Formal Language Space Time Block Code for Mobile Network

Hanaa Mohsin Ahmed and Anwar Abbas Hattab

Computer Science Department - University of Technology

Received 22 September 2016 ; Accepted 15 January 2017

Abstract

Formal Language for Space Time Block Code (FL-STBC) is proposed to protect data in physical layer for mobile network and it can replace network code (NC) within STBC coding in which each pixel will change its location as 2D standard map and change the value of pixel by using set of keys (key, rx,ry) and two index or keys (h1 and h2). Key, rx and ry are generated based on Number Theory which is different and unduplicated. This method can generate keys in infinite keys, fast and simple manner. h1 and h2 which are generated according to color of each pixel. In (FL-STBC) new method 4-dimensions standard chaotic map is proposed to make diffusion and confusion on data. Test results show the strong of the proposed method. It makes randomness in transfer's data as Network Code and it operates in all cases if attacker channel is noiseless. Results of security measures for physical layer security, measures of image cipher (used as media through sending and receiving) and measure of randomness keys ensure an efficient and strong of method (FL-STBC).

Keyword: Physical layer security, Formal Language, 2D standard chaotic map, one-time pad, Multiple-input multiple-output(MIMO), 4D standard chaotic map.

لغه رسميه لترميز مجموعة الوقت والمكان لشبكه الوبايل

هناء محسن احمد و انوار عباس حطاب

قسم علوم الحاسبات - الجامعة التكنولوجية

الخلاصة

افترضت طريقة اللغة الرسمية لترميز الحزمة المساحة والوقت (FL STBC) لحماية البيانات في الطبقة المادية لشبكة المحمول ويمكن ان تحل محل ترميز الشبكة (NC) ضمن ترميز STBC . حيث كل بكسل سوف تتغير كطريقة التحويل القياسية للفوضى ثنائيه الابعاد وتغير قيمه البكسل بأستخدام مجموعه مفاتيح key ,rx ry . المفاتيح key ,rx ry تتولد اعتمادا على نظرية الاعداد . وهذه المفاتيح تكون مختلفه وغير مكررة (هذه الطريقه تولد مفاتيح غير منتهية وسريعة وبأسلوب

بسيط) . والمفاتيح h1, h2 تتولد وفقاً للون البكسل . في طريقة اللغة الرسمية لترميز الحزمة المساحة والوقت (FL STBC) افترضت طريقه التحويل القياسية للفوضى رباعية الابعاد لعمل التشويش والانتشار في البيانات . واظهرت نتائج الاختبارات قوة الطريقة المفترحة والتي عملت عشوائية في البيانات المنقوله كترميز الشبكة (NC) وتعمل في كل الحالات واذا كانت قناة العدو اقل ضوضاء. النتائج من مقايس الامنية في الطبقة المادية ، ومقايس تشفير الصور (استخدمت الصور كبيانات لتوضيح عملية الارسال والاستقبال) ومقايس عشوائية المفاتيح تؤكد كفاءة وقوة طريقة FL STBC.

الكلمات المفتاحية : امنية الطبقة الفيزيائية، اللغة الرسمية، طريقة التحويل القياسية للفوضى (2 ابعاد) ، وسادة لمرة واحدة، تعدد الهوائيات الادخال والاخرااج STBC MIMO ، طريقة التحويل القياسية للفوضى (4 ابعاد).

Introduction

The broadcast nature of wireless communications makes its physical layer vulnerable to eavesdropping attacks. The eavesdropping attack refers to an unauthorized user attempting to intercept the data transmission between legitimate users [1-3]. Therefore, physical-layer security (PLS) is emerged as a promising paradigm designed for improving the security of wireless transmissions [4].One of the methods in fourth generation (4G) is Multiple-input multiple-output (MIMO) methods, as a result of their ability to enhance the system's reliability. MIMO antenna is executed to achieve a higher ratio of information and improve the spectral competence. Space time code (STC) known as multi antenna coding is class of MIMO [5]. A number of schemes employing multiple antenna arrays with STC were advanced in. Space time trellis code (STTC) and space time block code (STBC) are the two types of STC channel code, STBC as lower complexity than STTC [6]. Mobile networks lack physical outlines and infraction comes from the outer without the request of a real telecommunication. The lack of boundaries in these methods makes them weak in PLS. The defense becomes a major attention in the physical-layer. PLS –information theory works by limiting the amount of information that can be extracted at the physical level by an attacker. This is performed by designing appropriate coding and precoding schemes (network coding), and by exploiting the channel state information (CSI which can be defined as a set of information which describes channel) available at the network nodes [7] .There are many real systems that cannot benefit from PLS-information theory for example system without feedback , if an eavesdropper has a better channel than legitimate receivers , PLS methods will either offer no protection or limited

protection depending on how much information the transmitting party knows about systems[8,9]. Therefore, this paper suggest a new method to protect data in physical layer (MIMO_STBC) called formal language_STBC (FL-STBC) in which not need any keys from user all keys deduce from data-transfer in which a method is used to generate one _time pad keys and a new 4-dimenasions standard map is suggested to represent data to another present on numeral curve, this produces confusion and diffusion on data transfer and produces randomness in data transfer as network coding. Hence, FL_STBC can be suggested as a new method to secure data in physical layer working at all times, even if the enemy channel has less noise, randomness operates in the data transmitted can replace the network code.

