British Journal of Applied Science & Technology
8(1): 107-125, 2015, Article no.BJAST.2015.190
ISSN: 2231-0843

SCIENCEDOMAIN *international*
www.sciencedomain.org

Speech Encryption Using Stream Cipher

Aissa Belmeguenai[1*], Khaled Mansouri[2] and Mohamed Lashab[1]

[1] *Electrical Engineering Department, University of Skikda, BP.26 Route d'El Hadaiek, Skikda, 21000, Algeria.*

[2] *Department of Electronics, Badji Mokhtar University, Annaba, Algeria.*

Article Information

DOI: 10.9734/BJAST/2015/14744
Editor(s):
(1) Jos M. Garrido-Balsells, Dept. of Communications Engineering, University of Malaga, Spain.
(2) Singiresu S. Rao, Department of Mechanical and Aerospace Engineering, University of Miami, Coral Gables, USA.
Reviewers:
(1) Himanshu Gupta, Amity Institute of Information Technology, Amity University, Noida, India.
(2) Anonymous, India.
(3) Anonymous, China.
(4) Anonymous, Algeria.
(5) Anonymous, China.
Complete Peer review History:
http://www.sciencedomain.org/review-history.php?iid=1069&id=5&aid=8546

Original Research Article

Received: 17th October 2014
Accepted: 21st February 2015
Published: 23rd March 2015

Abstract

In this work, we have realized an efficient implementation of stream cipher algorithm for speech data encryption and decryption. The design consists of a 128-bit non linear feedback shift register (NLFSR), a 128-bit linear feedback shift register (LFSR) and a Boolean function. First of all three speeches were recorded from different speakers and were saved as wav file format. The developed program is used to transform the original speech data wav file into positive data, and then transform the positive data into positive digital data file. Finally, we use our implemented program to encrypt and decrypt the speech data. The proposed scheme is compared to a similar one of Grain-128. The results show that the proposed scheme is secure and the encrypted speech was very different than the original speech and no significant information on the original speech could be retrieved. Thus, the results given by the proposed scheme are better than the results given by Grain-128.

Keywords: Correlation coeffecient; key stream generator; stream cipher; speech encryption
2010 Mathematics Subject Classification: 05A10, 05A19, 05A15, 05A99

**Corresponding author: E-mail: belmeguenaiaissa@yahoo.fr*

1 Introduction

The speech communications become more and more widely used in everyday life and even have been known to be vulnerable to interception unauthorized access. The importance of providing a high level of security is dramatically increasing. In this field of research, a variety of speech encryption techniques have been introduced [1, 2, 3, 4, 5]. The characteristics of the speech data make the cryptographic algorithms [1] and [2] inefficient for speech encryption due to speech inherent features, especially high volume speech data. For this reason a stream cipher algorithm for speech communication was introduced.

A stream ciphers are very important parts of the symmetric encryption algorithm which operates with a time-varying transformation on individual basic message of digits. A stream cipher usually consists of a pseudo random generator. The generator takes as input a secret key and then generates a pseudorandom sequence $Z_1, Z_2, ..., Z_i$ of digits known as the running keystream. The cipher message $C_1, C_2, ..., C_i$ is obtained by the bitwise addition of the keystream digit $Z_1, Z_2, ..., Z_i$ and the basic message of digits $M_1, M_2, ..., M_i$ as follows:

$$C(i) = M(i) \oplus Z(i) \quad (1.1)$$

where $\oplus$ is sum modulo 2 (XOR function). The cipher message at the receiver is decrypted by producing the same keystream and adding it to the cipher message such as:

$$M(i) = C(i) \oplus Z(i) = M(i) \oplus Z(i) \oplus Z(i) \quad (1.2)$$

Recently, the attacks [6, 7, 8, 9, 10] and [11] concerning the stream cipher systems based on LFSRs led a lot of researchers to be interested to stream ciphers based on nonlinear feedback shift registers (NLFSR), [12], [13], they are used in a privileged way in the case of communications likely to be strongly disturbed because they have the advantage of no error propagation [14], and are particularly suitable for use in environments where no buffering is available and /or plaintext elements need to be processed individually. They are faster and have a lower hardware complexity than block ciphers (DES) and RSA algorithm.

In this paper we continue our investigations in this field by giving new version for Grain-128 with improvements at the level of the filtering function. In the new version, we kept the same linear feedback shift register(LFSR) and nonlinear feedback shift registers (NLFSR) used in original Grain-128, also we kept the key size 128-bit and the IV size 96-bit, and we changed only the filtering function h of nine variables (see section 2) by the function f of eight variables (see section 4). In order to provide the system with high performance an implementation of new version for speech data encryption/decryption was done, statistical tests and security analysis are presented.

The paper is organized as follows. Section 2 gives brief description of the original Grain-128. Section 3 presents the description of speech encryption and decryption method. In section 4 we present a new version of the Grain-128. In Section 5 we present the software implementation of the cipher for speech data and experimental results. In section 6 we give the security analysis of the design. Section 7 concludes the paper.

2 Grain-128

An LFSR of length n is composed of a shift register containing a series of n bits $s_0, s_1, \cdots, s_{n-1}$, and a Boolean function of linear feedback $g : F_2^n \rightarrow F_2$ called the feedback function. This type of register is easy to implement in hardware and has the advantage of generating sequence with maximal period equal to $(2^n - 1)$ when polynomial feedback is primitive. If the Boolean function g is nonlinear, then the register is called an NLFSR.

The Grain is a bit oriented synchronous stream cipher, it was proposed by Hell, Johansson, Maximov, and Meier [13] as a variant of Grain-v1 [12, 15]. The cipher consists of a 128-bit NLFSR, a 128-bit LFSR and a Boolean function h. The key size and the IV size of Grain-128 are respectively 128 bits and 96 bits. The polynomial feedback of the NLFSR has algebraic degree of two, and h has algebraic degree of three, it has nonlinearity of 240.

We denote respectively by $s_{i+1}, s_{i+2}, ..., s_{i+128}$ and $b_{i+1}, b_{i+2}, ..., b_{i+128}$ the content of the LFSR and the content of the NLFSR.

The output bit of LFSR at time i is computed by the recurrence relation as:

$$s_{i+128} = s_i \oplus s_{i+7} \oplus s_{i+38} \oplus s_{i+70} \oplus s_{i+81} \oplus s_{i+96}. \quad (2.1)$$

The output bit of NLFSR at time i is computed by the recurrence relation as:

$$\begin{aligned} b_{i+128} = s_i \oplus b_i \oplus b_{i+26} \oplus b_{i+56} \oplus b_{i+91} \oplus \\ b_{i+96} \oplus b_{i+3}b_{i+67} \oplus b_{i+11}b_{i+13} \oplus b_{i+17}b_{i+18} \oplus \\ b_{i+27}b_{i+59} \oplus b_{i+40}b_{i+48} \oplus b_{i+61}b_{i+65} \oplus b_{i+68}b_{i+84}. \end{aligned} \quad (2.2)$$

The concatenation of bits (e.g., $b_{i+3}b_{i+67}$) explained as a multiplication of bits.

