Stream Cipher with Space Time Block Code Hanaa
Mohsin Ahmed and Anwar Abbas Hattab
Pages 227 – 235
DOI: http://dx.doi.org/10.21700/ijcis.2016.127

Stream Cipher with Space-Time Block Code

Hanaa Mohsin Ahmed and Anwar Abbas Hattab
Department of Computer Science,
Iraq University of Technology
Baghdad, Iraq
[110113, anwarabbas76]@ uotechnology.edu.iq

Abstract: *This paper proposes a new method to secure data in the physical layer (physical layer cipher) in mobile networks using a cipher with channel code (space-time block code or STBC), which is used to increase reliability in wireless networks. In this method, we will cipher the STBC codewords and use a new approach to produce keys related to arithmetic attributes of images as an average value. There is no requirement to insert any major key by the user. In this method, the average value of the packet is used as a seed for the linear feedback register (LFSR). Then, it will generate keys as complex forms that are used to cipher STBC codewords; the results practically and theoretically show a stronger method against plain attackers, known-plaintext attacks, choice plaintext attackers, and ciphertext attackers and creates more confusion and diffusion to make cipher analysis more difficult. Their effect on security is discussed. Performance, system architecture, and the proposed method satisfy the performance analysis tests (of the image), such as the histogram, power spectrum, correlation, large key space, NPCR, UACI, and entropy, and it is resistant to statistical, brute force, and differential attacks.*

Keywords: *Physical Layer Security, STBC, Stream Cipher, Image Cipher, Complex Number.*

Received*: May 01, 2016* | **Revised***: August 10, 2016* | **Accepted***: September 10, 2016*

1. Introduction

One of the most important technologies in current wireless communications is multiple-input multiple-output (MIMO) antenna systems because of their capability to increase the system's capacity and reliability. The system of the MIMO antenna is used in the current fourth generation (4G) wireless networks, such as Wi-Fi (IEEE 802. 11n) and long-term evolution (LTE), to perform a significantly higher rate of data transfer and to enhance the spectral efficiency. The invention of the MIMO system [1] led to the introduction of the multiple-antenna coding scheme, known as the space-time code (STC) [2]. The scheme has the potential to significantly exploit MIMO gains offered by multiple-antenna transmission and coding offered by the encoding scheme, which is distributed. Several schemes employing multiple-antenna arrays with STC were advanced in [3–7]. Space-time trellis code (STTC) and space-time block code (STBC) are two essential kinds of STC techniques. Several recent wireless standards have used STBC due to its low decoding complexity in comparison to STTC. Mobile networks lack physical outlines and infraction comes from the outside, without the request of real telecommunication. The lack of boundaries in these methods makes them weak in physical-layer security. The security becomes an essential element of attention in the physical layer. Cryptographical methods can be applied to supply security to a mobile network. The protection in a traditional cryptography system is formed on unproved assumptions (regarding the complexity of certain calculative functions), which are insecure if assumptions are wrong or if efficient attacks are developed.

Reference [8] indicated that the physical-layer protection below the information-theoretic security patterns can be obtained to be close to ideal privacy in theory if long codes are applied to secrecy expansion. There are no computational bounds to be placed on the attacker in a physical-layer protection method; nevertheless, the information-theoretic protection is an average-information scale. The technique can be planned for precise planes of security [9]. In this paper, a new method is proposed to protect data in a mobile network in the physical layer by joining STBC with stream cipher, as shown in Figure 1.

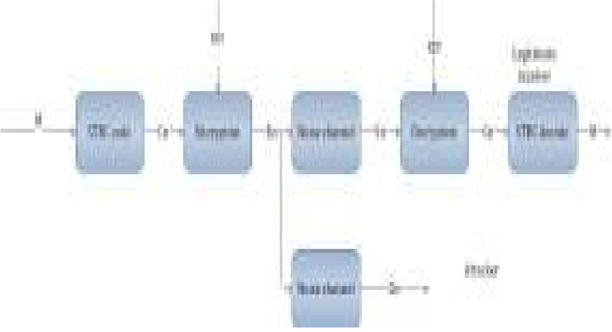


Figure 1. Proposed encryption method after STBC

Confidentiality is urged in the physical layer by encoding the channel and then encrypting the data. The critical benefit of the method is preventing eavesdroppers from obtaining advantageous data since decryption of encrypted codes is unfeasible due to the need for distinguishing the master key.

We presented that, in the noise channel, this prime key is needed to split change due to the channel noise and encryption. Additionally, the attackers must acquire proper duplication from the obtained information without realizing the prime key, and attacker will notice the unacceptable channel with noise and errors. In the previous case, the attackers are not capable of collecting the cryptograph samples without error. In the second situation, the attackers may be able to obtain key samples applied to encrypt famous encodings of plaintext patterns but cannot gain the ciphertext of encodings with plaintext patterns in similar cases. The attacker's ability to catch and examine the cipher is reduced [10].

The rest of this paper is ordered as follows: Section 2 explains the normal STBC. Section 3 describes the proposed method and key generation. Section 4 explains the action of a legitimate receiver. Section 5 explains the performance analysis. The conclusion from this paper is presented in Section 5.

2. Normal STBC

The STBC is a complicated scheme of Alamouti's STC in [11]. The input data are formed as an array, which has the same number of rows as the transmit antennas in addition to its columns having the same time slot number needed to transfer the input data. At the receiver edge, while signals are attained, they are initially joined and then conveyed to the "maximum likelihood detector" where the decision rules are carried out. The STBC codes were planned to reach the maximum variety. Figure 2 shows a block diagram of STBC (2X1).