The rest of this paper is arranged as follows: Section 2 explains related works, section 3 explains randomness examination, section4 explain standard map, section 5 described chaotic cryptography, section 6 described proposed methods, and section 7 explain proposed key generation and section 8 described performance analysis. This paper is concluded present in Section 9.

Related Works

Many of researches consider as a related works of this paper as: [10] proposed a cryptosystem which is based on the set of theory as a mean to represent any alphabetic character (English language) and the set of prime residue classes of any integer number N. The prime residue classes represent the language alphabetic character (plaintext). [11] proposed fingerprint random number generator (FPRNG) which produces non repeated random number. The location of minute points on the fingerprint image is used as a seed for RNG were carried out by using residue classes and the complete system of these residue classes module n. [12] utilize the properties of chaotic signals to implement secure communication. It consists of a chaos signal generator (use Henan map), a delayed unit, a multiplier and an addition. The chaos signal is delayed and multiplied by information bits. Then the original chaos signal and multiplier output is added and it is transmitted. Then this signal is passed through the threshold and then it is decoded to recover the information signal and improve BER. [13] provides CodeHop scheme for physical layer error correction and security. It employs nonsystematic Low Density

Parity Check (LDPC) codes to combine channel coding and data encryption in a single step. [14] this paper suggests a method to transmit color image (after convert to grayscale) through STBC(2X1) channel and measure the quality of received image and suggest applying RSA(Ron Rivest, Shamir, and Adleman) algorithm on each pixel and decrypt them in legitimate receiver.

Randomness Examination

The randomness quality of the output sequences is examined by using statistical tests of NIST (National Institute of Standards and Technology of the U.S. Government). The NIST statistical test suite is a package initially developed for randomness evaluation of AES (Advanced Encryption Standard) after DES (Data Encryption Standard's) cracking [15]. Such suite is a statistical package of 15 tests advanced to quantify and to examine the randomness of binary sequences generated by cryptographic pseudo random number generators. A set of p-value is calculated for each statistical test, and it is compared to a constant significance level α= 0.01where only 1% of the sequences are prospective to fail. A p-value of zero demonstrates that, the tested sequence has all the earmarks of being not irregular (not random). At the point when a p-value is greater than α, it shows that the tested sequence is an arbitrary (random) sequence with 99% of a certainty (confidence) level [16].

Standard Chaotic Map

Chaotic maps have attributes are as primer value sensitivity, parameter sensitivity, state ergodicity, mixing and like randomness, therefore, these maps are beneficial in data encryption [17]. Many of chaotic equations used to encryption, for example standard map (2-D) was introduced in [18]:

$$Xi+1= (xi+rx+yi+ry) \bmod M$$

$$Yi+1= (yi+ry+Ksinxi+1M2\pi) \bmod M \quad (1)$$

We were rx, ry, key are keys.

Chaotic Cryptography

The chaotic cryptography methods are usually made by integration of two processes called permutation also called shuffling and diffusion if both processes repeatedly border till the appropriate encryption plane is achieved[18, 19].

Proposed Method

It is suggested jointing formal language with STBC (2X1) (two antennas for sending and one antenna for receiving data) and Quadrature Phase Shift Keying modulation(QPSK) to make data in physical layer more secure and protect data from attacker. As show in figure (1), method steps are explained in flowcharts in figure (3) and figure (4).

Fig (1) Formal-language-STBC

In our method, Formal language_STBC(FL-STBC) is suggested formal language is used to represent data as color image to anther representation on curve number by using color array and standard chaotic map 2D to produce new 4-D standard map. Firstly, color array must explain as follow:

a. Color Array: is array of (16, 16) used to represent each color in gray image. As show in Table (1), each color is represented by using two classes (class1, class2) used as index to color in array color. This array is used to represent each color to anther color by using standard chaotic map by using eq. (2,3 and 4) as follows:

Base=15+1.

Color=class1+class2*base (2)

Class1=mod (color, base) (3)

Class2=trunk (color/ base) (4)

Example (2): If color =20, it can be represented by using color array as:

Color=20

Class1: mod (20, 16) =4

Class2: trunc (20/16) =1

b. Input Data: To demonstrate the process of sending and receiving data after you apply LF_STBC, the power of the way is illustrated through the watching changes to the data transmitted therefore colorful images have been used through the process transmitter and receiver, images contain three channels (red, green, blue) here in the physical layer working with bit stream thus conveys the image pixel by pixel, as described in the algorithm (1)