The combining function of Grain-128 produces an output value based of the selected bits from the NLFSR and the LFSR:

$$h(i) = s_{i+8}b_{i+12} \oplus s_{i+13}s_{i+20} \oplus b_{i+95}s_{i+42} \oplus s_{i+60}s_{i+79} \oplus b_{i+12}b_{i+95}s_{i+95}. \quad (2.3)$$

The output stream of the system generates from the selected bits of the LFSR and NLFSR states and the output of h:

$$y(i) = \oplus_{j \in A} b_{i+j} \oplus h(i) \oplus s_{i+93}. \quad (2.4)$$

The expression $\oplus_{j \in A} b_{i+j}$ explained as the set of exclusive ORs between all bits b_{i+j}, where $j \in A$ and $A = \{2, 15, 36, 45, 64, 73, 89\}$.

3 Speech Encryption Method

The novel speech encryption and decryption method is proposed, this is based on stream cipher. The block diagram of the overall system is shown in figure 1.

Speech data consist of great number of bits which contain both negative and positive bit values, these data serve as input to the proposed algorithm. The algorithm is based on XOR function and the speech data is normalized to obtain values between 0 and 255 before starting the encryption operation.

Let Y and X respectively the original speech data and positive speech data. The novel encryption and decryption scheme works as follow:

Converting the original speech data into positive speech data using the following relation:

$$X = 255 \times (\frac{Y - Min}{Max - Min}). \quad (3.1)$$

where Max and Min are respectively maximal value and minimal value of Y. Then converting the positive speech data into positive digital speech data. The positive digital speech data is stored in file then it is encrypted and sent to the receiver. The flow chart of the encryption process is presented in figure 2.

The receiver function is to decrypt the encrypted positive digital speech data file and convert it into speech data. The flow chart of the decryption process is depicted in figure 3. Figure 4 illustrates the flow chart diagram for encryption and decryption.

3.1 Speech Encryption Algorithm

Input: Positive digital speech file M.
Output: Encrypted positive digital speech file C.
The detailed steps of the algorithm are given below:

- Read the original speech data;
- Convert the original speech data into positive speech;
- Convert the positive speech into positive digital speech and store it in the file M;
- $T \leftarrow$ the length of M;
- Generate the keystream Z_i as shown by the keystream generator algorithm;

- for $i = 1$ to T to make :

  Encrypt the positive digital speech using the relation $C_i = M_i \oplus Z_i$ and store it in the file C;

  End to make ;
- Send the encrypted positive digital speech file .

3.2 Speech Decryption Algorithm

Input: Encrypt the positive digital speech file C.
Output: Decrypted positive digital speech file M.
The detailed steps of the algorithm are given below:

- Read the encrypted positive digital speech file C;
- $T \leftarrow$ the length of encrypted positive digital speech file;
- Generate the keystream Z_i as shown by the key stream generator algorithm;
- for $i = 1$ to T to make :

  Decrypt the encrypted positive digital speech file using the following relation

  $M_i = C_i \oplus Z_i$;

  End to make ;
- Convert the decrypted positive digital speech file into decrypted positive speech;
- Convert the decrypted positive speech into decrypted speech data;
- Get the speech data.

4 Modified Grain-128

In this work, a modified the Grain-128 for speech data protection is introduced. In the modified Grain-128 version we keep the same LFSR and NLFSR which are employed in Grain-128 and the filtering function h is replaced by a Boolean function f from $F_2^8 \rightarrow F_2$ presented in [16]. This function is chosen to be balanced, the correlation immunity is of order 3, with algebraic degree 4, having nonlinearity of 112 and an algebraic immunity of 4.

The inputs of filtering function f is taken as six variables from the LFSR and two variables from the NLFSR. It is defined as

$$\begin{aligned} f(x) = \\ (x_5 \oplus x_8x_5 \oplus x_8x_6 \oplus x_8x_7)\,(x_1x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_2 \oplus x_3) \\ \oplus x_1x_4 \oplus x_3x_4 \oplus x_2 \oplus x_1. \end{aligned} \tag{4.1}$$

Where the variables $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ and x_8 correspond to the top positions

$b_{i+12}, s_{i+8}, s_{i+13}, s_{i+20}, b_{i+95}, s_{i+42}, s_{i+60}$ and s_{i+79} respectively.

The Key stream bit $Z(i)$ is produced by combining the seven bits from the state of NLFSR and one bit from the state of LFSR with the output of a non-linear Boolean function f, it is computed as:

$$Z(i) = \oplus_{j \in B} b_{i+j} \oplus f(i) \oplus s_{i+93}. \tag{4.2}$$

Where $B = \{2, 15, 36, 45, 64, 73, 89\}$.
The modified Grain-128 schematic is depicted by figure 5. The flow chart of the key stream generator (KSG)of the modified Grain-128 is presented in figure 6.

4.1 Keystream Generator Algorithm

Inputs:

- M: positive digital speeche file ;
- $s_1, s_2, ..., s_{128}$ are initially loaded into the LFSR;
- $b_1, b_2, ..., b_{128}$ are initially loaded into the NLFSR;

Results:

- s_i and b_i: binary sequences produced respectively by LFSR and NLFSR;
- f_i: binary sequences generated by filtering function f.
- Z_i: Keystream.

Treatment:

- Read T, the length of positive digital speeche file M;
- Introduce the secret key, the values of initialization of LFSR and NLFSR respectively $s_1, s_2, ..., s_{128}$ and $b_1, b_2, ..., b_{128}$;
- for $i = 1$ to $T + 127$ to make :

  Generate the binary sequences s_i and b_i produced respectively by LFSR and NLFSR according to (2.1) and (2.2);

  End to make ;
- for $i = 1$ to T to make :

  Generate the the binary sequences $f(i)$ according to (4.1);
  Generate the key stream $Z(i)$ according to (4.2);

  End to make ;

5 Test and Experimental Results

In this section we present the results for the proposed approach also we discuss the obtained results from the proposed and implemented scheme system. In order to implement such system, one must go through several steps which were described in details in the preceding sections. The implementation for this simulated project is written by MATLAB.7.5.

In this work, three originals speech data depicted in figures 7 (a), 8 (a) and 9 (a) were recorded from different speakers and were saved as wav file format. These speeches are encrypted and decrypted for both the proposed approach and the Grain 128, we have obtained the following results. To encrypt these speeches, first all we transform the original speech data wav file into positive speech data, and then we transform the positive speech data into positive digital speech file. The encryption programs take the positive digital speech file as input and performe the encryption operation on the file to produce an unreadable encrypted positive digital speech file and save it into another file.

On the other hand, the decryption program take the encrypted positive digital speech file as input and perform decryption operation on the file to produce the decrypted positive digital speech file, then go through several steps which were described in the decryption program to get the original speech data.