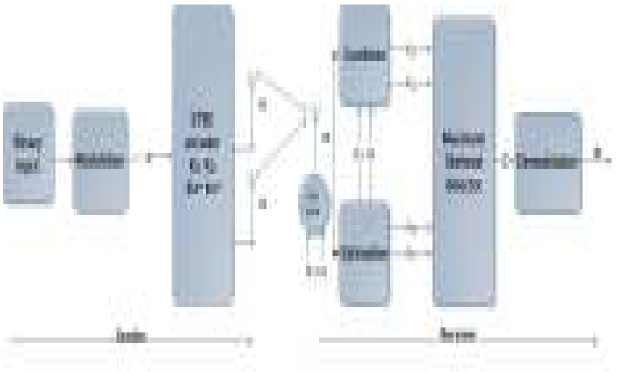


Figure 2. STBC (2X1)

On the sender side, input data enters the modulator device and then the Alamouti encoder picks two blocks, $K1$ and $K2$, at the same time and produces a matrix. Then, $K1$ is sent through Antenna 1 and $K2$ is sent through Antenna 2, which are defined as follows:

$$K = \begin{bmatrix} K1 & K2 \\ -K2* & -K1* \end{bmatrix} \quad (1)$$

where the symbol * denotes the complex conjugate. Thus, $K1*$ is the complex conjugate of $K1$. The encoder's outputs are transmitted in two sequential transmission periods from the two transfer antennas. In the first transmission period, the signal $K1$ is transmitted from Antenna 1, and the signal $K2$ is transmitted from Antenna 2, at the same time. In the second transmission period, the signal $K2*$ is transmitted from Antenna 1, and the signal $K1*$ is transmitted from Antenna 2:

$$K1=[K1 \;\; K2*]$$
$$K2=[K2 \;\; K1*] \quad (2)$$

The inner product of $K1$ and $K2$ corresponds to null (zero). This affirms the orthogonality of the Alamuti (STBC) method, which is transferred from Antenna 2. The fading coefficients symbolized by $Ht1$ for Antenna 1 and $Ht2$ for Antenna 2 are assumed to be fixed through the two consecutive, where H is the phase shift and amplitude gain, and the corresponding T is the transmission period. They can be explained as follows:

$$H1\,(\mathrm{t}) = H1\,(t+T) = H1 = |H1|e^{J\theta 1}$$

$$H2\,(\mathrm{t}) = H2\,(t+T) = H2 = |H2|\, e^{J\theta 2} \quad (3)$$

The receiver receives $R1$ and $R2$, indicating the two received signals over the two sequential symbol periods for time t and $t + T$. The received signals can be stated by:

$$\begin{bmatrix} R1 \\ R2 \end{bmatrix} = \begin{bmatrix} K1 & K2 \\ -K2^* & K1^* \end{bmatrix} * \begin{bmatrix} H1 \\ H2 \end{bmatrix} + \begin{bmatrix} N1 \\ N2 \end{bmatrix}$$
$$= \begin{bmatrix} H1K1 + H2K2 + N1 \\ -H1K2^* + H2K1^* + N2 \end{bmatrix} \quad (4)$$

1. **Combining operations**

The combiner constructs signals ($K3$, $K4$) by replacing Equation (4) using $R1$ with $R2$ into Equation (5), and then $K3$ and $K4$ can explain:

$$\begin{bmatrix} K3 \\ K4 \end{bmatrix} = \begin{bmatrix} H1^* * & H2 \\ H2^* & -H1 \end{bmatrix} * \begin{bmatrix} R1 \\ R2 \end{bmatrix}$$

$$= \begin{bmatrix} H1^* * R1 + H2 * R2 \\ H2^* * R1 - H1 * R2^* \end{bmatrix} \qquad (5)$$

Maximum likelihood detection operation

It is constantly assumed that the receiver has an ideal knowledge of the channel coefficients ($H1$, $H2$). Then, the decoder will use them as the channel state information (CSI). The maximum likelihood (ML) method chooses a pair of signals ($C1$, $C2$) from the signal constellation to minimize the difference between the receiver signals and these signals ($C1$, $C2$). The decision rule can be expressed by the distance metric over all possible values of $C1$ and $C2$.

$$d2(R1, H1C1+H2C2) + d2(R2, -H1C1^*+H2C2^*)$$

$$= |R1 - H1C1 - H2C2|^2 + |R2 - H1C2 - H2C1|^2 \quad (6)$$

Equation (4) can be divided into $K3$ and $K4$ using Equation (5):

$$\text{K3}= (|H1\text{^}2| + |H2\text{^}2|)K1 + H1^*N1 + H2N2^*$$

$$\text{K4}=|H1\text{^}2| + |H2\text{^}2|)K2 + H1N2^{**} + H2N1 \qquad (7)$$

Equation (6) can be divided by applying Equation (7) into two decoding rules for $C1$ and $C2$:

$$C1 = \arg\min\,(|H1| + |H2|\text{-}1)\; C1+d2\;(K3, C1) \qquad (8)$$
$$C2 = \arg\min\,(|H1|+|H2|\text{-}1)\; C2+d2\;(K4, C2)$$