Table (1) Color array

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	5
0	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
1	1	17	33	49	65	81	97	113	129	145	161	177	193	209	225	241
2	2	18	34	50	66	82	98	114	130	146	162	178	194	210	226	242
3	3	19	35	51	67	83	99	115	131	147	163	179	195	211	227	243
4	4	20	36	52	68	84	100	116	132	148	164	180	196	212	228	244
5	5	21	37	53	69	85	101	117	133	149	165	181	197	213	229	245
6	6	22	38	54	70	86	102	118	134	150	166	182	198	214	230	246
7	7	23	39	55	71	87	103	119	135	151	167	183	199	215	231	247
8	8	24	40	56	72	88	104	120	136	152	168	184	200	216	232	248
9	9	25	41	57	73	89	105	121	137	153	169	185	201	217	233	249
10	10	26	42	58	74	90	106	122	138	154	170	186	202	218	234	250
11	11	27	43	59	75	91	107	123	139	155	171	187	203	219	235	251
12	12	28	44	60	76	92	108	124	140	156	172	188	204	220	236	252
13	13	29	45	61	77	93	109	125	141	157	173	189	205	221	237	253
14	14	30	46	62	78	94	110	126	142	158	174	190	206	222	238	254
15	15	31	47	63	79	95	111	127	143	159	175	191	207	223	239	255

Algorithm read color-image (1):
Input: Img (I, j, k), image three dimensions.
Output: Blok, image one domination. (Send red, green, and blue for each pixel).
Step 1:FOR j=1: w
Step 2: Assign ii to 1
Step3: FOR i=1: h
Step4: FOR k=1:3
Assign block to img (i, j, k)
Assign blok (ii, j) to block., Assign ii to ii+1.
Step5: ENDFOR
Step6: ENDFOR
Step7: ENDFOR
Step8: END.

Chaotic equations 2D are used to make permutation solely for data and 4-D standard map which is for permutation data and change pixel value which makes substitution or confusion as shown in algorithms (2) and (3); and we used method to generate keys without need any key from user as show in algorithm (4) to make one time-pad cipher , a set of keys generated from data transfer in fast manner is show below, to make H(M/K)=H(M) and H(K)≥ H(M). In gray scale image each pixel take 8-bit and in color image have three channels (red, green, blue) each pixel in any color channel has 8-bits. 8-bits represent numbers from (0-255) when color array is used each color used it can be represented by class1 and class2 and base=16 as follows:
Example (3): Let A be sub image (color image) as in table (2), by using color array and equations (5, 6). Two arrays of keys can be generated which are used after that.

Table (2) a sub image

222	220	223	222	228	226
225	222	225	224	228	227
222	222	221	224	226	224
224	223	225	226	227	227
226	226	225	228	225	223
225	226	225	226	228	226

When eq (5) is applied to A (sub image), class1 called key1-array is generate as shown in table (3). When eq (6) is applied to A sub image, class2 called key2-array is generated as shown in table (4).

Table (4) Key2-array

13	13	13	13	14	14
14	13	14	14	14	14
13	13	13	14	14	14
14	13	14	14	14	14
14	14	14	14	14	13
14	14	14	14	14	14

Table (3) Keys1-array

14	12	15	14	4	2
1	14	1	0	4	3
14	14	13	0	2	0
0	15	1	2	3	3
2	2	1	4	1	15
1	2	1	2	4	2

Standard map (2 dimensions) is used as a first step to distribute data and scatter by a specific amount to the x-axis and y d Y by using keys generate from key generated algorithm (3), these generate new location (new-x, new-y) amounts which are used as keys to change the value of the pixel after changing location of pixel as show in equations (5) and (6):

New-class1=key1 (class1) +new-x (5)

New-class2=key2 (classs2) +new-y (6)

Finally, using eq (7) produces new color as:

New-color=New-class1+New-class2*base (7)

The new color (as in eq (7)) in the new location of the output is equivalent to new 4-D standard map here it changes locations and changes the color of the image with new keys generated from data transfer with simple manner and produces new representation of data on number line with confusion and diffusion as show in figure (2) and color store in new location as in eq (8).

Pixel (new-x, new-y) = New-color (8)