Figures 7, 8 and 9 show the experimental results of encryption and decryption for three speeches using the proposed design. Figures 10, 11 and 12 show the experimental results of encryption and decryption for three speeches using the Grain-128.

6 Security Analysis

In this section, we discuss the security analysis of the proposed encryption scheme including some important ones like key sensitivity analysis, key space analysis and statistical attacks. The objective of this section is to prove the security of the proposed cryptosystem against the most common attacks.

6.1 Berlekamps-Massey Attack

The output sequence $Z(i)$ of the modified Grain-128 is a linear recurring sequence. It is essential to estimate its linear complexity. The linear complexity of $Z(i)$ is related to the LFSR and NLFSR length and to the algebraic degree of the filtering function f. According to [17] and [18]

the linear complexity of $Z(i)$ is lower bounded by $\binom{128}{4}$. The Berlekamps-Massey attack [6] requires $2 \times \binom{128}{4}$ data. A binary sequence with linear complexity lower bounded by $\binom{128}{4}$ is sufficiently large which implies that we completely exclude the use of the Berlekamp-Massey attack.

6.2 Time-Memory Trade-off Attacks

A generic time-memory-data trade-off attack (TMTOA) on stream ciphers costs $O(2^{k/2})$, where k is the number of inner state variables in the stream cipher, [19]. The size of LFSR and NLFSR used in modified Grain-128 is 256-bit. Thus, the expected complexity of a time-memory-data trade-off attack is not lower than $O(2^{128})$.

6.3 Correlation Attack

The filtering function f used in the modified Grain-128 is chosen to be correlation immune of third order, which make it very vulnerable to correlation attacks, see [8]. The function f produces its output value based on the selected bits from the NLFSR and the LFSR and f is xored with seven bits from the state of NLFSR and one bit from the state of LFSR, which will make the correlations between the output of f, LFSR and NLFSR bits small that they will not be exploitable by correlation attacks.

6.4 Algebraic Attack

Today, we know that to resist algebraic attacks, the chosen Boolean functions must have an algebraic immunity degree greater than seven. The function f has an algebraic immunity lower bounded by 4, which make it very vulnerable to algebraic attacks, see [10] and [11]. On the other hand, the function f tack its inputs from six bits from the LFSR and two bits from the NLFSR, as the update function of the NLFSR has algebraic degree two, and f is xored with a linear combination of NLFSR-state bits, the algebraic degrees of the output bits when expressed as a function of LFSR-bits, are large in general, and varying in time. This will make the work of algebraic attacks very difficult.

6.5 Correlation Coefficient

Correlation coefficient is a measure of the linear dependence between two variables U and V, giving a value between +1 and 1 inclusive, where 1 is total positive correlation, 0 is no correlation, and 1 is total negative correlation. The correlation coefficient is defined as:

$$Cor(U,V) = \frac{Cov(U,V)}{\sigma_U \sigma_V}. \qquad (6.1)$$

Where Cov is the covariance, σ_U is the standard deviation of U. By Cor_1 and Cor_2, we denote respectively the correlation factors between original speech and its encrypted data, and the correlation factors between original speech and its decrypted data using the modified Grain-128. We denote by Cor_3 and Cor_4 respectively the correlation factors between original speech and its encrypted data, and the correlation factors between original speech and its decrypted data using Grain-128. Table 1 gives the correlation coefficient results.

It is observed that the examined correlation factors in both cases are small for both the original speeches and their encrypted speeches. This implies that the original speeches are independent of encrypted speeches.

By simple comparison between the correlation factors obtained by the modified Grain-128 and those obtained by the Grain-128, we can confirm that the correlation factors obtained by the proposed design are ten times lower than those obtained by the Grain which implies that the proposed design is better than the Grain-128.

6.6 Comparison with Grain-128

Table 2 gives the comparison between Keystream bit specification of the modified Grain-128 and the keystream bit specification of Grain-128. It is observed in table 2 that most of cryptographic properties of keystream bit of the modified Grain-128 are better than those of the original Grain-128.

Table 1: Correlation Coefficients Analysis

Cases	Cor_1	Cor_2	Cor_3	Cor_4
Speech 1	0.00089	1	-0.0089	1
Speech 2	0.0012	1	-0.0117	1
Speech 3	0.00029	1	0.0012	1

Table 2: Comparison between Modified Grain-128 and Grain-128

Specification of Keystream bit	Grain-128	Modified Grain-128
Balancedness	is balanced	is balanced
Algebraic Degree	3	4
Correlation Immune	7	11
Nonlinearity	61440	28672
Algebraic Immunity	-	lower bounded by 4
Number of variables	17	16
Linear Complexity	lower bounded by $\binom{128}{3}$	lower bounded by $\binom{128}{4}$