3. Proposed method

The physical layer is applied to STBC to repair the errors that are generated by real transmittals. The sender and receiver can achieve ideal privacy, meaning that the understanding of the cryptograph *En* does not reduce the attacker's uncertainty about the input data, as $H(M|\ En) = H(M)$, where H means the entropy, and this case applies ideal secrecy, which is achievable if and only if: $H(K) \geq H(M)$ [13]. Hence, ideal privacy is achieved by a one-time-pad, if the key used in the cipher has a length equal to or larger than the number of input data. In this paper, a novel STBC method called stream cipher STBC, in which the stream cipher uses linear feedback shift register (LFSR) to generate a key in complex form. This method does not require any key from the employer for any operation, but each key is deduced from arithmetic attributes of the image using the average value (can use any other properties, such as the summation value). First, if the input data is binary, we can partition the data to packets that are 512 bits and enter the quadrature phase-shift keying (QPSK) modulation. The output from these steps is used in the STBC encoder to produce codewords as in Equation (1). Keys must be generated at the same time and used to multiply with codewords to increase confusion. The receiver receives the signal as:

Legitimate receiver: *Yn* = *En* + encryption sequence (*ES*) + noise channel (*Nc*)

The error case by the channel is called the noise channel. The legitimate receiver can create an encryptions sequence and calculate $En = Yn + ES$. The legitimate receiver thus returns the bits' reverse, which is generated by the noise channel. However, the attacker surveys the channel output as follows:

Attacker: *Zn* = *En* + *ES* + *Nc* ⟶I(*Zn*, *En*) = 0, mutual information between *Zn* and *En* equals zero.

The attacker is not able to obtain *En* by decoding *Zn*. The attacker has an error, which is generated by the attacker's canal, and he or she does not have any knowledge of the encryption sequence. Thus, lacking a best option, the attacker may first use redundancy in the encryption to decode *Zn* or suggest a key to create the encryption sequence and behave as a legitimate receiver. To stop an attacker from applying redundancy to obtain knowledge from *Zn*, in our method, we use keys (Key 1, Key 2) that are multiplied with codewords ($K1$, $K1^*$). This will remove any redundancy that can be used by the attacker. The total string of keys is very long and is difficult to enter by the user; therefore, in this method, a new key generator technique is used and will be explained below in detail. Figure 3 shows the main steps of the proposed method.

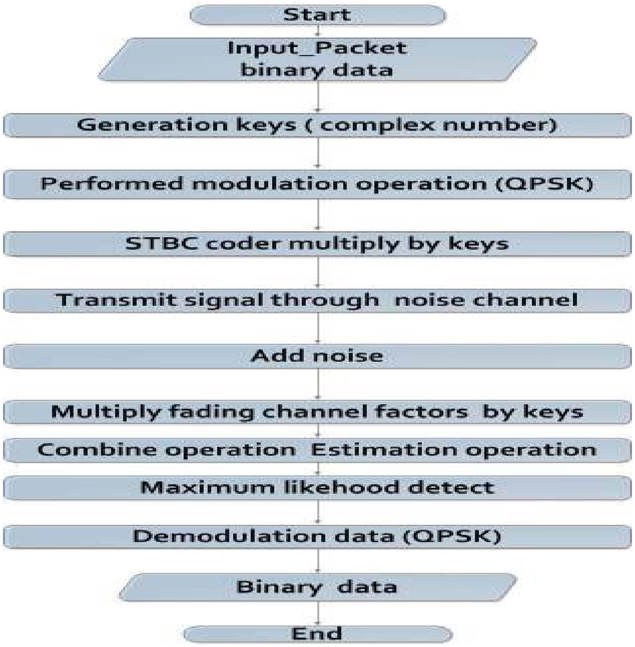

Start
Input_Packet binary data
Generation keys (complex number)
Performed modulation operation (QPSK)
STBC coder multiply by keys
Transmit signal through noise channel
Add noise
Multiply fading channel factors by keys
Combine operation Estimation operation
Maximum likehood detect
Demodulation data (QPSK)
Binary data
End

Figure 3. The proposed method steps (stream cipher STBC).

3.1. Complex Numbers

Complex numbers can be represented in three methods:

1. Rectangular form, (a + jb);
2. Polar form;
3. Exponential form, which utilizes the trigonometric functions of both the cos (cos) and sine (sin) values of a right-angled triangle to explain the complex exponential form as a rotating point in the complex plane. The exponential form for finding the location of a point is based on Euler's identity. Then, Euler's identity can be described by the following rotating phasor diagram in the complex plane, as shown in Figure 4. In this method, the exponential form is used to produce a key, as in Algorithm 2 [12].

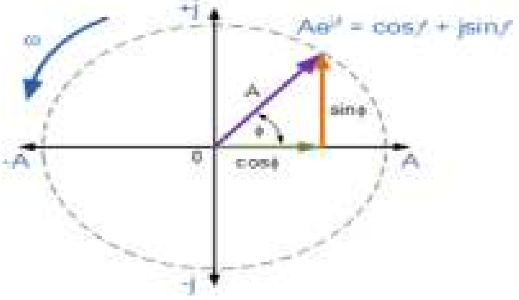


Figure 4. Diagram of complex number.

3.2. Key generation process

In the proposed method, multiple different keys are needed in the decryption and encryption. This method consists of two stages (in key generation). The first stage uses LFSR1, which has 31 bits and uses the polynomial (x^3+x^{31}) bits, and LFSR2, which has 19 bits and the polynomial (x^2+x^{19}), explain in Figure 5. We need to find the average value for every block (between [0, 1]). The average value is a fraction (four digits), the first two digits are used as a seed for LFSR1 and another two digits are used as a seed for LFSR2. Register 1 and Register 2 are used to produce the key, which has 2048 bits. The key (2048 bits) is stored as an array with (128x32) bits, and each row is converted to a decimal number, and each has 8 bits. Hence, this array becomes (128*4) in decimal form.