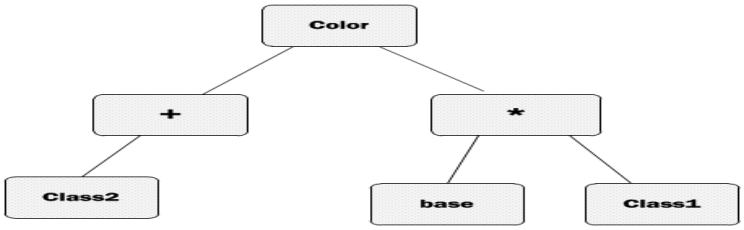

Fig (2) Colors representation

Algorithm (2): Formal Language - _STBC

Input: Img(packet (binary)),h, w, base,key,rx,ry(h_high,w_width,base=16)
Output: packet (binary).
Step1: Convert img from binary to 8_bit for each pixel.
Step2: Convert img to h, w (2_dimensions).
Step3: Assign h11to img mod base. Assign h22 to trunc (img / base).
Step4: FOR row=0:h-1
Step5: FOR col=0:w-1
x=row, y=col.
Assign h1to h11 (row+1, col+1. Assign h2 to h22 (row+1, col+1).
Assign new_x to mod(x+rx+ry+y, h);
Assign k to sin (((new_x+rx)*w)/ (2*(22/7))).
Assign new_y to mod (round(y+ry+ (key*k)), w).
Assign x2 to mod ((new_x+1)*(x+1), base).
Assign y2 to mod ((new_y+1)*(y+1), base). To remove iteration from process mod
Assign new_h1 to mod (h1+x2, base).
Assign new_h2 to mod (h2+y2, base).
Assign new_color1 to new_h1+base*new_h2.
Assign new_img (new_x+1, new_y+1) to new_color1.
Step6: ENDFOR
Step7: ENDFOR
Step8: Convert new-img to one row. Convert new_img to binary
Step9: Assign packet to new_img.
Step10: End

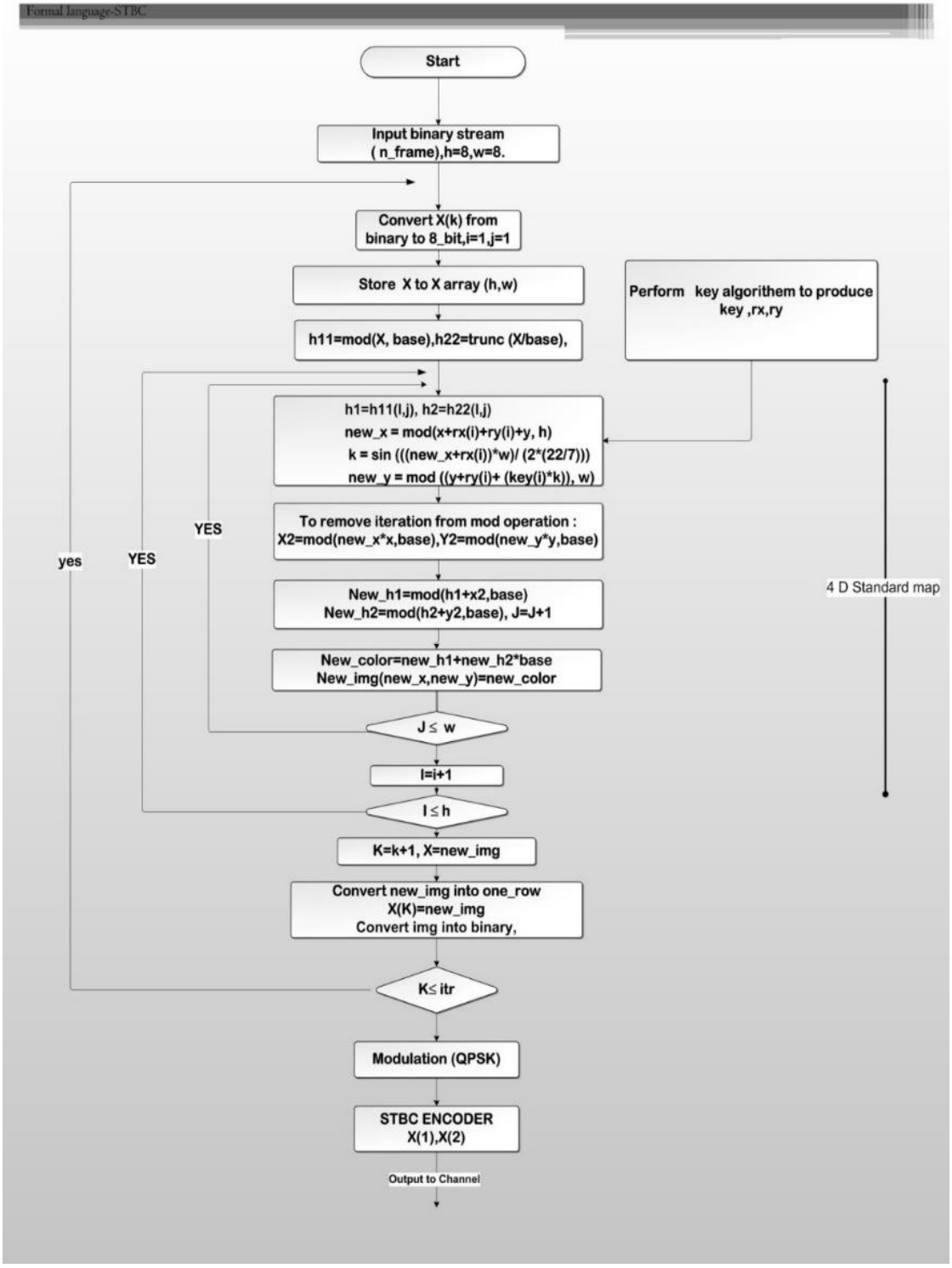

Fig (3) Flowchart of Formal language-STBC steps at sender side

Algorithm (3): Inverse-Formal Language

Input: Img, packet (binary), h, w, base, key, rx, ry.