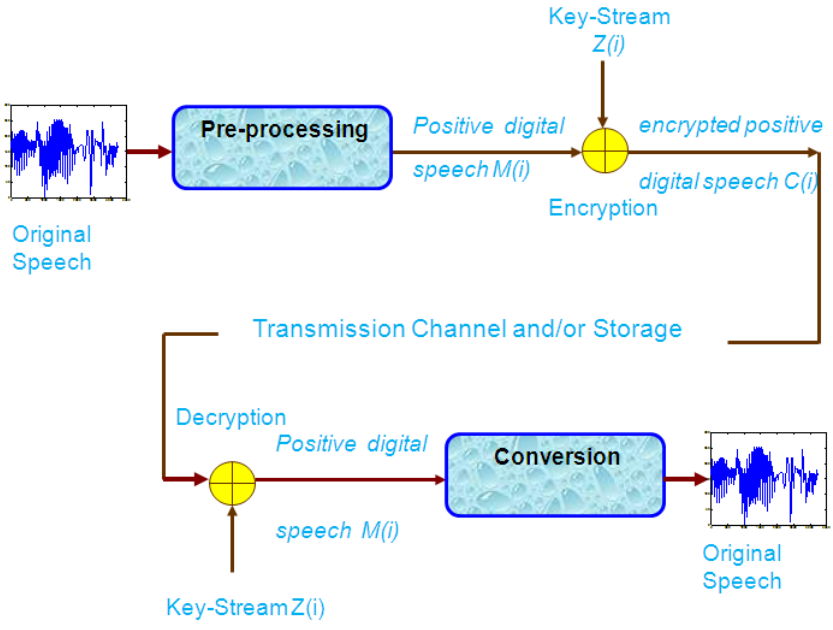

Figure 1: *Block Diagram of the Proposed Approach.*

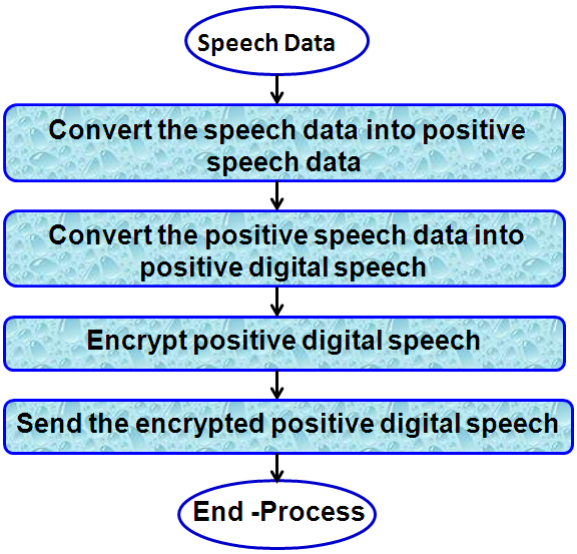

Figure 2: *Flow Chart of the Encryption Process.*

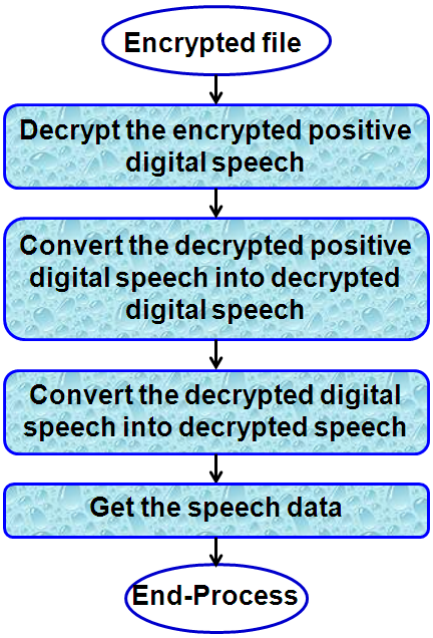

Figure 3: *Flow Chart of the Decryption Process.*

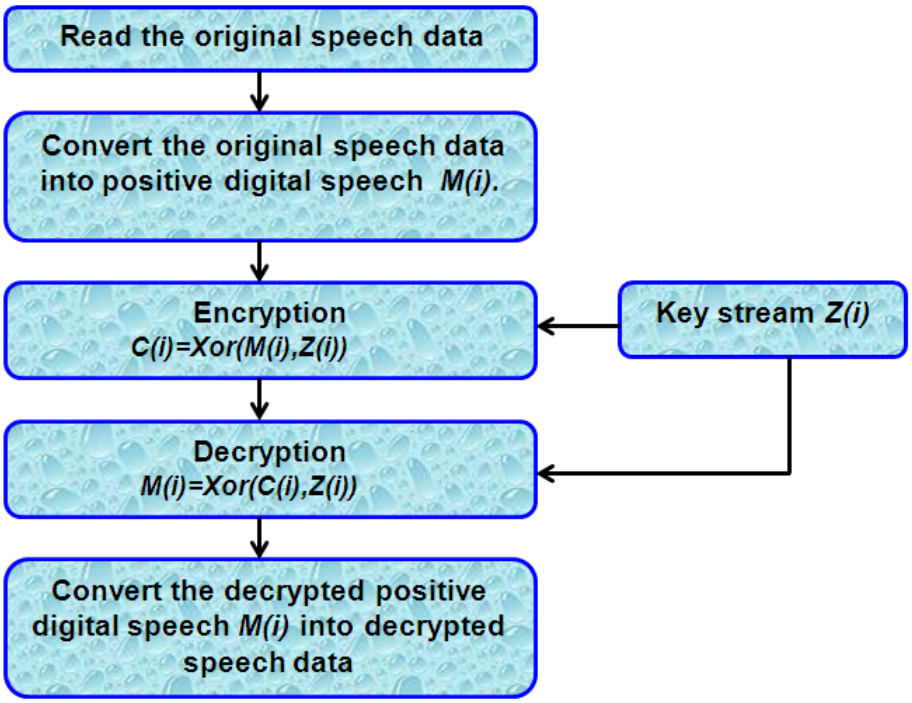

Figure 4: *Flow Chart Diagram for Encryption and Decryption.*

