Journal of Advanced Computer Science and Technology Research, Vol.6 No.2, June 2016, 37-51

Voice Encryption Using Twin Stream Cipher Algorithm

Omar.M.Hammad[1,a], HebahH.O.Nasereddin[1,b,] Abdulkareem.O.Ibadi[2,c]

[1] Faculty of Information Technology, Middle East University (MEU), Amman, Jordan

[2]Baghdad College for Economic Sciences

[a]omarmejbel@gmail.com, [b]hnasereddin@meu.edu.jo, [c]dr.ibadi@yahoo.com

ISSN: 2231-8852

ABSTRACT

There are many techniques and methods that are currently used in information security. One of these techniques hide the information (cryptography) sent through various media; so that the observer did not feel of the existence of secret information within the sent information through the public communication channels. In this paper the encryption discussed as a voice encryption used of the twin stream cipher algorithm. There were two methods for measuring randomness that need satisfied for the binary strings used as key-stream, the first method examines the hypothesis that the string based on Bernoulli trials. The second method for examining the strength of a key-stream generator measured the complexity of the strings produced. This paper based on two algorithms the base and the twin algorithm the results shown and discussed with a lot of details corresponding to the stream cipher.

Keywords: Cryptography, communication channels, LFSR, FCSR, Non-linear FSR

1. Introduction

During the past years, information security has become the most interest issue for many researches that are trying their effort to reach solutions, techniques and new ideas to ensure the transfer of information safely through the network without any penetration and detection of the information. As a result, there are many techniques and methods that are currently used in information security. One of these techniques is to hide the information (cryptography) sent through various media; so that the observer does not feel of the existence of secret information within the sent information through the public communication channels. Fig. 1 illustrates the cryptography suggested by Abadi, (2010). In this paper the encryption will be discussed as a voice encryption using the twin stream cipher algorithm.

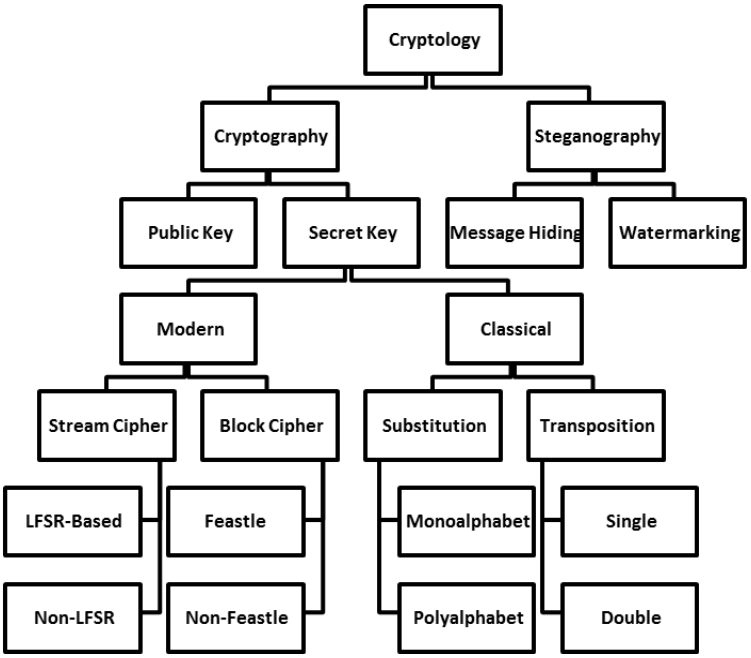

Fig. 1. Cryptology classification (Abadi, 2010)

The largest problem of the communication and computer security is shielding the secret information from interceptions. The art and science of saving messages secure are called the cryptography. The procedure of transformation the plaintext to cipher-text is called encryption or the encipherment, while the procedure of transformation the cipher-text to plaintext is called decryption or the decipherment, see Fig. 2. The strength of the cryptosystem or the cipher system can be established on the secrecy of the enciphering algorithm or the secrecy of its parameters (Ghosh, 2011).

The security of a cipher does not depend only on the algorithm secure, even though modern technology allows the encapsulation of algorithm implementations as a coordinated circuits that are resistant to reverse engineering attacks that is include secret parameters called keys. In most applications, except the military or secret government communications, the algorithms are a public knowledge and the security of the cipher is based exclusively on the secrecy of keys.