Output: packet (binary).

Step1: Convert img from binary to 8_bit for each pixel.

Step2: Convert img to h,w (2_dimenations).

Step3: Assign h11 to mod (img, base).Assign h22 to trunc (img /base).

Step4: FOR row=0:h-1

Step5: FOR col=0:w-1

new_x=row;new_y=col;

k2=sin (((new_x+rx)*w)/ (2*22/7))

y=mod (round (new_y-ry-key*K2), w)

x=mod ((new_x-rx-ry-y), h).

new_h1=h11 (new_x+1, new_y+1). new_h2=h22 (new_x+1,new_y+1).

X2=mod ((new_x+1)*(x+1), base); y2=mod ((new_y+1)*(y+1), base).

h1=mod (new_h1-x2, base); h2=mod (new_h2-y2, base).

old_color1=h1+base*h2.

New_img(x+1,y+1)=old_color1

Step6: ENDFOR

Step7: ENDFOR

Step8: Convert new-img to one row. Convert new_img to binary

Step9: Assign packet to new_img.

Step10: END

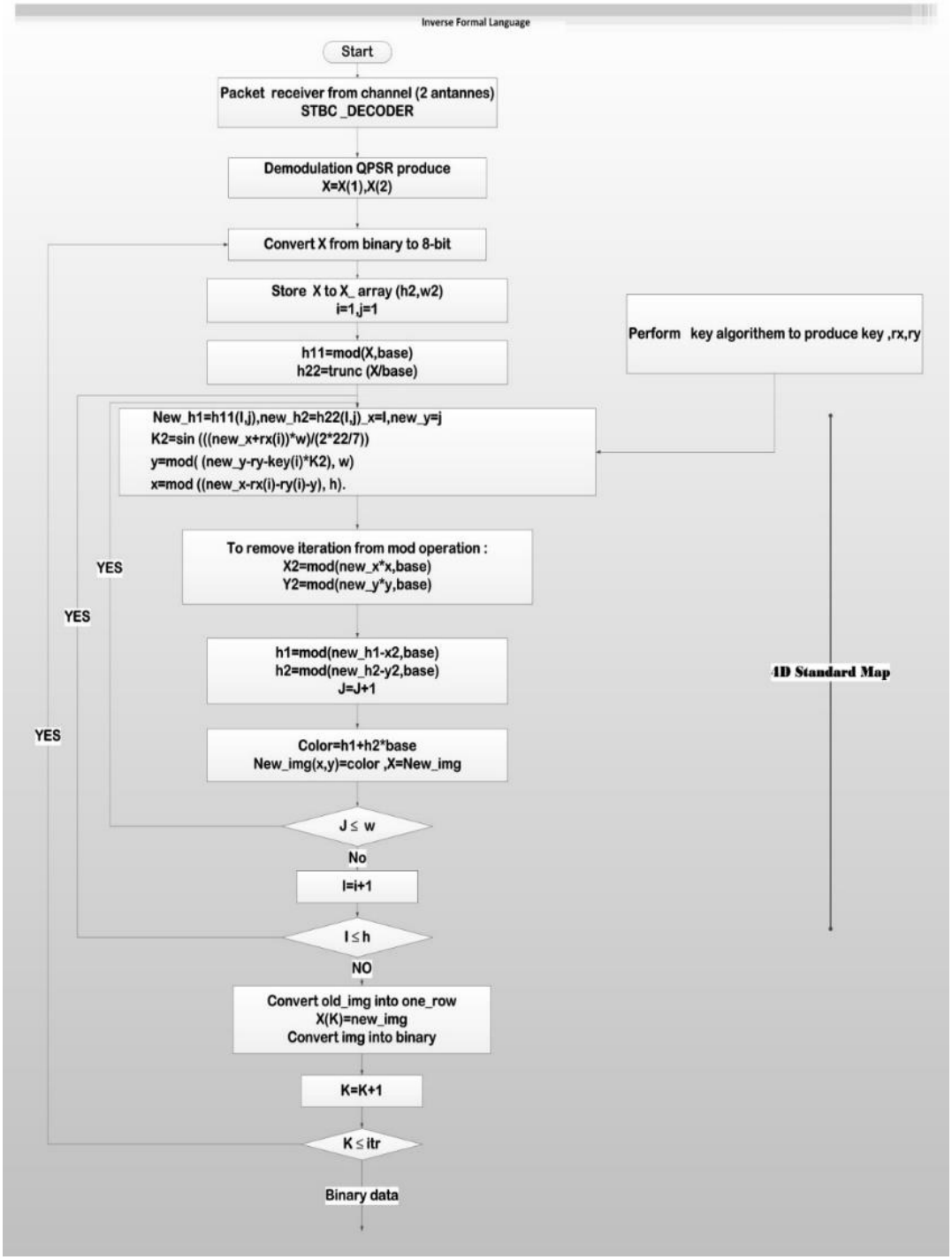

Fig (4) Flowchart of inverse-formal language-STBC steps at receiver side

Proposed Key Generation

New method has been suggested to generate keys random, non-repeated and unfinished based on number theory. It makes one-time pad. Algorithm (4) shown key generate steps in which Start value is prime and must determine firstly as 2. Eq (15) which is used to make special start for each packet and it should be prime class as:

Start =start+5(i_packet-1) (15)

Where start =2 and i_packet represent consequence of packets. Start is used as a seed to random function to generate random numbers which are denoted for location value which is used in eq (16):

Key=start + location (i)*based (16)

Algorithm (4): Key_Formal language

Input: Start, h, w, packet, itr, k=true, Start as constant ,h(high),w(width),itr(round)

Output: Key, rx, ry.

Step1: Assign base to h*w. Assign Start to Start+5*(packet -1)

Step2: IF Start > base

Assign Start to1

END

Step3: WHILE (k== true)

Check if start prime number Assign p=true

IF p== true

Assign k to false.

ELSE assign Star to Start+1.

END

Step4: ENDWHILE

Step5: Generate different random numbers x=randperm(10000,itr*3)

Step6: Convert x to x2(itr,3)

Step7: FOR i=1 : itr

Assign key (i) to Start+ x2(i,1)*base

Assign rx(i) to Start+ x2(i,2)*base

Assign ry(i) to Start+ x2(i,3)*base

Step8: ENDFOR

Step9: END

Keys,rx and ry are generate based on Algorithm (4) Where h and w represent height and width of image and base value equal (h*w-1) that which produce classes as show:

[0]

[1]

[2]= [(key_1, rx_1, ry_1), (key_2, rx_2, ry_2), (key_3, rx_3, ry_3), (key_4, rx_4, ry_4),…….]

[3]

[4]

[5]

[6]

[7]= [(key_1, rx_1, ry_1), (key_2, rx_2, ry_2), (key_3, rx_3, ry_3), (key_4, rx_4, ry_4),…….]

-
-

[12]=[(key_1 , rx_1, ry_1), (key_2 , rx_2, ry_2), (key_3 , rx_3, ry_3), (key_4 , rx_4, ry_4),…….]

-
-

[h*w-1]

If start point equal 2, according to eq (15), class [2] will be used to generate all keys to packet 1, if(i_packet=2) refer to second packet according to eq (15) class[7] is used to generate all keys to packet 2 . The work continues on the steps algorithm for the rest of the packets. The total number of classes continue to a number equal to (h*w-1) as shown above.

Performance Analysis

Three sets of tests must be used, first test set is used to measure security in physical layer (Bit error rate (BER) and Signal noise rate (SNR)), second test set is used to measure image cipher, finally, set use to measure randomness of keys as follows:

a. Physical layer security: In this paper, fading channel is assumed; fading coefficients are assumed constant during convey of one packet but randomly transformation between packets. In FL_STBC scheme suppose three antennas used, two for sender and one antenna for receiver with Quadrature Phase Shift Keying modulation (QPSK), bit error ratio (BER) used to measure security in physical because it presents a number of bits errors with signal noise ratio (SNR) as shown on in figure (5) the attacker receives signals with full errors but legitimate receiver side the signal's errors can experience bit error ratio less than $10^{-4.}$ This shows that our scheme is secure.

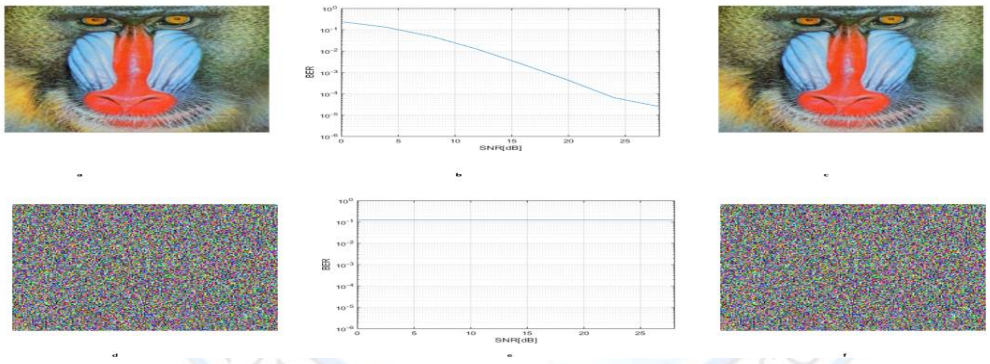

Fig (5) (a) Baboon_image (200x200) before sending (d) Baboon_ image_ cipher (200x200) before sending (c) Baboon's_ image (200x200) after receiver and decryption in legitimate receiver (f) Baboon's_image (200x200) after receiver and decryption in attacker (b) BER performance of formal language-STBC for baboon's_image in a legitimate receiver (e) BER performance of FL)STBC on attacker side

b. Image Cipher Tests: 1. Histogram with Power Spectral Density

Histogram describes how pixels in an image are distributed by plotting the number of pixels. This means that the histogram shows the number of pixels for any grey value in the image Fig (6) shows the 2D_power spectrums and histograms of baboon plain and cipher image with size is 200x200. Eq (9) is used to define power spectrum:

$$P(p) = \sum_{x=0}^{m-1} 1 \sum_{y=0}^{n-1} f(x,y)\exp(-j(\pi/m)ux)\exp(-j(2\pi/n)vy) \quad (9)$$

