bits.

2.5 Counter (CTR) Mode

Counter (CTR) mode is as like as CFB mode with counter except feedback process. Initially counter, which is same as initialization vector for CBC and CFB mode, is loaded in the upper register and almost similar for sender and receiver. Then elements of the counter is encrypted with that particular key and placed in the lower register and after that the initial plaintext block is XORed with the contents of the bottom register that results the corresponding cipher text block [3].

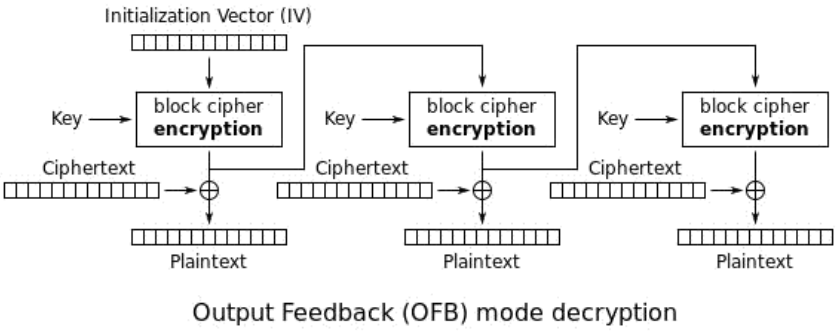

Figure 4: Process of Encryption and Decryption of Output Feedback (OFB) Mode [1]

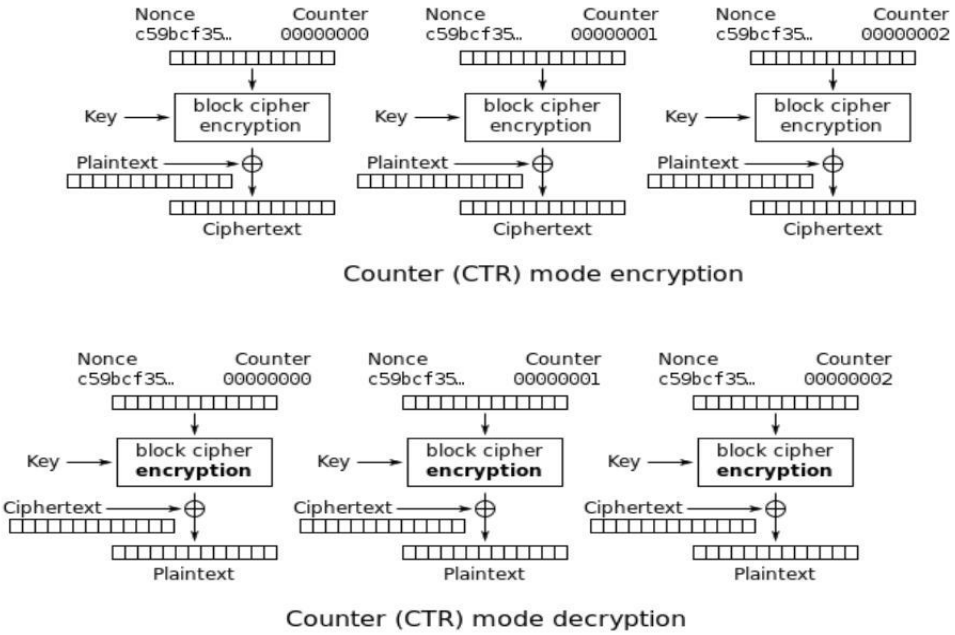

Figure 5: Process of Encryption and Decryption of Counter (CTR) Mode [1]