In the second stage, we must convert the key (decimal form) to a complex number due to the output from the modulation operation in complex number form; hence, the STBC encoder produces codewords in a complex form key, which can be produced using the following equations:

Complex number = R (cos (ɵ) + i*sin (ɵ)) (9)

ɵ = tan-1($\frac{y}{x}$) (10)

It is assumed $R = 1$ to reduce computation time. In Equation (10), x and y can be produced from the key array. The key is converted to (128, 2), and the first column represents x, while the second column represents y. Moreover, x and y are used in Equation (10) to produce ɵ, and ɵ is used to produce the key in complex number form in Equation (9). In this scheme, suppose that the packet (512 bit) is sent to the modulation (QPSK). This packet is divided into two blocks (256 bit) Block 1 represents $K1$, and Block 2 represents $K2$. Therefore, $K1$ is processed in the QPSK modulation process and produces (128x1) complex numbers. Regarding $K2$, afterwards, the key must be generated using Algorithm 2, multiplying the keys (Key 1, Key 2) with $K1$ and $K2$, respectively.

$K1$ * Key 1 (11)

$K2$ * Key 2 (12)

Conj ($K2$)*k = Key 1 (13)

Conj ($K1$) * Key 2 (14)

Output from Equation (11) and Equation (12) contains (128x2) complex number codewords and is sent through Antenna 1 and Antenna 2 during Time 1, and output from Equation (13) and Equation (14) is sent through Antenna 1 and Antenna 2, respectively. We suppose the receiver has one antenna. In Equation (11), $K1$ is multiplied by Key 1, and conj ($K1$) is multiplied by Key 2 in Equation (14). This step is very important to prevent attackers from using redundancy in data between the original data and the data image in conj (original data); this step makes cryptanalysis very difficult, as shown in Figure 6. Figure 7 shows the key generation algorithm steps.

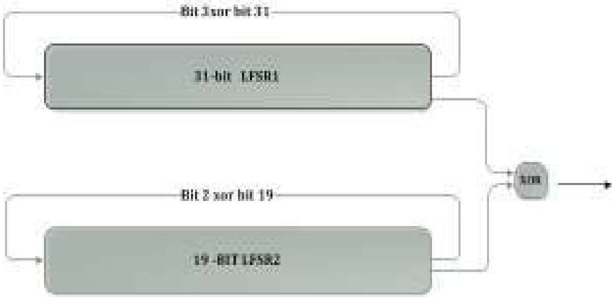


Figure 5. LFSR (Register 1, 31 bits, and Register 2, 19 bits).

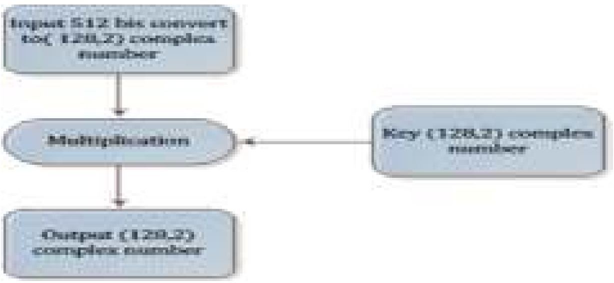

Input 512 bit convert to(128,2) complex number
Multiplication
Key (128,2) complex number
Output (128,2) complex number

Figure 6. Key multiplied with codewords.

3.3. Algorithm 1: Key generation

This section presents the key generation algorithm listed in Algorithm 1 below.

Algorithm 1: Key generation

1. Input average value.
2. Output Key 2 (complex form).

```
1.  Let $n\_frame$ = 2048  (128*2*8 $x, y$ 2 columns and 128 rows, each row has 8 bits)
2.  $x1$ = (average-trunc(average*10000), fraction part to real $x1$ consider seed
3.  $j = 1; j2 = 1; i = 1$; tap1 = [5, 31]; tap2 = [5, 19]
4.  $m1$ = size($x$,2); $m2$ = size($x2$,2); rnd= [ ]
5.  for $i = 1: n\_frame$
6.      $k = 0; b = 0; n = 0;$
7.      $b$ = xor (x(tap1(1)), $x$(tap1(2))) multiple tap 1, 2 only
8.      $n$ = xor ($x2$(tap2(1)), x2(tap2(2))) multiple tap 1, 2 only
9.      $k$ = xor ($x$(31), $x2$(19)), bit key
10.     for $j2 = m1$: -1:2      shift from 1 bit to 31 bits
11.         $x(j2) = x(j2-1)$;
12.     end
13.     for j2=m2:-1:2 shift from 1 to 19 bits
14.         $x2$(j2) = $x2(j2-1)$;
15.     end
16.     $x(1) = b$
17.     $x2(1) = n$
18.     rnd = $k$
19. end
20. Convert rnd from binary form to digital, each one has 8 bits called rnd2.
21. Change rnd2 to array, has 128 rows ($x, y$) let Key 2
22. $x1$ = Key 2(:,1); let column 1 represent $x$, Column 2 represent $y$, $y$ = Key 2(:,2)
23. $g1 = \tan^{-1}(y/x)$;
24. $K$ey 2=cos ($g1$) + $i$ sin ($g1$)
25. End
```