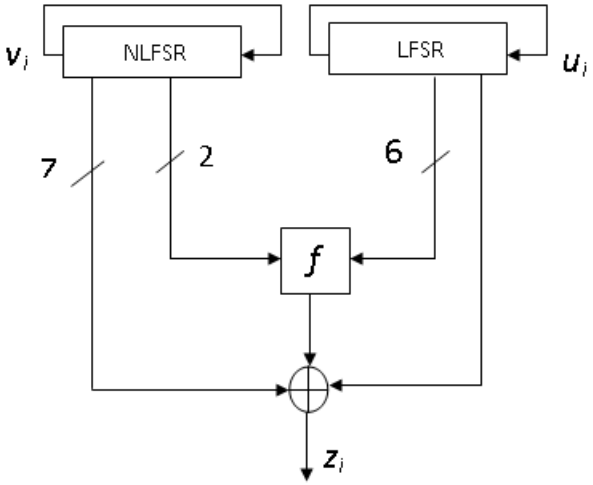

Figure 5: *Modified Grain-128 Key stream Generator.*

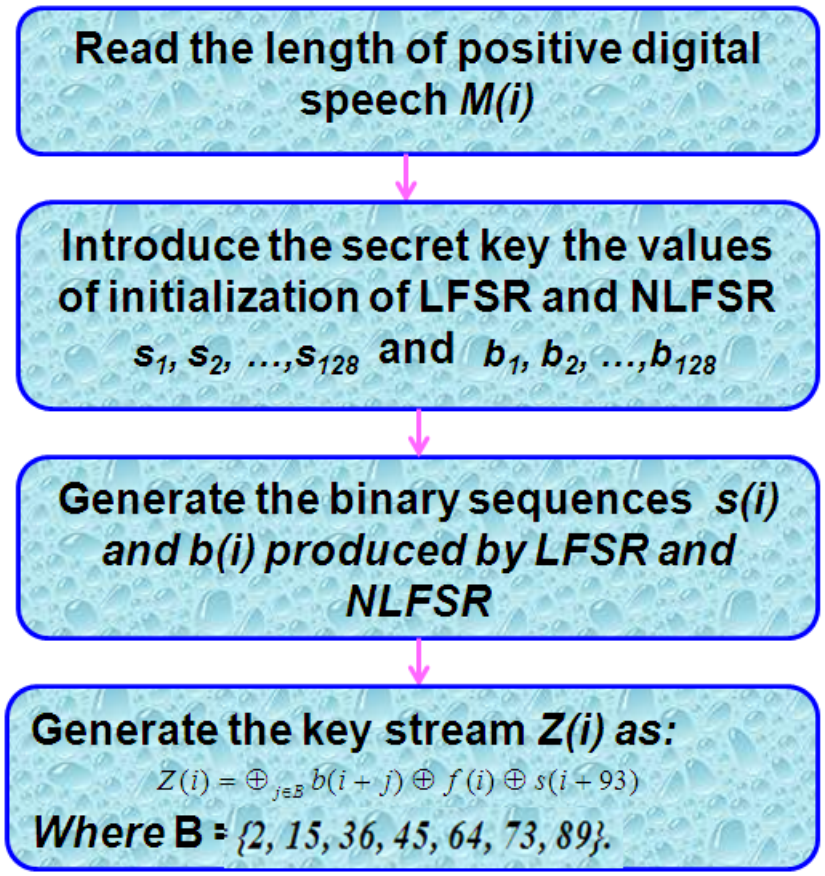

Figure 6: *KSG Flow Chart of Modified Grain-128.*

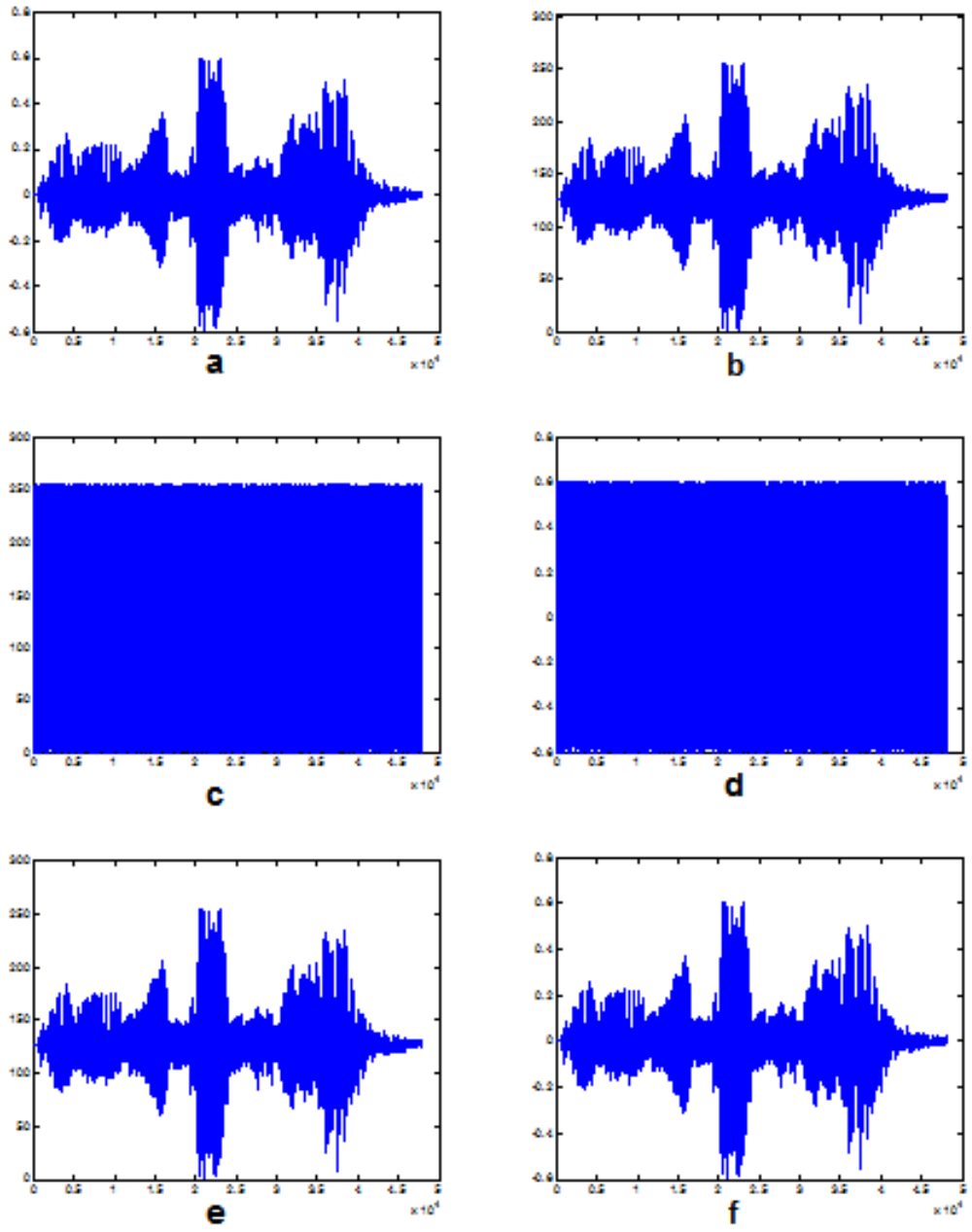

Figure 7: *Experimental Results for Speech 1 Using Modified Grain-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