3. System Model

A DWT based wireless communication system with multiple users and 2 × 2 input-output has been proposed as depicted in Figure 6. In this MC-CDMA system, the text message for four users has been passed through multiple antennas with different block cipher modes of operation for Cryptographic purpose. This is done for

minimizing the unlawful access of text data. Here, Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode, Output Feedback (OFB) mode and Counter (CTR) mode have been used for comparing and deciding that which one performs better. After applying these process, the encrypted data are passed through a channel encoder which is ½-rated and convolutional. After that, they are interleaved as well as digitally modulated using BPSK. Then, the symbols are combined with Walsh Hadamard codes, passed through IDWT and spatially multiplexed. The encrypted signals are then transmitted from the multiple transmitting antennas. While receiving, the transmitted signals are equalized using ZF channel equalization technique and then sent for decoding and FWT and mixed with Walsh–Hadamard codes. The bits are then passed through decopier, modulation technique, deinterleaving section and decoder precisely. Finally the bit stream is manipulated with different decryption algorithms like block cipher mode of operations for retrieving the original transmitted text scrupulously.

4. Simulation Parameters

Here, MATLAB 10 has been used for simulation of DWT oriented MIMO MC-CDMA system where different texts have been utilized for encryption and decryption using different block cipher mode of operations and retrieved the plaintexts again. The proposed system for this wireless communication system is simulated using the following parameters shown in table 1.

Table 1 Parameters for simulation

Parameters	Types
User	4
Input Data	Text
Signal Processing Scheme	Wavelet
Modulation	BPSK
SNR	0 – 10 dB
Spreading Code	Walsh- Hadamard Code
Signal Detector (Equalizer)	ZF
Cryptographic Algorithm	ECB, CBC, CFB, OFB, CTR
Antenna Detection	2 x 2

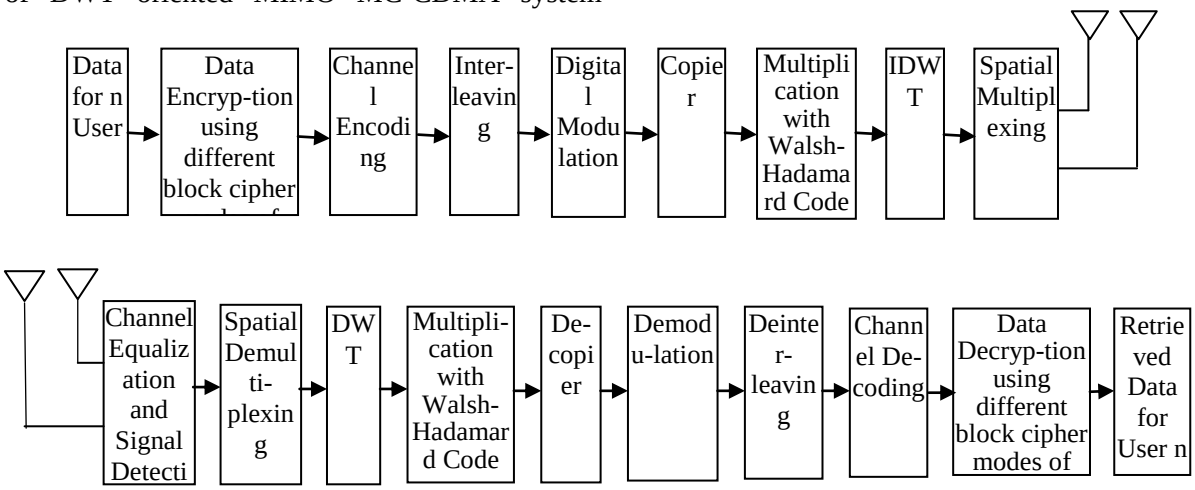

Figure 6: Block diagram of a DWT oriented MIMO MC-CDMA wireless communication sytem

5. Simulation Results and Discussion

The diagram presented in figure 7 shows the original transmitted messages, encrypted and decrypted messages for four users using Electronic Codebook (ECB) mode of operation in DWT based MIMO MC-CDMA system using BPSK digital modulation with implementation of ZF channel equalization scheme at 10 dB SNR value. It is observed from the figure that, in all cases the encrypted text message is totally unintelligible, that is, it does not have any similarity to that of the original text message whereas this message can be retrieved with the

decrypted one. One important point has been noticed here that, user 3 and user 4 transmitted same messages and the corresponding encrypted texts are also same. This property is a threat for security because it is easy to guess what the original text could be.