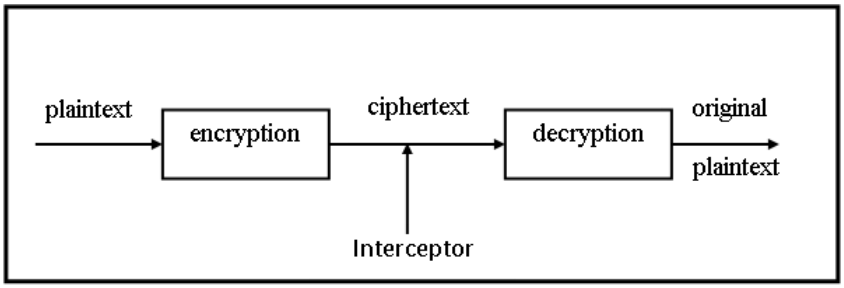

Fig. 1. Encryption and decryption (Ghosh, 2011)

In general there are two types of key-based algorithms; symmetric and asymmetric algorithms. In symmetric algorithms the encryption keys and the decryption keys are the same. These algorithms, also called the secret key algorithms need that the sender and the receiver agree on the key before they communicate securely. The security of symmetric algorithms reset in the key. Encryption and decryption with symmetric algorithm can be denoted by: (Singhal and Raina, 2011)

EK (P) = cipher-text resulting from encryption of the plaintext (P) using key (K).

DK(C) = plaintext resulting from decryption of the cipher-text(C) using key (K).

Symmetric algorithms can be separated into two classes, the first class called the stream algorithms or stream ciphers when some operate on the plaintext a single bit or byte at a time, where the second class called the block algorithms or block ciphers when operate on the plaintext in groups of bits, the groups of bits are called blocks. (Singhal and Raina, 2011)

Asymmetric algorithm is designed when the encryption keysis not the same as the decryption keys, this algorithm may be called public key algorithm because the encryption key can be public. (Singhal and Raina, 2011)

The key administration considered is the significant part of cryptography, as well as the main point of cryptography is to hold the plaintext or the key secret from any unauthorized user eavesdroppers. While the cryptanalysis defined as the science of recovering the plaintext or the key and an attempted cryptanalysis is called the attack. There are four general types of cryptanalytic attacks (Moldovyan, 2008):

1. Cipher-text only attack: The attacker knows only the cipher-text and attacks of the knowledge of statistical properties of the language for the plaintext; such as the frequency of a certain symbols or groups of symbols (letters) or by predicting the most possible string of symbols for the plaintext (word).

2. Known plaintext attack: The attacker knows both the plaintext and the corresponding cipher-text.

3. Chosen plaintext attack: The attacker knows the cipher-text for the plaintext of choice.

4. Adaptive-chosen plaintext attack: This is a special situation of a chosen for the plaintext attack. Not only the attacker can choose the plaintext that encrypted, but they can also modify the choice depends on the results of previous encryption.

Different algorithms suggest different degrees of security depend on how hard they are to break. An algorithm is unconditionally secure if no matter how much cipher-text of cryptanalyst has, there is not enough information to recover the plaintext In point of fact, only one-time pad is unbreakable given infinite resources. A brute- force attack is called when the unauthorized user trying every possible key one by one and checking whether the resulting plaintext is meaningful, this attack for breakable cryptosystems in a cipher-text-only attack. (Hirota, Sohma, Fuse and Kato, 2005).

Stream Cipher

A stream cipher which is defined as the process of encryption that is applied in a binary plaintext and encrypted it one bit at a time interval (t) of a pseudo-random sequence K (t), it is combined by utilizing modulo two addition with plaintext bit P(t), at time interval (t) to create the cipher-text bit also at time interval (t) which is denoted by C(t). The sequence K(t) is called the key-stream for the stream cipher which is seen in Fig. 3.The encryption process and The decryption process can be expressed as below (Abdulsalam, 2011):

$C(t) = P(t) \oplus K(t)$ (1)

$P(t) = C(t) \oplus K(t)$ (2)

Where :