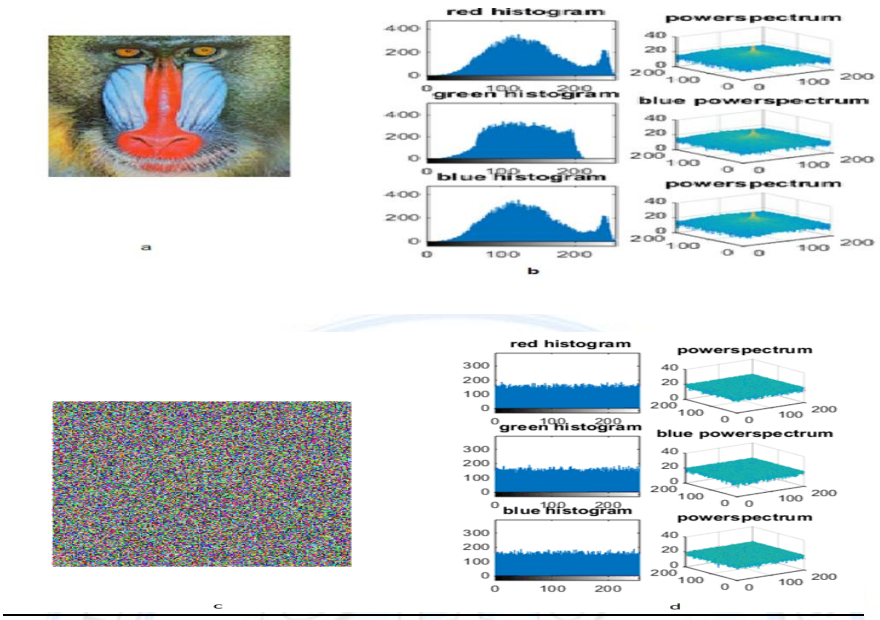

Figure (6) a. Plain baboon image, b. Power spectrum and histogram of baboon plain (red, green, blue). c. Baboon cipher image by FL-STBC. d. Power spectrum and histogram of baboon cipher image by FL-STBC+ (red, green, blue)

2. Correlation-Coefficients

The covariance (COV) and the correlation coefficient (LCY) with the variables x and y are grey-scale values of pixels in various images or two neighboring pixels in the same image are used to measure correlation between pixels. Image correlation test in encrypted images and main are explained in table (5), correlation coefficient is defined as following eq (10):

$$COV = 1/n \sum_{i=0}^{n} (a\,i - E(a))(bi - E(b))$$

$$LCY = \frac{cov(a,by)}{\sqrt{D(a)\sqrt{D(b)}}} \quad (10)$$

The functions E (a) and E (b) are expressed as:

$$E(a) = \frac{1}{n}\sum_{i=1}^{n} ai \quad \text{and} \quad D(a) = \frac{1}{n}\sum_{i=1}^{n} (ai - E(a))\text{^}2$$

Table (5) Correlation between two images (cipher and plain images)

Plain image /cipher image		Red	Green	Blue
Pepper image	Red	-0.004256824028042	-0.004256824028042	0.006707211047192
	Green	0.002906849721567	-0.003256486773138	0.001645996547586
	Blue	0.002714981576375	-0.002546862784032	0.003974649789925
Baboon image	Red	0.008023538050669	-0.003758062047597	-0.003368588768060
	Green	-0.001226706746139	-0.002700090897674	-0.001186741955271
	Blue	0.003852159602569	0.006358162564836	0.008023538050669

3. Image Entropy: Entropy describes the degree uncertainty in the image as show in table (6) and eq (11) defines entropy as:

$$\text{Entropy (a)} = \sum p(a_i) \log \frac{1}{p(ai)} \quad (11)$$

Table (6) Entropy for cipher image

Image		Entropy
Peppers Image	Plain image	7.336671306890284
	Cipher image	7.995322691465507
Baboon Image	Plain image	7.512635946703251
	Cipher image	7.994885029377151

c. The Randomness Tests

The Formal Language_STBC gives accepted and reasonable implications according to the NIST. Table (7) shows statistical tests for keys generation and use through FL-STBC.