In Figure 8, the transmitted, encrypted and decrypted messages for different users at SNR value of 10 dB have been presented using Cipher Block Chaining (CBC) mode of operation in DWT based MIMO MC-CDMA system. It is observed from the figure that, there is no similarity in plain text and cipher text but the original message is retrieved precisely after decryption. Here, user 3 and user 4 transmitted same messages but the corresponding encrypted texts are different.

Text for User 1	**Encrypted Text**	**Decrypted Text**
Wireless technology has progressed significantly during the past decade.	KMÍU6ì`ª÷ • t.E-n1éÜª Vn°Yaõ-}Þ·lå2lÍü^hÌY& Í2Cgn§H¬"aAññ.ùã6xA0Zð äF+q^q üÂh%NÀ+_-Ä xÅAò £8¯8H~a´'àÉ/Vâ	Wireless technology has progressed significantly during the past decade.
Text for User 2	**Encrypted Text**	**Decrypted Text**
An error correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system complexity.	]JU(û¦ªàe4Nv7-þÜ¡ A+à[kà9wß©h¦$ÒdÅó]sÜ%Ñ2A p□Må:pÅÂI¥µ/èå%qMÑY4î3âæÄ c4Jq3ã • «Kn¥Ekà8a • äk«%bÇáP-Y&AÇkTpjéLã;hÙI • üÿJW	An error correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system complexity.
Text for User 3	**Encrypted Text**	**Decrypted Text**
Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.	NEÛY5©géëx*Dk;° • °)¥Ekà>tÁ½)© xÊóQdË!AÀwU • f'¦I¬"aÕ • êµ?ð á#uKÑ;çwÐéì~(LQo;ø ¦HD"¯Ei²(qÙ¬)-$ÒfÆñQtÂ) ÑaTÀvh§[þ9$ÈCë¸;éåy	Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.
Text for User 4	**Encrypted Text**	**Decrypted Text**
Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.	NEÛY5©géëx*Dk;° • °)¥Ekà>tÁ½)© xÊóQdË!AÀwU • f'¦I¬"aÕ • êµ?ð á#uKÑ;çwÐéì~(LQo;ø ¦HD"¯Ei²(qÙ¬)-$ÒfÆñQtÂ) ÑaTÀvh§[þ9$ÈCë¸;éåy	Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.

Figure 7: Transmitted plaintext, encrypted and decrypted texts for four users using Electronic Codebook (ECB) Mode of operation