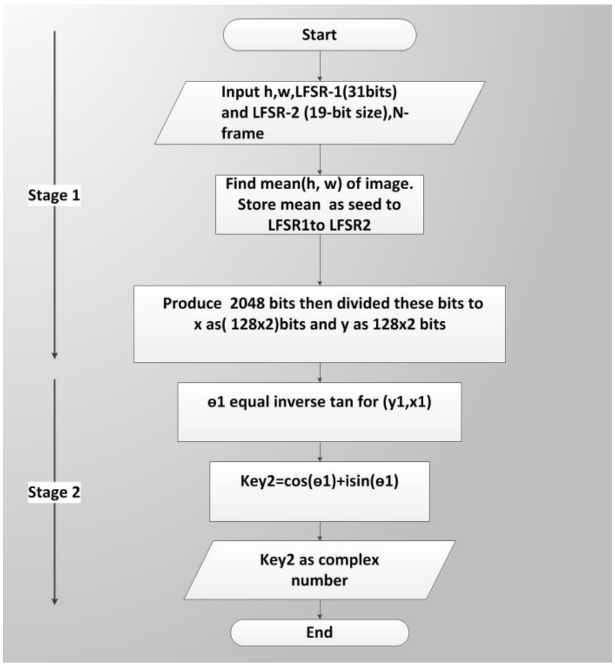

Start
Input h,w,LFSR-1(31bits) and LFSR-2 (19-bit size),N-frame
Find mean(h, w) of image. Store mean as seed to LFSR1to LFSR2
Produce 2048 bits then divided these bits to x as(128x2)bits and y as 128x2 bits
ɵ1 equal inverse tan for (y1,x1)
Key2=cos(ɵ1)+isin(ɵ1)
Key2 as complex number
End
Stage 1
Stage 2

Figure 7. Key generation algorithm steps.

3.4. Action of the legitimate receiver

The legitimate receiver knows the order stages, when the transmitter conveys the signals to the legitimate receiver. He will discover the signals at the next steps, Equation (16) to Equation (22). The following key generation in Algorithm 1, in which Key = [Key 1 Key 2] must be multiplied with the code matrix in Equation (1), creates a matrix in Equation (15).

$$\mathrm{K} = \begin{bmatrix} K1 * key1 & K2 * key2 \\ -K2^{*} * key1 & K1^{*} * key2 \end{bmatrix} \tag{15}$$

The legitimate receiver receives $R1$ and $R2$ denoting the two received signals over the two consecutive symbol periods for time t and $t + T$. The received signals can be expressed by:

$$\begin{bmatrix} R1 \\ R2 \end{bmatrix} = \begin{bmatrix} K1 & K2 \\ -K2^{*} & K1^{*} \end{bmatrix} * \begin{bmatrix} H1 * KEY1 \\ H2 * KEY2 \end{bmatrix} + \begin{bmatrix} N1 \\ N2 \end{bmatrix}$$
$$= \begin{bmatrix} H1K1 * KEY1 + H2K2 * KEY2 + N1 \\ -H1K2^{*} * KEY1 + H2K1^{*} * KEY2 + N2 \end{bmatrix} \tag{16}$$

1. Combining operation

The combiner creates the following signals that are conveyed to the ML detector changing $R1$ and $R2$ from Equation (16) into Equation (17), and then the rules can be formulated as follows:

$$\begin{bmatrix} K3 \\ K4 \end{bmatrix} = \begin{bmatrix} H1^{*} * KEY1 & H2 * KEY2 \\ H2^{*} * KEY2 & -H1 * KEY1 \end{bmatrix} \begin{bmatrix} R1 \\ R2 \end{bmatrix}$$
$$= \begin{bmatrix} KEY1 * H1^{*} * R1 + KEY2 * H2 * R2 \\ KEY2 * H2^{*} * R1 - KEY1 * H1 * R1^{*} \end{bmatrix} \tag{17}$$

2. Maximum likelihood detection operation

The ML decoder chooses a pair of signals ($C1$, $C2$) from the signal constellation to minimize the shift or error for phase-shift key (QPSK) signals. The decision rule can be expressed by the distance metric for all values of $C1$ and $C2$.

$$d2(R1, KEY1*H1*C1+KEY2*H2*C2)+d2(R2, KEY1*H1*C1^{*}+KEY2*H2*C2^{*})$$
$$=|R1 - KEY1 * H1 * C1 - KEY2 * H2 * C2)|^{2} + |R2 - KEY1 * H1 * C2 - KEY2 * H2 * C1|^{2} \tag{18}$$

Equation (16) can be divided into $K3$ and $K4$ using Equation (17):

$$K3 = (|KEY1 * H1^{2}|+|KEY2 * H2^{2}|)K1+KEY1*H1*N1+KEY2*H2N2^{*} \tag{19}$$
$$K4 =(|KEY1 * H1^{2}|+|KEY2 * H2^{2}|)\ K2+KEY1*H1\ N2^{*} +KEY2*H2^{*}\ N1$$

Equation (18) can be divided into rules for $C1$ and $C2$ using Equation (19):

$$C1= \arg\min\ ((|H1*KEY1|+|KEY2*H2|-1)\ C1+d2\ (K3, C1) \tag{20}$$

$$C2 = \arg\min\ (|H1*KEY1|+|KEY2*H2|-1)\ C2+d2\ (K4, C2))$$

An attacker can discover the signals via Equation (2) to Equation (8), but the legitimate receiver processes deal with Equation (16) to Equation (20).

4. Simulation results

In this method, we use the grayscale Lena image size (512, 512) to show the send and receive operations with MATLAB (2014) in simulation, which discusses the security in the physical layer and the image encryption as follows.

4.1. Performance features

In this section, the efficiency of the proposed communication system is simulated by calculating the bit error rate (BER) of the legitimate receiver and the attacker. In this method, we assume a block Rayleigh fading channel (i.e., fading coefficients are constant during the transfer of one packet with random conversions between packets). The BER performance of the Alamouti code scheme with two transfer antennas and one received antenna QPSK modulation is employed. First, the transmitter and receiver are assumed to know the perfect CSI. The simulation results in Figure 8 show that the attacker will receive the signal with almost full errors when the intended receiver can receive the signal with errors less than BER of 10-4.