Table (7) The Statistical Tests of keys

Statistical Tests	Result	P-Value >=0.01
1-Block Frequency Test	Successful	0.186809464593713
2-Mono-bit Frequency Test	Successful	0.0268566955075244
3-Overlapping Templates Test	Successful	0.339425652470701
4-Non- Overlapping Templates Test	Successful	0.987271934931365
5-Serial Test	Successful	0.106541727676038
6-Aproximate Entropy Test	Successful	0.999980633452663
7-Linear Complexity Test	Successful	0.339425652470701
9-Cumulative Sums Test (Forward)	Successful	0.0107782589860941
10-Runs Test	Successful	0.172788841175563
11-Longest Run of ones Test	Successful	0.0235528800196006
12-Binary Matrix Rank Test	Successful	0.842727765244472
13-Spectral DFT Test	Successful	0.86338894368862

d. Key space-analysis: FL-STBC has key space used for encryption and decryption. If security method has key space larger than 128bit, it is considered as secure system and the brute force attack on such system is infeasible. FL-STBC method uses key (x_0, y0, key, Rx, ry, itr), if x_0, y0 ∈ [0, M]. Therefore, FL_STBC has key space larger than 2^{128}, hence this method is very strong against brute force attack

Conclusions

FL-STBC is new security method based on information theory to protect data on physical layer .The main idea is using 4_dim standard chaotic map to make permutation and change each pixel value then that presents input data to another form on number line and residue class is used to generate key (one time pad).from FL-STBC can be deduced many points as: a.New 4-dim standard maps to make confusion and diffusion, b.FL-STBC can be used to resolve problems of network coding (as channel attacker is less noisy than main channel, in this state NC not useful) and c.Keys randomness makes one time pad cipher, (H (M/K) =H (M)), H denotes entropy, M message K key that make perfect security. FL-STBC is efficient and makes security continuous and it is a strong method according to measures mentioned above which is cover histogram, power spectrum, correlation, large key space, ,PSNR, PCNR with UACI.

References

1. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, " A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", arXiv: 1505.07919v2 [cs.IT], 2016.
2. Y. Zou, J. Zhu, X. Wang and V. C.M. Leung, "Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques" , arXiv: 1405.3725v1 [cs.IT], 2014.
3. S. Sesia, I. Toufik, M. Baker, "LTE – The UMTS Long Term Evolution", John Wiley & Sons Ltd, 2011.
4. M. Bloch and J. BARROS, "Physical-Layer Security from Information Theory to Security Engineering", Cambridge University, 2011.
5. A. H. Alqahtai, A. Iyanda Sulyman, and A. Alsanie" Rateless Space Time Block Code for Massive MIMO Systems", Hindawi publishing corporation International Journal of Antennas and Propagation Volume 2014.
6. M. Elizinati, " Space Time Block Code for Wireless Communications", thesis 2008.
7. Willie K. Harrison," Physical-layer security: Practical aspects of channel coding and cryptography", Dissertation (ph.d), Georgia Institute of Technology, 2012.
8. Y. Zou, J. Zhu, X. Wang, and L. Hanzo,"A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", arXiv: 1505.07919v2 [cs.IT] 23 Apr 2016.
9. X. Zhou, L. Song, Y. Zhang ," Physical Layer Security in Wireless Communication " Taylor & Francis Group, LLC, 2014.", fifth edition, 2011.
10. H. M. A. Salman,"A Hana'a Salman Encryption", the International Arab Journal of Information Technology, Vol. 1, No. 0, 2003.
11. H. M. A. Salman, "Proposal Design: Fingerprint Random Number Generators", the 13th International Arab Conference on Information Technology ACIT', 2012.
12. S. Ganurkar, "Performance of Chaos Communication System using MIMO Techniques and OFDM", International Journal Of Core Engineering & Management (IJCEM) Volume 2, Issue 3, 2015.

13. Z. Chen, L. Yin, Y. Pei1 and J. Lu," Code Hop: Physical Layer Error Correction and Encryption with LDPC-based Code Hopping", Science China Press and Springer-Verlag Berlin Heidelberg, 2016.

14. A. Majumder, M. Raihan Ruhin, T. Hashem, Md. Imdadul Islam, "Recovery of Image through Alamouti Channel with Incorporation of RSA Algorithm", Journal of Computer and Communications, Scientific Research Publishing2016, 4, 1-10

15. J. Soto and L. Bassham, "Randomness Testing of the Advanced Encryption Standard Finalist Candidates", U.S. department of commerce technology administration computer security division National Institute of standards and Technology Gaithersburg, 2000.

16. A. Rukhin, J. Soto, J. Nechvatal, M.Smid, E. Barker, S. Leigh, M. Levenson, M.Vangel, D. Banks, A. Heckert, J. Dray and S. Vo "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standard and Technology, 2010.

17. G. Hanchinamani, L. Kulakarni , "A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System", International Journal of Computer Applications (0975 – 8887) Volume 96– No. 11, June 2014

18. S. Ansari, S. Agrawal," A Review on Chaotic Map Based Cryptography", International Journal of Scientific Engineering and Technology Volume No.1, Issue No.4, pp : 24-27 ,2012.

19. K. Wong, B. Sin-Hung Kwok, and W. Shing Law ," A Fast Image Encryption Scheme based on Chaotic Standard Map", 2010.