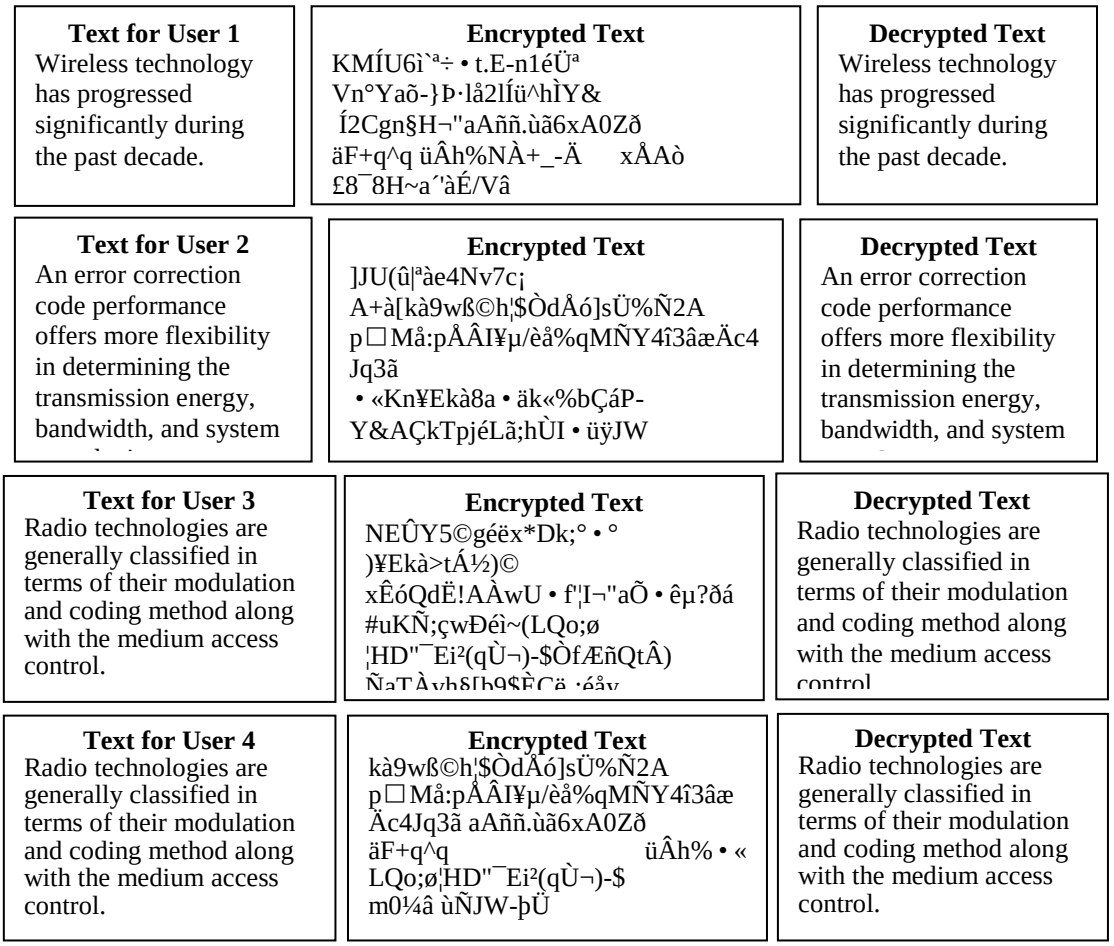

Figure 8: Transmitted plaintexts, encrypted and decrypted texts for four users using Cipher Block Chaining (CBC) mode of operation

Another example of Cipher Block Chaining (CBC) mode of operation is shown in figure 9. In this case, I have changed the first word of plain text of user 4. A disaster happened in decrypted text; original text is not retrieved for any user, though I have changed only one word of a user. This is because, CBC acts like a chain, therefore any small change can affect broadly.

In figure 10, the transmitted, encrypted and decrypted messages for different users at SNR value of 10 dB have been presented using Cipher Feedback (CFB) mode of operation. Using this algorithm, original texts are retrieved accurately, but in case of slight changes in plaintext causes slight changes in decrypted output. For this reason, the overall performance of CFB mode is much better than CBC mode.

Figure 11 shows the plain text, cipher text and the retrieved original text for four users using Output Feedback (OFB) mode of operation in DWT based MIMO MC-CDMA system. It is observed from the figure that, the original message is retrieved precisely after decryption. If any changes in plain text is made like user 4, only those bits are changed after decryption. So, this algorithm provides better performance.

In Figure 12, the transmitted, encrypted and decrypted texts for different users at SNR value of 10 dB have been presented using Counter (CTR) mode of operation in MIMO DWT based MC-CDMA system with BPSK digital modulation and ZF channel equalization technique. In this algorithm, it is noticeable that, encrypted texts are different for every user even the plain texts are same for two users. By using this algorithm, all the required original texts are retrieved precisely by decryption. Therefore, CTR mode provides much satisfactory performance than others.