$\oplus$: modulo two addition

T : time interval

K (t) : pseudo-random sequence

P (t) : plaintext bit

C (t) : cipher-text bit

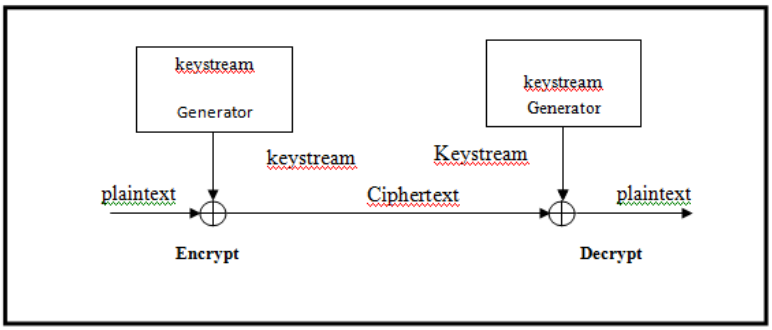

Fig. 2. Stream cipher (Abdulsalam, 2011)

The equations (1) and (2) indicated that the encrypt and the decrypt needed to produce the same key stream sequence K(t). The key (k) for the stream cipher is defined as the initial seed to start the generator. Both encrypt and decrypt needed to procedure this key. At the same time, the security of the stream ciphers depends completely on the key-stream generator. (Abdulsalam, 2011)

Advantages of Stream Cipher

Stream cipher systems have many advantages, which is made them the mainly extensively used systems, these are:

1. It can be generated a long bit streams from a small number of the initial parameters, so it is extremely able for practical applications.
2. It can be simply operated at speeds above 20 Mbit/s; therefore it is enabling real-time enciphering of speech.
3. It can be depended on a number of shift registers which is relatively cheeped.

4. It is comparatively insensitive to errors introduced throughout the transposition. If a bit of the cipher-text is modified throughout the transposition then only this bit will be deciphered wrongly when the text reaches to the receiver.

Shift Registers

The most important component of the most stream ciphers is the shift register (SR). The universal structure of the SRs, as shown in Fig. 4, is that every SR contains of m stages; every stage can be hold one bit. A clock input on each pulse of a clock is controlled the SR; the bits are shifted one stage to the right. The bits which are generated at the stage number 0 form the output of the SR, as the bits are shifted to the right; it is essentially to provide a new group of bits to stage m-1for the SR of length m. These bits can obtain from the feedback loop contain the module which is calculated the value of the fresh bit SR with a feedback called the *feedback shift register* (FSR). (Hell, Johansson, Maximov and Meier, 2006)

It is too obvious that if there are m numbers of stages then there will be 2^m probable states, since there are 2^m probable states there will be 2^{2^m} possibilities for the function of the feedback .There are three types of FSR, which are LFSR, FCSR, and Non-linear FSR.

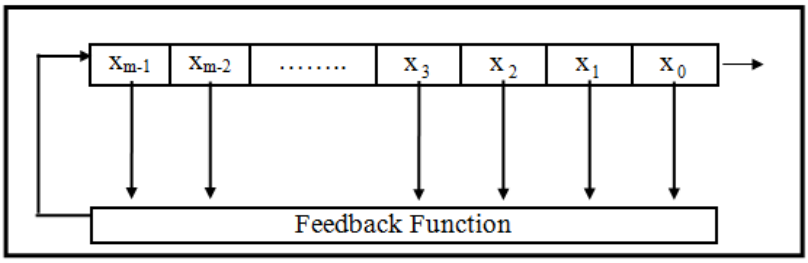

Fig. 3. Feedback shift register (Hell, Johansson, Maximov and Meier, 2006)

- **Linear-Feedback Shift Register**

The linear feedback shift register (LFSR) is distinct as the feedback shift register that's the feedback function $f(x_0, x_{1\ldots}x_{m-1})$ is a linear function, i.e. the feedback function can be expressed as (Hell, Johanssin and Meier, 2007):

$F(x_0, x_{1\ldots}x_{m-1})=c_0x_0+c_1x_1+\ldots\ldots\ldots+c_{m-1}x_{m-1}$

$$= \sum_{i=0}^{m-1} c_i x_i \qquad (3)$$

The coefficients $c_{0\ldots}c_{m-1}$ can be assumed to be two values 0 or 1, and so determines whether or not a particular stage is linked to the feedback loop or not. Consequently, there are 2^m linear functions in total; as shown in Fig. 5 below.