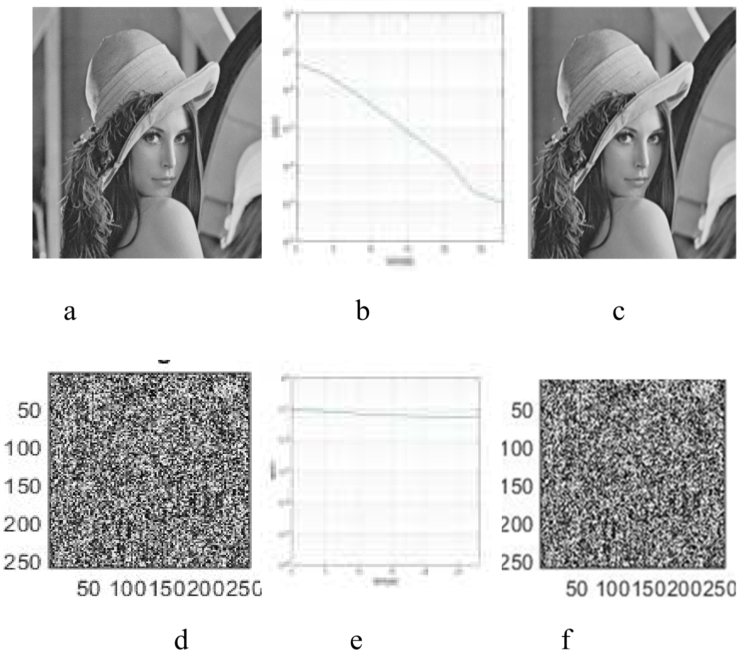


Figure 8. (a) The Lena image (512x512) before sending (d) the Lena image cipher (512x512) before sending (c) the Lena image (512x512)) after receiver and decryption with the true key (f) the Lena image (512x512) after receiver and decryption with the wrong key (b) BER performance of stream STBC for the Lena image in a legitimate receiver (use true key) with QPSK demodulation (e) BER performance of P-stream STBC for the Lena image on the attacker side (using the wrong key) with QPSK demodulation.

Subfigures (b) and (e) in Figure 8 show the plot of BER against the signal to noise ratio (SNR) for both the attacker and legitimate receiver in an additive white Gaussian noise (AWGN) channel and the modulation scheme is the QPSK. The plot shows how degraded the performance of the attacker's communication channel is opposed to that of the legitimate receiver. From the figure, the BER of the attacker stays almost constant, irrespective of the value of the SNR. However, in the case of the legitimate receiver, the BER reduces as the SNR increases. This proves that our scheme is secure, and it will be very difficult for attackers to recover messages because of the degradation of the channel.

4.2. Cryptanalysis – attacker

The security of the encryption sequence (*Es*) after STBC depends on the value of the noise channel (*Nc*) of the attacker. If the noise channel of the attacker is null, *Zn* = *En*, and this method assists the task of an attacker. Codes establish redundancy that can be used to create relations between parts of *Zn* and *En*, utilizing known-plaintext attacks against the encryptions sequence. For example, [14] presents a ciphertext-only attack against GSM. If the noise channel is not null, four types of attack are possible, as follows:

1. In ciphertext-only attacks, the attacker has several ciphertexts that were encrypted with an equivalent algorithm. The job of the cryptanalyst is to conclude as many plaintexts or keys as possible. The ciphertext-only attack is the weakest attack, and any cryptosystem that is weak under the ciphertext-only attack is useless. In our method, these attacks do not produce codewords. These produce direct plaintext, which is not the same as codewords. Hence, our method is very strong against ciphertext-only attacks. These means $I(M; Zn) = 0$; hence, *M* and *Zn* are independent. In other words, mutual information between *M* and *Zn* is zero.

2. In known-plaintext attacks, the cryptanalyst has access to the plaintext from which the ciphertext was generated and to the ciphertext. The attacker tries to conclude the key used to encrypt the plaintext or the algorithm that may be used for the decryption of consequent ciphertexts with the aid of the same key. In our method, these attacks do not produce codewords, instead producing direct ciphertext, which is not the same as codewords. Hence, our method is very strong against ciphertext-only attacks. This means $I(M; Zn) = 0$; hence, *M* and *Zn* are independent.

3. The chosen-plaintext attack is like the known-plaintext attack except that the attacker can choose precise plaintext with the desire that they will unveil more information about the keys. In our method, these attacks do not produce codewords. They produce direct ciphertext, which is not the same as codewords. Hence, our method is very strong against ciphertext-only attacks. This means $I(M; Zn) = 0$; hence, *M* and *Zn* are independent.

4. For Burt-force attackers, recovering *m* involves extracting the encryption sequence (*Es*) or breaking the secret key from the channel output *Zn* as in Figure 1. Due to the noisy channel (*Nc*), the attacker is not capable of splitting the encryption sequence from the noisy channel, unless he or she finds the key. In the other words, without knowing the key, the attacker has no way to determine whether data of *En* was changed by the encryption sequence or by the noisy channel. The attacker can find the key (and thus the encryption sequence), by carrying out an exhaustive search, in which the attacker takes a candidate key and produces the encryption sequence, and the attacker adds the encryptions sequence to *Zn* to obtain *Wn*. If the key is not equal to the original key, then $Wn = Zn + Es = En + Es + Es + Nc$, which means that attacker is unable to eliminate the encryption sequence from *Zn,* and if the key is the original key, then $Wn = Zn + Es = En + Nc$, but in our method, a key is used as a complex form. Therefore, suggesting a key in a complex form is very difficult to impossible. The attacker is incapable of removing the encryption sequence from *Zn*. Hence, it is believed that our method is strong against all types of attacks if the noise channel is not null.