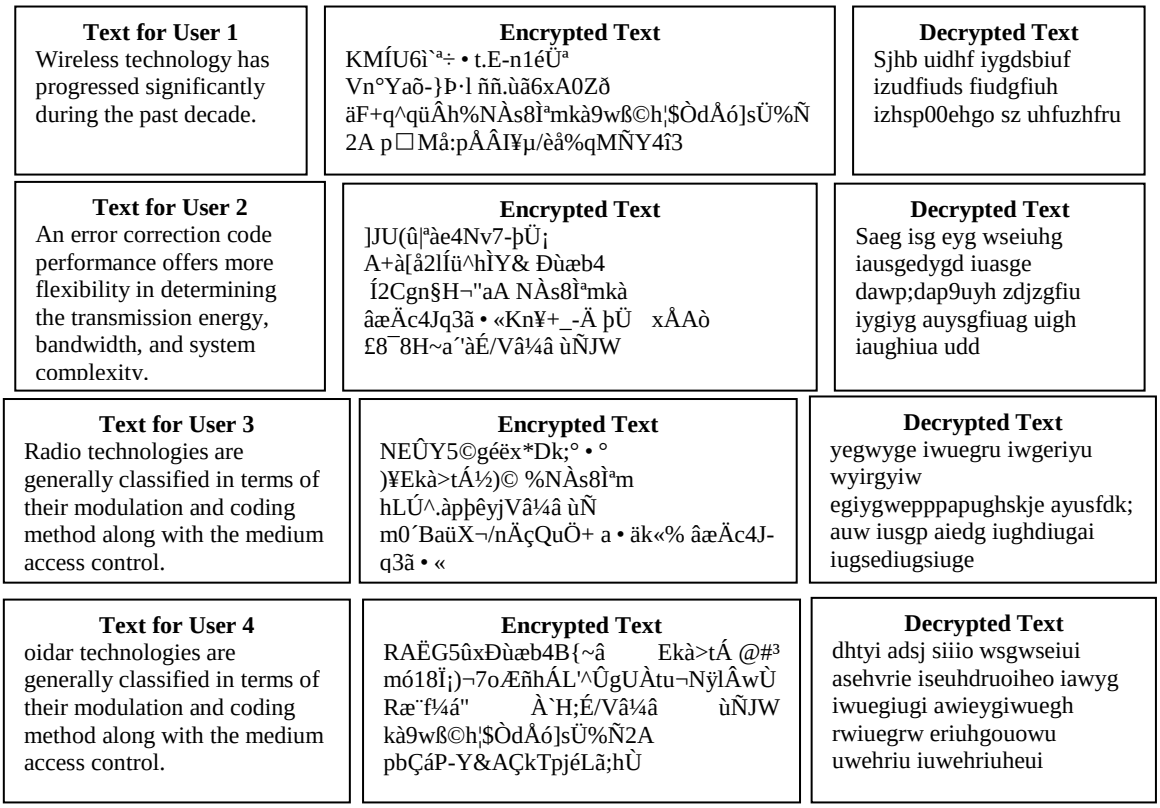

Figure 9: Second example of transmitted plaintexts, encrypted and decrypted texts for four users using Cipher Block Chaining (CBC) mode of operation