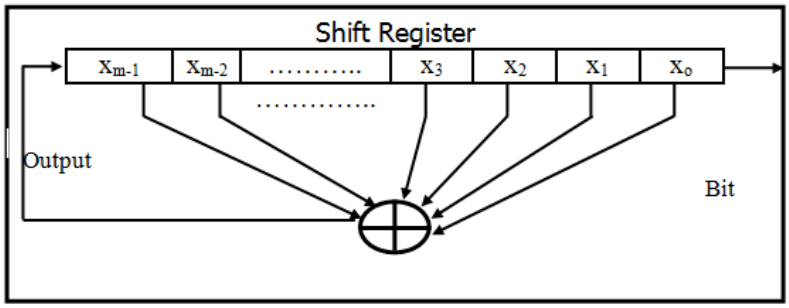

Fig. 4. Linear feedback shift register (Hell, Johanssin and Meier, 2007)

The m stage LFSR can be generated sequences with utmost period lengths of 2^m–1. Whether the SR is able to produce the utmost length sequences based on whether f(x) is a primitive polynomial. The primitive polynomial of the order m is an irreducible polynomial which is cannot to be factorized further, and which has an exponent equal to 2^m-1. If f(x) is a primitive polynomial of order m then the connected shift register will create the maximum length sequence with a period equal to 2^m -1 (Hell et al, 2007).

- **Feedback with Carry Shift Registers**

The feedback with carry shift register (FCSR) is alike to (LFSR) that both of them have SRs and feedback functions, but the FCSR has a carry register as shown in Fig. 6. Additionally, in place of XO-Ring all the bits in the tap sequence added the bits collectively and added the contents of the carry register. The summation result mod 2 becomes the new bit, and summation div 2 is the new content of the carry register.(Arnault, Berger and Pousse, 2011).

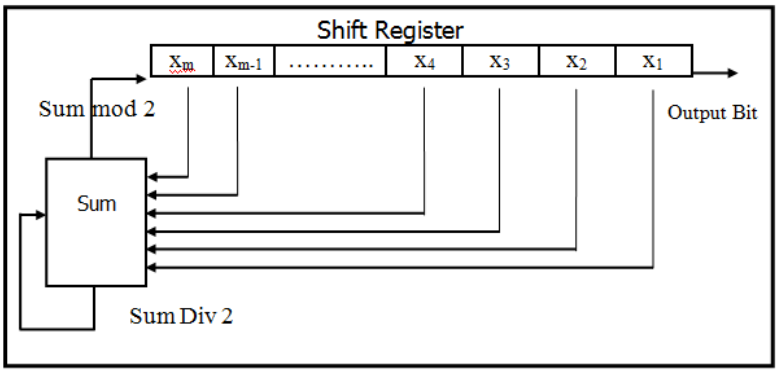

Fig. 5. Feedback with carry shift registers (Arnault, Berger and Pousse, 2011)

- **Non-linear feedback shift registers**

Non-linear FSR be able to design by defining non-linear feedback functions. It is easy to visualize more complex feedback sequence than the one used in LFSRs or FCSRs. The problem is that there isn't any numerical theory that can be analyzed them. Particularly, here are few problems with nonlinear feedback shift register sequences,(Chen et al, 2005):

1. There may be biases, for example more ones than zeros or fewer runs than the predictable in the output sequence.
2. The utmost period of the sequence may be much lower than the predictable.
3. The period of the sequence may be dissimilar for different string values.
4. The sequence may be appeared random for a while, but then "dead end" into a single value. (This can simply be solved by XO-Ring the non-linear function with right-most bits).

On the other side, if there is no theory to analyze the non-linear feedback shift registers for security, there are few tools to cryptanalyst the stream cipher depend on them. The non-linear feedback shifts registers can be used in a stream cipher design, but it have to be careful. In the nonlinear feedback shift register, the feedback function can be anything wanted, see Fig. 7 below.