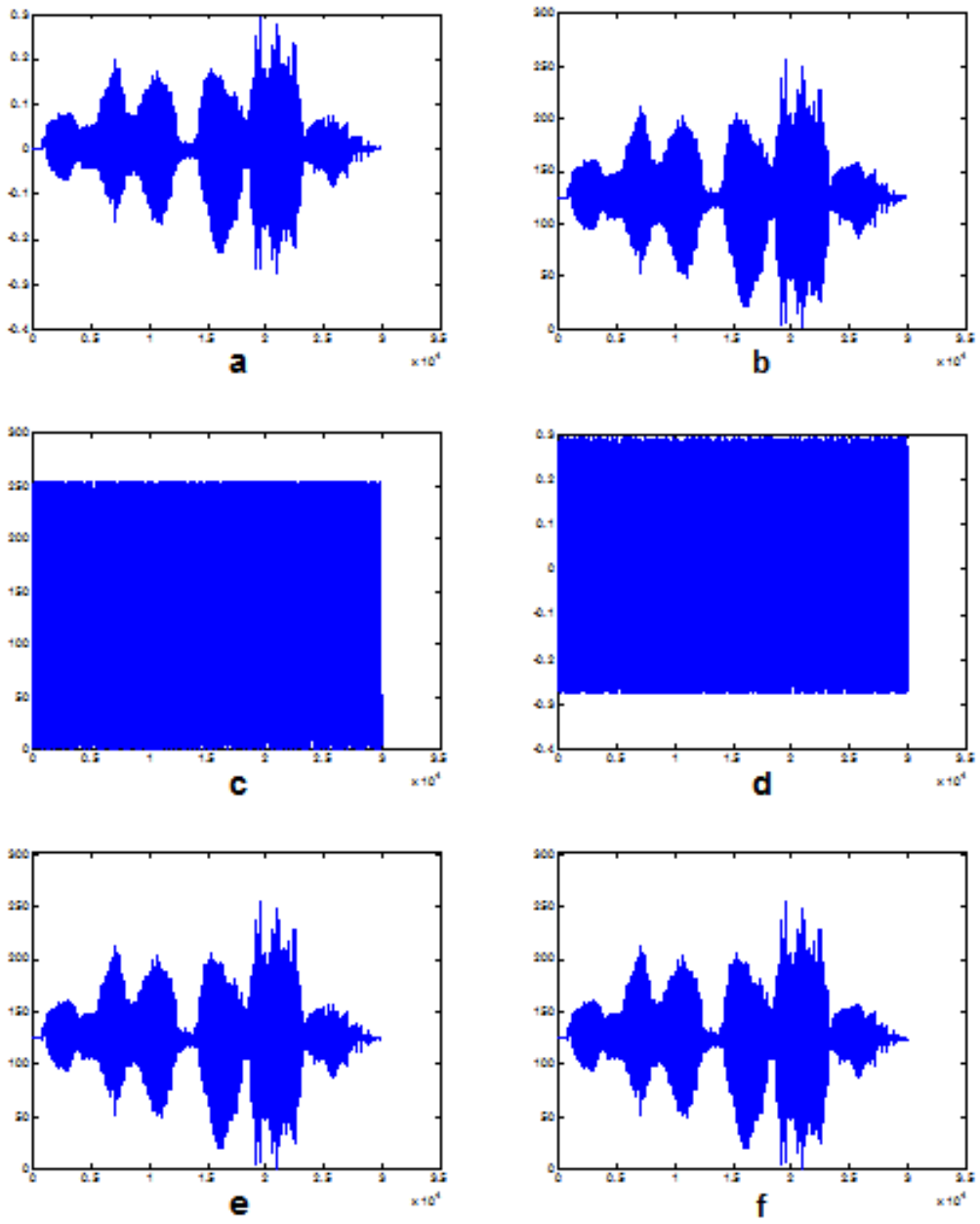

Figure 8: *Experimental Results for Speech 2 Using Modified Grain-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

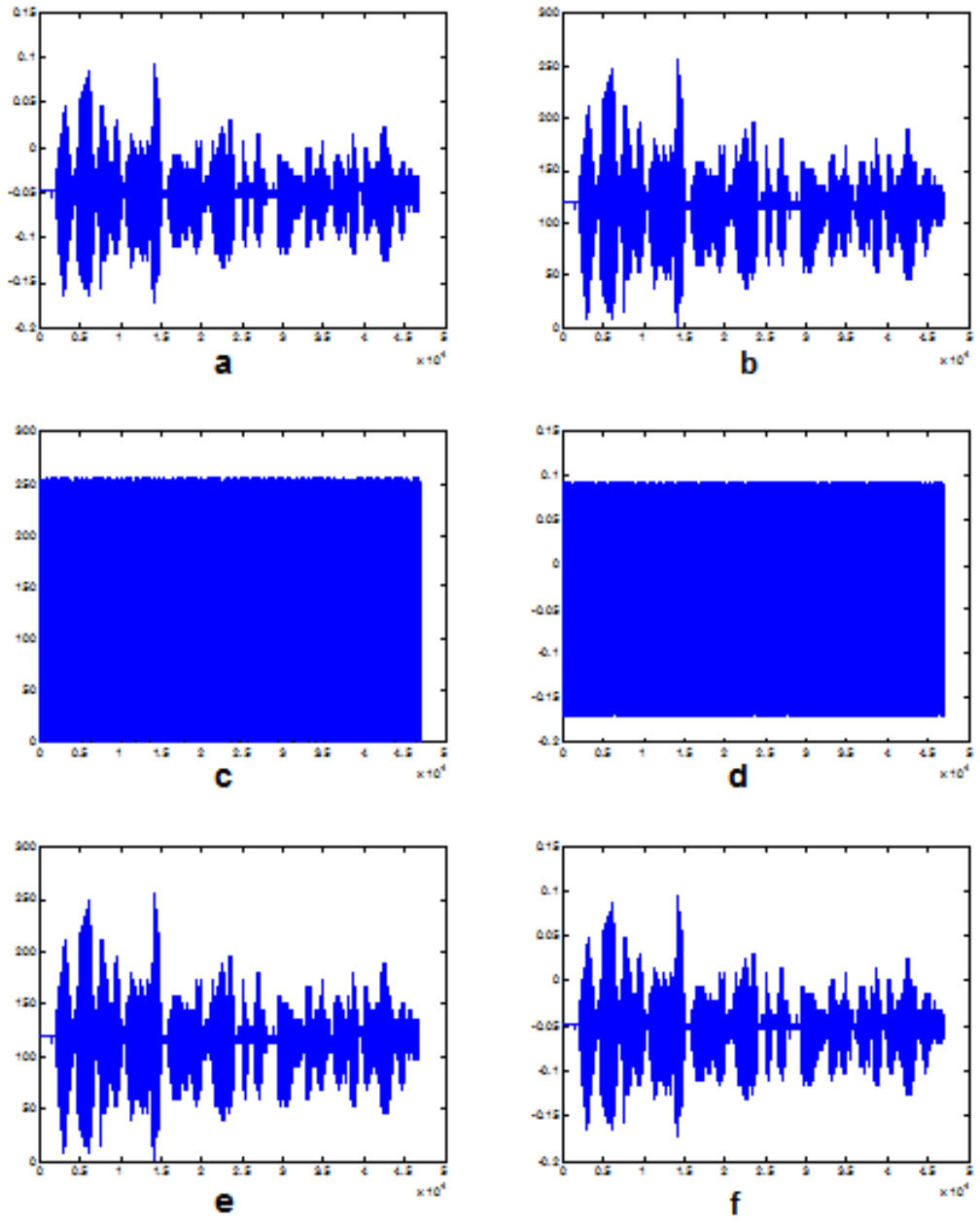

Figure 9: *Experimental Results for Speech 3 Using Modified Grain-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