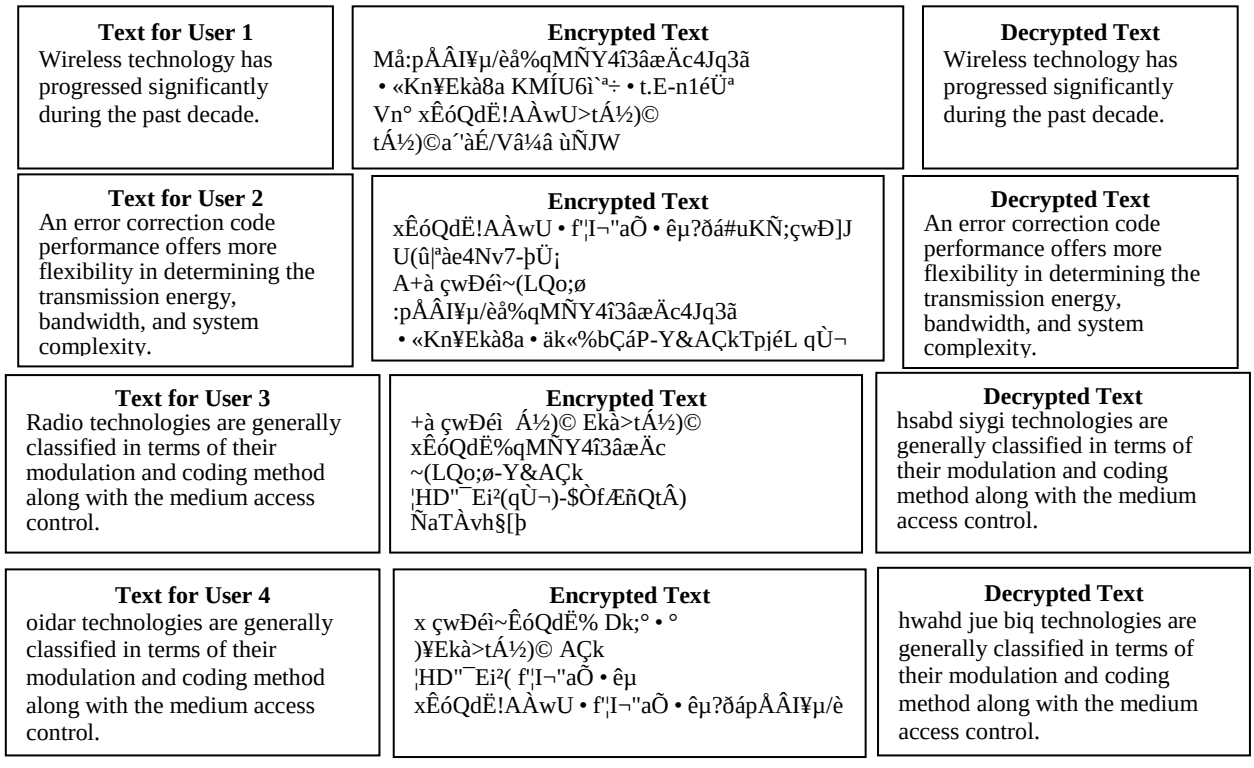

Figure 10: Transmitted plaintexts, encrypted and decrypted texts for four users using Cipher Feedback (CFB) mode of operation

Text for User 1	Encrypted Text	Decrypted Text
Wireless technology has progressed significantly during the past decade.	KMÍU6ì`ª÷ • t.E-n1éÜª Vn°Yaõ-}Þ·lå2lÍü^hÌY& Í2Cgn§H¬"aAñn.ùã6xA0Zð äF+q^q üÂh%NÀ+_-Ä xÅAò £8¯8H~a´'àÉ/Vâ¼â ùÑJW	Wireless technology has progressed significantly during the past decade.
Text for User 2	**Encrypted Text**	**Decrypted Text**
An error correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system complexity.	]JU(û|ªàe4Nv7-þÜ¡ A+à[kà9wß©h¦$ÒdÅó]sÜ%Ñ2A p□Må:pÅÂI¥µ/èå%qMÑY4î3âæÄc4Jq3ã • «Kn¥Ekà8a • äk«%bÇáP- Y&AÇkTpjéLã;hÙI • üÿJW	An error correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system complexity.
Text for User 3	**Encrypted Text**	**Decrypted Text**
Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.	NEÛY5©géëx*Dk;° • °)¥Ekà>tÁ½)© xÊóQdË!AÀwU • f'¦I¬"aÕ • êµ?ðá#uKÑ;çwÐéì~(LQo;ø ¦HD"¯Ei²(qÙ¬)-$ÒfÆñQtÂ) ÑaTÀvh§[þ9$ÈCë¸;éåy	Radio technologies are generally classified in terms of their modulation and coding method along with the medium access control.
Text for User 4	**Encrypted Text**	**Decrypted Text**
oidar technologies are generally classified in terms of their modulation and coding method along with the medium access control.	NEÛY5©géëx*Dk;° • °)¥Ekà>tÁ½)© xÊóQdË!AÀwU • f'¦I¬"aÕ • êµ?ðá#uKÑ;çwÐéì~(LQo;ø	fgrid technologies are generally classified in terms of their modulation and coding method along with the medium access control.