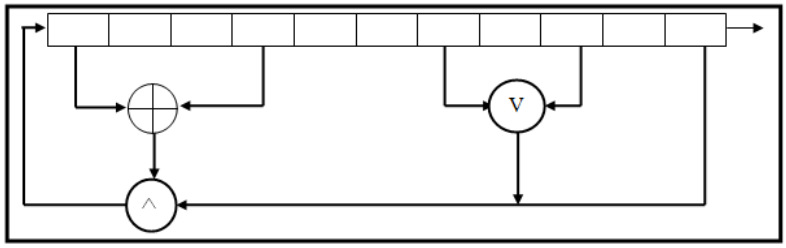

Fig. 6. Non-linear feedback shift register (Chen et al, 2005)

Non-Linear Combiner of LFSRs

The essential technique to design the key-stream generator is by using the LFSRs. It is easy; first take one or more LFSRs, usually of dissimilar lengths and with different feedback polynomials. (If the lengths are all relatively prime and the feedback polynomials are all primitives; the whole generator is maximal (length)). The output bit is a function if at all possible a nonlinear function of some of the bits of the LFSRs. This function is called the combining function, while the whole generator is called a combination generator. (Deepthi, John and Sathidevi, 2009).

Complications have been added, some generators have LFSRs clocked at different rates, and sometimes the clocking of one generator depends on the output of the other one. Clock control can feed onward where the output of one LFSR controls the clocking of another, or feedback where the output of one LFSR controls its own clocking. (Deepthi et al, 2009).

Random Properties of Sequences

The sequences with a large period have an advantage that is their predictability is far small than the sequences with a small period. However, this is not the only principle for cryptographic applications. For instance a particular text with a long period is represented by a sequence of first all zeros and then all ones, it will be completely inappropriate for enciphering since, the cipher-text will be equal to the plaintext as long as only zeros are processed. When ones are created the cipher-text will be equal to the inverted plaintext. Adequately random means that succeed bits

cannot be predicted with any trouble, if a given number of bits of sequence are known. One probable description of a pseudorandom binary sequence was proposed by (Golomb, 1989),he defined a pseudo-random sequences "pseudo-noise sequences" to be a binary sequence of period (P) that satisfy the next three randomness postulates:

R1: If P is even and the cycle of a length equal to P should have an equal number of zeros and ones, if P is odd and the number of zeros shall be one less or more than the number of ones.

R2: In the cycle of length equal to P, half of the runs have length equal to1 a quarter have length equal to 2, an eight have length equal to 3 and in general for every i for which there are at least $1/2^i$ of runs have length equal to i. Moreover, for each one of these lengths there are uniformly many gaps and blocks. A run of length equal to r is a string of r the same bits which is both preceded and succeeded by the reverse bit.

R3: The out-of-phase auto-correlation is a stable or constant. The auto-correlation function $C(\tau)$ of a binary sequence $S_0S_1S_2\ldots\ldots$ of a period P is defined by:

$$C(\tau) = \frac{A(\tau) - D(\tau)}{P}$$

Where;

- $A(\tau)$: the position numbers in which $S_0S_1S_2\ldots\ldots S_{p-1}$ and $S_\tau S_{\tau+1}.....S_{\tau+p-1}$ agree.
- $D(\tau)$: the position numbers in which they disagree.

Over and over again one can discover that a sequence is not random, but certify that a sequence is random is a hard mission indeed. As a suggestion, no sequence created by computer ability, in fact, it is random but getting sequence that exhibits a lot of the properties for the random numbers. Unluckily, it is regularly not possible to articulate precisely which properties of random numbers are significant for a exacting application (Golomb, 1989).

2. Research Problem

According to the traditional conceptions over secure group communications such as (confidentiality, authenticity, and integrity) will become a critical networking issues, and the secure communication between parties takes the great attention in recent researches. There are many problems that occur in the communication process, one of these problems is producing pure key bits corresponding to the silence periods in a speech encryption because of frequently generating zero's to represent the silence between pronounced words during speech. The main objective of this research is to design a new concept of stream cipher algorithms used in an advanced application for protecting data and information in network communications.

3. Research Methodology

The main purpose is to obtain sequences which behave as if random. No infinite sequence generated by a sequence generator using a finite key can be truly random; the best that can be hoped is any subsequence of length less or equal to the period should be "indistinguishable" from a random sequence of the same length. Such a sequence is termed pseudorandom sequence, these sequences are not really random, but they can be useful as approximations to random numbers. There are two methods for measuring randomness that need to be satisfied for the binary strings used as key-stream. Each of these methods will be described below; the first method examines the hypothesis that the string based on Bernoulli trials, for which:

$P_r (k(t) = 1) = p_r(k(t) = 0) = ½$ (4)

Where:
K (t): pseudo-random sequence
Pr: Bernoulli trials

Tests employed in this study to examine this hypothesis are the frequency test, binary derivative test, change point test, serial test, poker test, and run test.