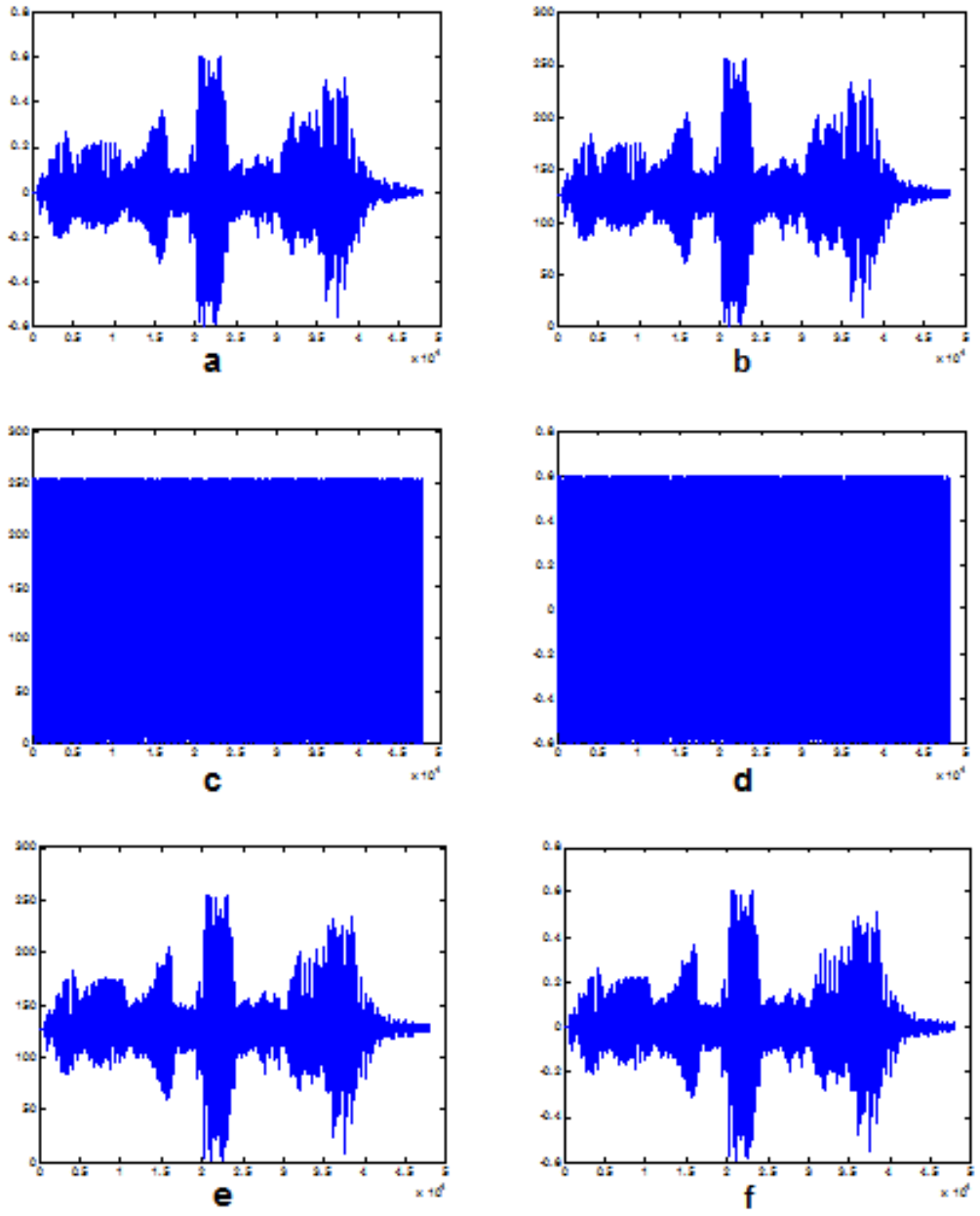

Figure 10: *Experimental Results for Speech 1 Using Graine-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

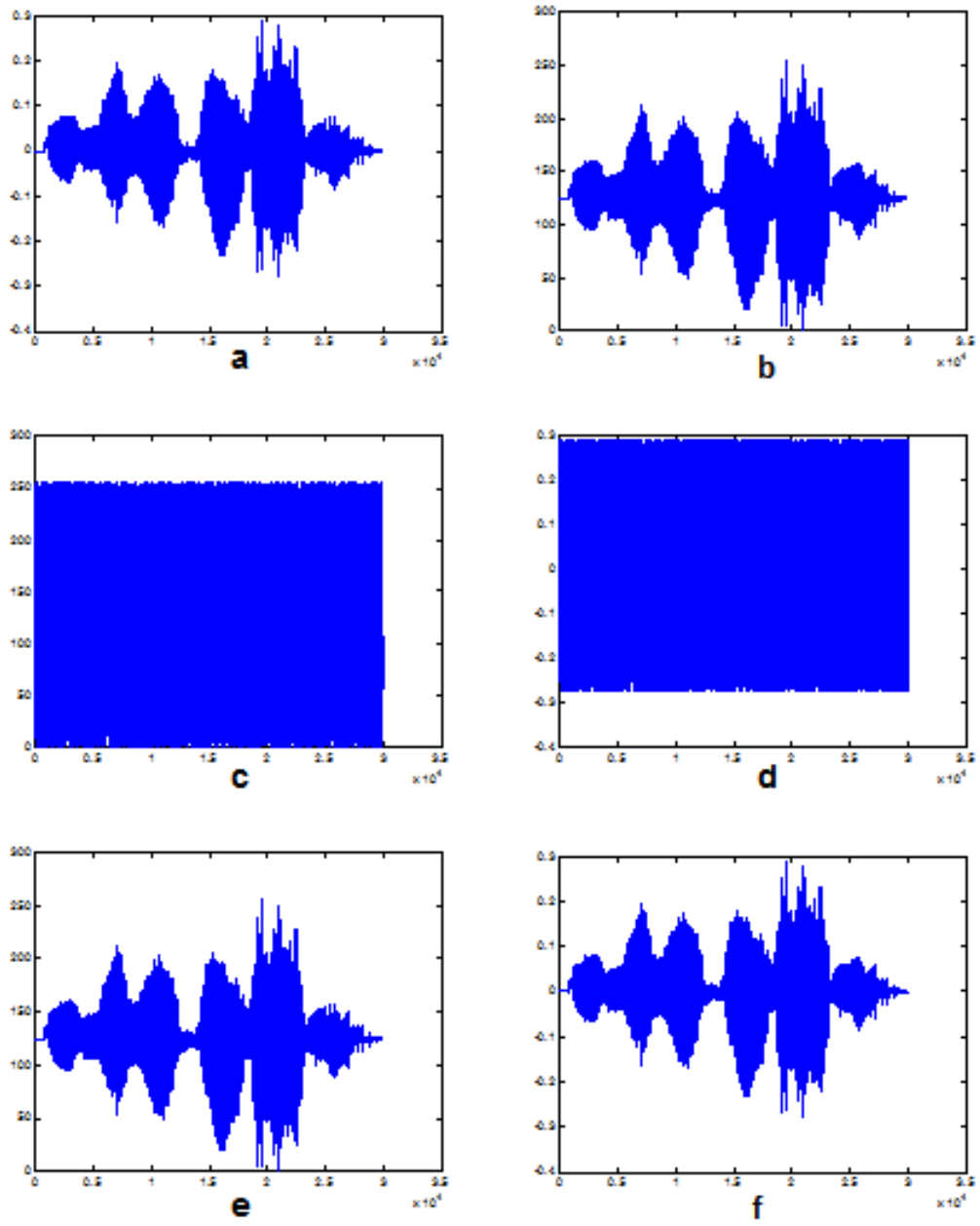

Figure 11: *Experimental Results for Speech 2 Using Graine-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