4.3.1 Histogram with power spectral density

The image histogram explains the number of pixels in a picture at various intensity values. Additionally, the two-dimensional (2D) spectrum explains the strength of the image intensity that can be obtained by a discrete Fourier transform (DFT) examination. Figure 9 explains the histograms and 2D power spectrums of the primary images. The initial image is the Lena image with 512x512. The intensity of every original image in the histogram is presented with various values in a specific shape, but when an image is encrypted by stream STBC, it produces an image that has a flat histogram and power spectrum; hence, the cipher images are diffused and invisible. The decoded image with the correct keys provides an image equivalent to the primary image. The image is secured. The power spectrum can be defined as follows in Equation (21):

$F=\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} f(x,y)\exp(-j(\pi/m)$ ux exp(-j(2π/n)vy) (21)

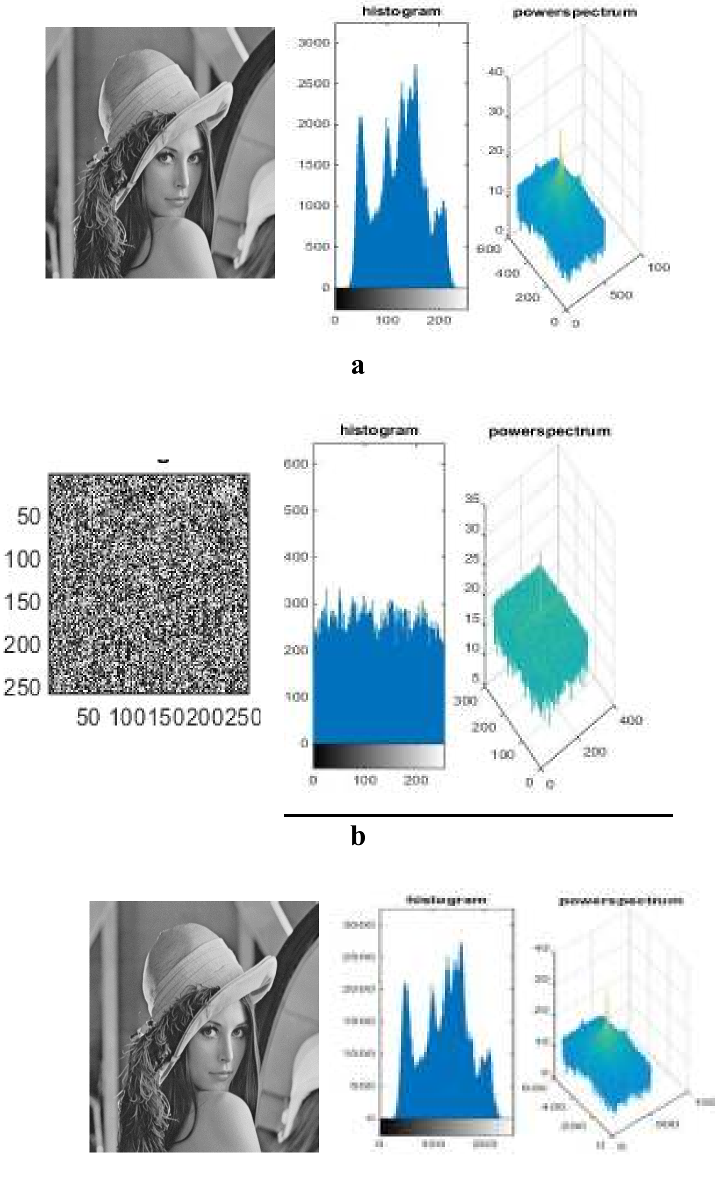


Figure 9. (a) Histogram and power spectrum of plain images (Lena), (b) histogram and power spectrum of cipher images (Lena), (c) histogram and power spectrum of image after decryption with true key.

4.3.2. Correlation-coefficient analysis

Correlation-coefficient analysis is a measure of the bonds between two pixel intensities of two images, if the images were analyzed horizontally, vertically, and diagonally adjacent pixels. The covariance *Cu* and the correlation coefficient *Icy*, and the variables *x* and *y* are grayscale values of pixels in equivalent pixels in different images or two adjacent pixels in the same image. The value of *Icy* is in the region [1, -1]. In other words, the values of *Icy* in the region (-1, 0) and (0, 1) correspondingly show positive and negative relationships, while the larger number close to 1 or -1 has stronger bonds. Table 1 explains the image correlation examined in the original and encrypted images, and the correlation coefficient is computed as follows:

$$\text{Cu}=1/\text{n} \sum_{i=0}^{n}(xi - E(x))(yi - E(y))$$

$$\text{Icy}=\frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (22)$$

The functions $E(x)$ and $E(y)$ are expressed as:

$$\text{E(x)}=\frac{1}{n}\sum_{i=1}^{n} xi \text{ and } D(x) = \frac{1}{n}\sum_{i=1}^{n}(xi - E(x))\text{\textasciicircum}2$$