The second method for examining the strength of a key-stream generator is to measure the complexity of the strings produced. Two different measures of complexity are employed, namely autocorrelation and linear complexity.

The innovation of the concept of the twin stream cipher algorithm design is the main and the novel designing concept. It is a new approach to design cryptographic algorithms. The concept of this research is to design two symmetric algorithms and to produce a key bit from one algorithm at a time using a random method. The reason of this research is refers for the designing such algorithms to avoid producing pure key bits corresponding to the silence periods in a speech encryption. In this paper, an LFSR-based stream cipher is used:

1- An application is build.
2-The samples are tested by randomness tests.

In this paper a new proposed twin stream cipher algorithm is introduced. Its concept, its main features, and its characteristics are discussed in details. To prove any stream cipher is designed well; we must compute its period which must be computationally secure and prove that it has a random behaviour by passing the standard statistical randomness tests.

To prove that the twin stream cipher algorithm is designed well, a single part of the twin must be tested and the produced key sequences must be examined. The following sections will these tasks in considerations.

a. The Twin Concept

Fig. 8 shows that the proposed algorithm consists of two main parts they are: the twining part and the combining part.

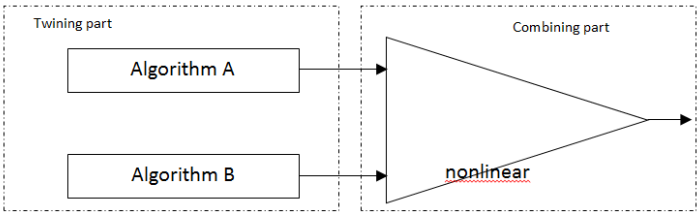

Fig. 8. Twin algorithm main components

The twining part must consist of two identical well-tested stream cipher algorithms (algorithm A and algorithm B). The combining part is a nonlinear function its inputs were the twining part outputs and its output is the generated key bit sequence.

b. Stream Cipher Algorithm

An LFSR-based stream cipher must be combining of two parts; the driving part (linear part) and the nonlinear part as shown in Fig.9.

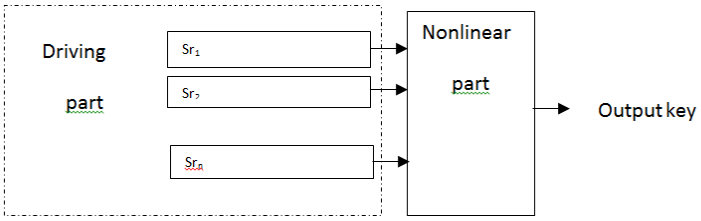

Fig. 9. Stream cipher algorithm parts

The driving part consists of one or more LFSR's. This part is responsible for determining the period of the algorithm. While the nonlinear part is one nonlinear function or mixed of linear and nonlinear functions which are used to generate the key bit sequence. The nonlinear part is responsible for the determining the algorithm complexity.

c. The proposed Twin Stream Cipher Algorithm

To design a twin stream cipher algorithm we must perform the following:

a) Design a new LFSR-based stream cipher algorithm or select one of the well-known pretested stream cipher algorithm as a part of the twin.
b) Design a new nonlinear compound function or select one of the well-known pretested one.

The designed stream cipher algorithm must satisfy the conditions of designing a stream cipher algorithm by designing the driving part and the nonlinear part. To do so, we must design the nonlinear part first to determine the inputs number which correspond the number of LFSR's in the driving part.

d. The Combining Part

It is too difficult to design a nonlinear function that should generate a balanced sequence and has no correlation with its inputs. For this reason we decided to use the nonlinear part of the stream cipher algorithm as the combining part for the twin algorithm.

Fig. 10 discussed the designed nonlinear function which is used as nonlinear part for the stream cipher algorithm and as combining part for the twin algorithm.

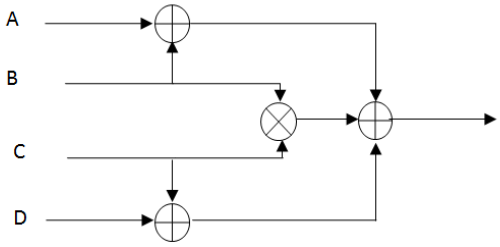

Fig. 10. The nonlinear part

Table 1 show that the truth table of the function is balanced because the number of 0's and 1's are equal.