Figure 11: Transmitted original messages, encrypted and decrypted messages for four users using Output Feedback (OFB) mode of operation

Text for User 1	Encrypted Text	Decrypted Text
Wireless technology has progressed significantly during the past decade.	lå2lÍü^hÌY 6ì`ª÷ • t.E-n1éÜª Vn°Yaõ-}Þ ªàe4Nv7-þÜ · & ½)© ªàe4Nv7Í2Cgn§H¬"aAñn.ùã6xA0Zð äF+q^q üÂh%NÀ+_-Äa • äk	Wireless technology has progressed significantly during the past decade.
Text for User 2	**Encrypted Text**	**Decrypted Text**
An ttht correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system	(û|ªàe4Nv7-þÜ¡ ªàe4Nv7-þÜ¡ \\kà9wß©h¦$ÒdÅó]sÜ%Ñ2A p□lå2lÍü^hÌY&ã6xA âæÄc4J • «K «%bÇáP;hÙI • üÿJW	An ttht correction code performance offers more flexibility in determining the transmission energy, bandwidth, and system
Text for User 3	**Encrypted Text**	**Decrypted Text**
Radio technologies are generally classified in terms of their modulation and coding method along with the medium access	n¥Ekà8a • äkgéëx*Dk;° • °)¥Ekà>tÁ½)© ªàe4Nv7-þÜ¡ /èå%qMÑY4î3âæÄc4Jq3ã -Y&AÇkTpjéLã	Radio technologies are generally classified in terms of their modulation and coding method along with the medium access
Text for User 4	**Encrypted Text**	**Decrypted Text**
Radio technologies are generally classified in terms of their modulation and coding method along with the medium access	n¥Ekà8a • äkgéëx*Dk;° • °)¥Ekà>tÁ½)© ªàe4Nv7-þÜ¡ /èå%qMÑY4î3âæÄc4Jq3ã -Y&AÇkTpjéLã	Radio technologies are generally classified in terms of their modulation and coding method along with the medium

Figure 12: Transmitted original messages, encrypted and decrypted messages for four users using Counter (CTR) mode of operation

6. Conclusion

In this research work, comparison between different block cipher modes of operation in DWT based convolutional encoded 2 × 2 antenna supported MC-CDMA system with implementation of BPSK digital modulation as well as ZF channel equalization scheme has been done. After getting the output of simulation, I can conclude that, Counter (CTR) mode provides the best result among the others though other modes also have satisfactory performance. By using this cryptographic algorithm, confidentiality of data can be ensured. Hence, by adopting this system, secured transmission of data is possible.

References

[1] John Black, Phillip Rogaway, "A Block cipher mode of operation for parallelizable message authentication", International Conference on the Theory and Application of Cryptographic Techniques, Eurocrypt 2002, pp. 384-397.

[2] Phillip Rogaway, "Evaluation of some Block cipher modes of operation", Cryptography Research and Evaluation Committees (CRYPTEC).

[3] Morris Dworkin, "Recommendation for Block Cipher Modes of Operation- Methods and Techniques", National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce (NIST), 2001 edition.

[4] Rifat Ara Shams, M. Hasnat Kabir, Mohammed Mustaqim Rahman, "Effect of Channel Equalization Schemes in Performance Evaluation of a Secured Convolutional Encoded DWT Based MIMO MC-CDMA System", Global Journal of Computer Science and Technology, Volume 14, Issue 6, Version 1, Year 2014.