4.3.3. Differential analysis

An important change is caused in the cipher image, regarding the diffusion and confusion, and then the differential attack loses its efficiency and becomes almost useless. There are two familiar scales used for differential analysis: the NPCR and UACI. The NPCR means the "number of pixels change rate" of the encrypted image, while UACI is the "unified average changing intensity scales," which is the average intensity of the differences between the basic and encrypted image. Let $h2$ and $h3$ have corresponding plain images, which have only one pixel difference. Table 1 shows NPCR and UACI for the Lena image, and the NPCR of two images is defined as:

$$\text{NPCR} = \left(\frac{\sum I,JM(i,j)}{W*H}\right) * 100 \quad (23)$$

where W and H represent width and height of image. Moreover, UACI is defined as:

$$\text{UACI}=\frac{1}{W1*H1}\sum ij\left(\frac{h2(I,J)-h3(I,J)}{255}\right) * 100 \quad (24)$$

4.4.4. Image entropy

Image entropy denotes the degree of randomness or uncertainty in the image. Entropy (m) is defined as:

$$\text{Entropy } (m) = \sum \text{p (mi) log}\frac{1}{p(mi)} \quad (25)$$

Table 1: Different and correlation coefficients (vertical, horizontal, diagonal) and entropy for image.

	Lena Image Encryption		
PCNR	98.0606		
UACI	33.17		
Entropy	7.9916		
Correlation coefficient of cipher image	Vertical	Horizontal	Diagonal
	0.0153	0.0966	0.0058
Correlation coefficient of plain image	0.9258	0.95993	0.9037
Correlation between cipher image and plain image	0.0498		

5. Conclusions

Stream cipher STBC generates encryption following the STBC code. We run secretly through the physical layer, and these methods avoid eavesdroppers from obtaining beneficial data since the decryption of an encoding is infeasible without this knowledge about the master key, which is used with authorized partners. Hence, we will prevent eavesdroppers from attaining useful data. In a fading channel, this prime key is needed to split change due to the channel noise and encryption. This prime key is needed by attackers to acquire the proper redundancy from the obtained information. Without realizing the prime key, the attacker regards the channel as a very noisy or as an unacceptable channel with noise and errors. We decrease the attacker's ability to analyze the cipher and makes the attack very difficult. In this method, a new method is used to generate a key in the complex form using LFSR. Mathematical properties of data as an image can be used as a seed to generate keys without the need for any keys from the users. Hence, the encryption after STBC or the physical layer encryption makes the cipher analysis more difficult. Our method is very strong against all types of attacks, if the channel noise is not null. Our method is simple and efficient, improves speed, and saves hardware usage.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, Space-time codes for high data rate wireless communication: performance criterion and code construction, *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744–765, 1998.

[2] G. J. Foschini and M. J. Gans, On limits of wireless communications in a fading environment when using multiple antennas, *Wireless Personal Communications*, vol. 6, no. 3, pp. 311–335, 1998.

[3] S. M. Alamouti, A simple transmit diversity technique for wireless communications, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[4] G. J. Foschini, Layered space-time architecture for wireless communication in a fading environment when using multielement

antennas, *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 1–59, 1996.

[5] J. Guey, M. P. Fitz, M. R. Bell, and W. Kuo, Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels, In *Proceedings of the IEEE 46th Vehicular Technology Conference*, pp. 136–140, May 1996.

[6] N. Dao and C. Tellambura, Semiorthogonal space-time block codes, *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 168–180, 2010.

[7] V. Tarokh, H. Jafarkhani, and A. R. Calderban, Space-time block codes from orthogonal designs, *IEEE Transactions on Information Theory*, vol. 45, No. 5, pp. 1456–1467, 1999.

[8] C. H. Bennett, G. Brassard, C. Crpeau, and U. Maurer, Generalized privacy amplification, *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[9] H. Wen, G. Gong and P. Han Ho, MIMO Cross-Layer Secure Communication Architecture Based on STBC, IEEE Communications Society *Globecom 2010*.

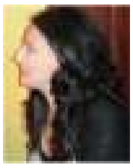
[10] A. Z´uquete, J. Barros, Physical-Layer Encryption with Stream Ciphers, Toronto, Canada, July 6–11, 2008.

[11] J. Yang, E. Masood, and Y. Sun, Performance of Space-time Block Coding Using Estimated Channel parameters, *London Communications Symposium Conference UCL*, 2004.

[12] Lecture-Notes: Complex Numbers https://www.math.wisc.edu/~angenent/Free-Lecture-Notes/freecomplexnumbers.pdf

[13] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[14] E. Barkan, E. Biham, and N. Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, in *Proceedings of the 23rd Annual International Cryptology Conference*, CA, USA, Aug. 2003



Asst. Prof. Dr. Hanaa Mohsin Ahmed

Dr. Hanaa M. A. Salman obtained her MSc and PhD from the University of Technology Iraq in 2002 and 2006, respectively. Currently, she is a lecturer in computer science and a member of the Scientific Committee and Promotion Committee in the Department of Computer Science. Dr. Hanaa has more than 23 years of experience, and she has supervised graduate students and preliminary. Her research interests include cryptography, computer security, biometrics, image processing, and computer graphics.

Anwar Abbas Hattab

Anwar Abbas Hattab is currently a PhD student in the Computer Science Department at the University of Technology, Iraq, Baghdad. Her BSc in Computer Science is from Baghdad University and her MSc degree in Network Management in 2003 is from the Iraq Commission for Computer and Informatics, Institute for Post Graduate Studies in Informatics. Currently, her research in physical layer security for mobile networks is based on information theory, and she is a lecturer in computer science. Anwar has more than 13 years of experience and has supervised BSc final year projects. Her research interests include cryptography, image processing, data security, network security, and databases.