Table 1: the truth table of the proposed function

A	B	C	D	Output
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

The correlation between the output and any of the input in the truth table are equal to 0.5. The correlation is computed by the following formula:

$$\text{Cor} = \frac{Ac}{Ac + Dc}$$

Where Ac is the number of similarity between the output and the input, Dc is the number difference between the output and the input.

e. The Driving Part

The proposed function need four input bits to generate one output bit for this reason the driving part of the stream cipher algorithm must have four LFSR's at least. So, a suitable LFSR length must be selected with tapping stages for the feedback function giving maximum period. Fig. 11 depicts the selected driving part for the stream cipher algorithm.

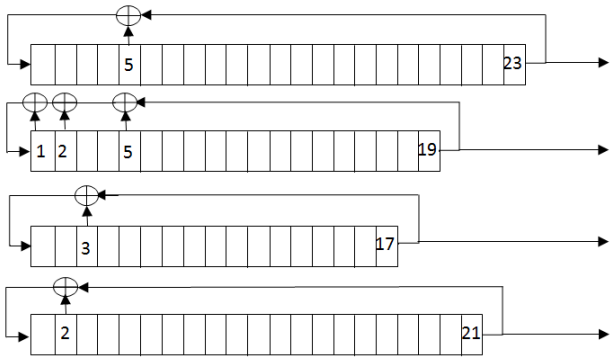

Fig. 11. The driving part of the stream cipher algorithm

The length of the LFSR's are 23, 19, 17, 21 respectively and tapping stages for the feedback functions are (23, 5), (19, 5, 2, 1), (17, 3), (21, 2) as shown in Fig. 11 The proposed stream cipher algorithm is shown in Fig. 12.

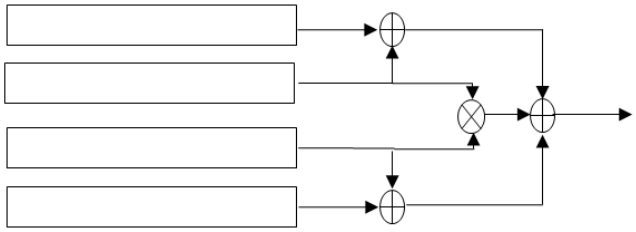

Fig. 12. The proposed stream cipher algorithm

f. The Proposed Twin Stream Cipher Algorithm

In the design of the proposed twin stream cipher algorithm, the nonlinear part is used to be the combining part. If the output bit of the combining part is 0 then the output key bit will be computed from the base algorithm otherwise the output key bit will be computed from the twin algorithm. Fig. 13 demonstrates the proposed twin stream cipher algorithm.

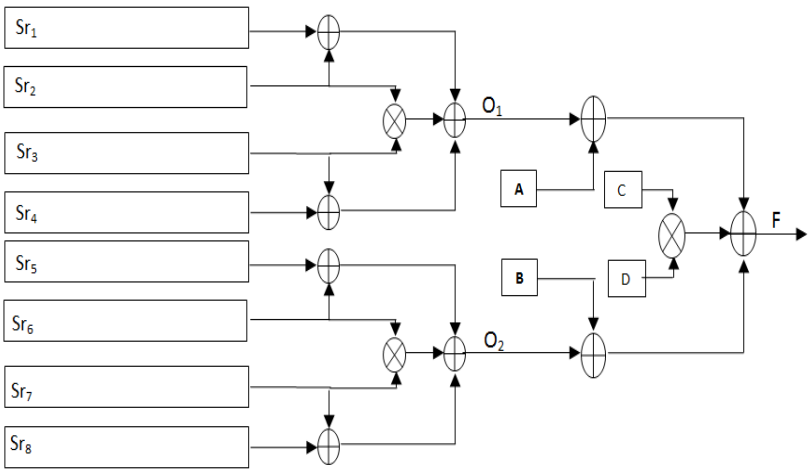

Fig. 13. The proposed Twin stream cipher algorithm

A, B, C, and D are computed by the following equations:

$A=sr_1[11]$ xor $sr_8[7]$

$B=sr_3[13]$ xor $sr_6[17]$

$C=sr_2[11]$ xor $sr_7[7]$

$D=sr_4[13]$ xor $sr_5[13]$

The produced key bit will be O_1 if F=0 else the key bit will be O_2.

4. Results

Table 2 and 3 illustrates the results of based algorithm and twin algorithm.

Table 2. The Based Algorithm Testing

Sequence length	Frequency Test PassMark chi^2 is The Computed Chi^2 is	Serial test Test PassMark chi^2 is The Computed Chi^2 is	Poker Test PassMark chi^2 is The Computed Chi^2 is	Run Test Test PassMark chi^2 is The Computed Chi^2 is	Autocorrelation test (d=8) (P=pass, F=fail) 3.49
6003	3.49 0.28 PASSED	7.53 2.14 PASSED	15.22 5.99 PASSED	0's is 19.39 0's is 12.78 1's is 20.74 1's is 17.12 T0=pass T1=pass	PPPPPPPP

Table 3. The Twin Algorithm Testing

Sequence length	Frequency Test PassMark chi^2 is The Computed Chi^2 is	Serial test Test PassMark chi^2 is The Computed Chi^2 is	Poker Test PassMark chi^2 is The Computed Chi^2 is	Run Test Test PassMark chi^2 is The Computed Chi^2 is	Autocorrelation test (d=8) (P=pass, F=fail) 3.49
5003	3.49 0.1 PASSED	7.53 4.79 PASSED	15.22 7.14 PASSED	0's is 24.71 0's is 30.26 1's is 20.74 1's is 7.55 T0=FAIL T1=PASS	PPPPPPPP

5. Conclusion

The security of a cipher does not depend only on the algorithm secure, even though modern technology allows the encapsulation of algorithm implementations as a coordinated circuits that are resistant to reverse engineering attacks that is include secret parameters called keys, the algorithms are a public knowledge and the security of the cipher is based exclusively on the secrecy of keys. Different algorithms suggest different degrees of security depend on how hard they are to break. An algorithm is unconditionally secure if no matter how much cipher-text of cryptanalyst has, there is not enough information to recover the plaintext In point of fact, only one-time pad is unbreakable given infinite resources. The twin algorithm contained of two main parts; the twining pat and the combining part. The twining part consisted of two identical well-tasted stream cipher algorithms, while the combining part is a non-linear function. LFSR-based stream cipher must be combining of driving part which is the linear part and the non-linear part. The linear part is used to determine the period of the algorithm, and the nonlinear part is used to generate the key bit sequence and the complexity. Designing the non-linear part by determining the input numbers that corresponding to the number of LFSR which were four with 23,19,17,21 length and (23,5), (19,15,2,1), (17,3), (12,2) as a tapping stages for the feedback function. After that we designed the driving part to satisfy the conditions of designed stream cipher algorithm. The proposed stream cipher algorithm passed the statistical random tests which are the frequency test, serial test, poker test, run test, and autocorrelation test. In the twin stream cipher algorithm, the nonlinear part used to be as a combining part. The output key bit was computed by the base algorithm if the output bit of the non-linear part was zero and by the twin algorithm if the output bit of the nonlinear part was not zero.

REFERENCES

Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995.

Thomas Beth and Fred Piper, the Stop-and-Go Generator. EUROCRYPT 1984, pp88–92.

Christof Paar, Jan Pelzl, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, a textbook for students and practitioners", Springer, 2009.
Merit.et.al "Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, 2012.
Ashraf D. Elbayoumy and Simon J. Shepherd, "Stream or Block Cipher for Securing VoIP?", International Journal of Network Security, Vol.5, No.2, PP.128–133, 2007.
Tin Lai Win, and Nant Christina Kyaw," Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", World Academy of Science, Engineering and Technology 48 2008.
Musheer Ahmad , Bashir Alam, Omar Farooq," CHAOS BASED MIXED KEYSTREAM GENERATION FOR VOICE DATA ENCRYPTION",2010.
Michael Backes, GoranDoychev , Markus D¨urmuth , and Boris K¨opf," Speaker Recognition in Encrypted Voice Streams",2009.
Nidhi Singhal ,J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.
Osamu Hirota.et.al, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme", 2008.
Sandip Karmakar and Dipanwita Roy Chowdhury," Fault Analysis of Grain Family of Stream Ciphers", 2009.
Francois Arnault, Thierry Berger, Marine Minier and Benjamin Pousse," Revisiting LFSRs for cryptographic applications", 2011.