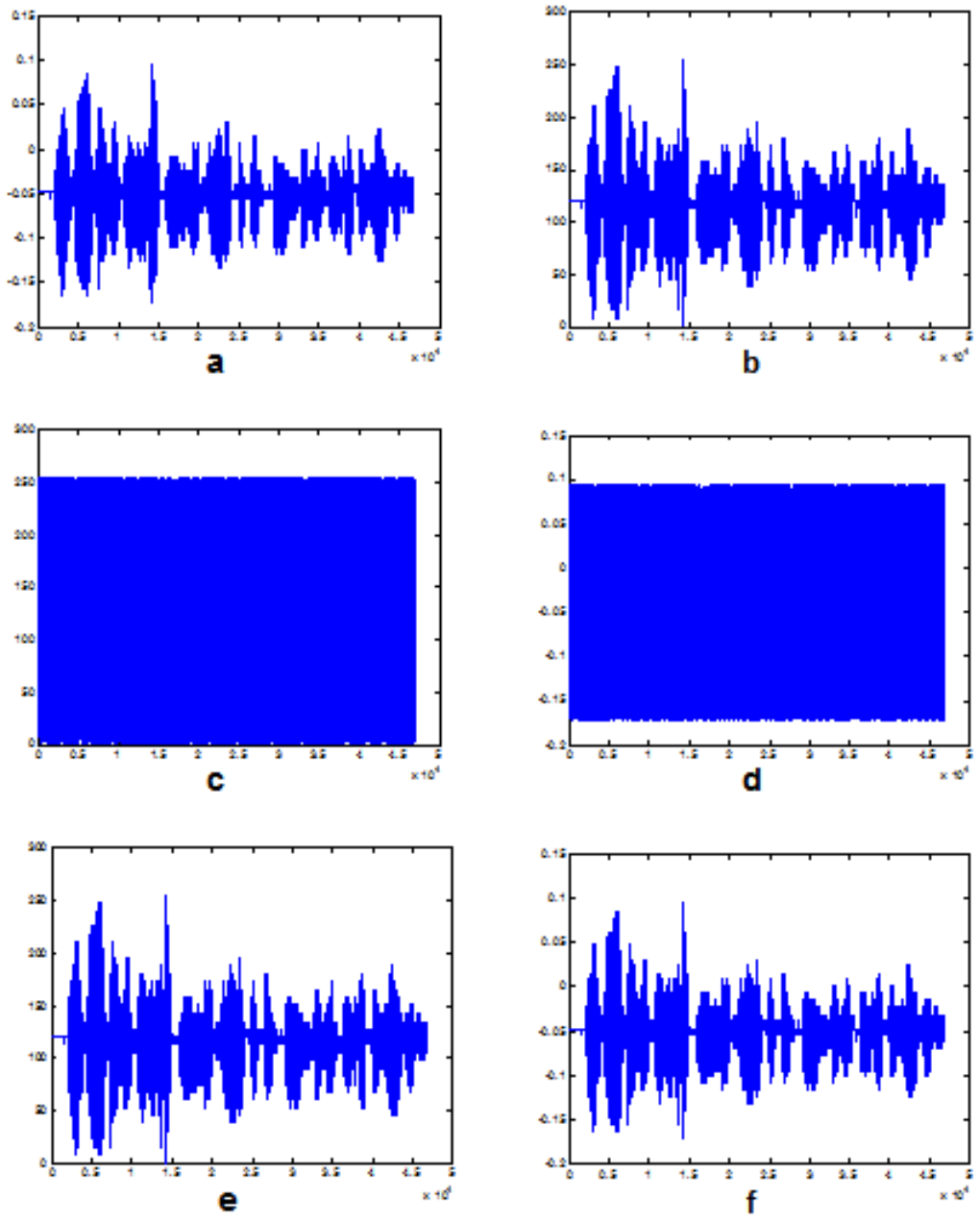

Figure 12: *Experimental Results for Speech 3 Using Graine-128: (a) original speech, (b) positive speech of original speech, (c) encrypted positive speech, (d) encrypted speech of original speech, (e) decrypted speech of encrypted positive speech, (f) decrypted speech.*

7 Conclusion

The main objective of this research work is to encrypt and decrypt speech data. In this work, a modified Grain-128 was introduced. Simulations were carried out for three different speeches. The test indicates that the encrypted speeches were very different than the original speeches. This method is very simple, fast to implement for either the speech encryption or the speech decryption.

Comparison of the proposed scheme and the original Grain-128 is investigated for different speeches. The test indicates that, the results given by the modified Grain-128 scheme are better than the results given by the original Grain-128. The proposed scheme needs some improvement regarding its possible vulnerability to algebraic attack. In future work, we intend to enhance the security of the scheme in respect to algebraic attack.

Competing Interests

The authors declare that no competing interests exist.

References

[1] Rahman Md. M, Saha TK, Bhuiyan Md. A. Implementation of RSA algorithm for speech data encryption and decryption. IJCSNS International Journal of Computer Science and Network Security. 2012;12(3):74-82.

[2] Merit K, Ouamri A. Securing speech in GSM networks using DES with Random permutation and inversion algorithm, International Journal of Distributed and Parallel Systems (IJDPS). 2012;3(4).

[3] Musheer A, Bashir A, Omar F. Chaos based mixed Keystream generator for voice data encryption. International Journal on Cryptography and Information Security (IJCIS). 2012;2(1).

[4] Kohad H, Ingle VR, Gaikwad MA. Security level enhancement in speech encryption using Kasami sequence. International Journal of Engineering Research and Applications (IJERA). 2012;2:1518-1523.

[5] Ashtiyani M, Moradi Birgani P, Karimi Madahi SS. Speech signal encryption using chaotic symmetric cryptography. Journal of Basic and Applied Scientific Research. 2012;1668-1674.

[6] Berlekamp ER. Algebraic coding theory. Mc Grow-Hill, New-York; 1968.

[7] Massey JL. Shift register synthesis and BCH decoding. IEEE Transactions on information Theory. 1969;Vol IT 15:122-127.

[8] Siegenthaler T. Decrypting a class of stream ciphers using Cipher text only. IEEE Transactions on Computers. 1985;C-34, N(1):81-85.

[9] Meier W, Staffelbach O. Fast correlation attacks on stream Chiper. In Advances in cryptology-EUROCRYPT'88, d. Par GNTHER (C.G), Lectures Notes in Computer science Springer Verlag. 1988;N(430):301-314.

[10] Courtois N, Meier W. Algebraic attacks on stream Ciphers with linear feedback. Advances in Cryptology EUROCRYPT 2003, Lecture Notes in Computer Science, Springer. 2656, 2003, 345-359.

[11] Courtois N. Fast algebraic attacks on stream Ciphers with linear feedback. Advances in cryptology CRYPTO 2003, Lecture Notes in Computer Science, Springer. 2729, 2003, 177-194.

[12] Hell M, Johansson T, Meier W. Grain - a stream cipher for constrained environments. Technical Report 2005/010, ECRYPT eSTREAM; 2005.

[13] Hell M, Johansson T, Meier W. A stream Cipher proposal: Grain-128. In IEEE International Symposium on Information Theory (ISIT 2006), 2006.

[14] Carlet C. On the cost weight divisibility and nonlinearity of resilient and correlation immune functions. Proceeding of SETA01 (Sequences and their applications 2001). Discrete Mathematics, Theoretical Computer Science. Springer. 2001;131-144.

[15] Hell M, Johansson T, Meier W. Grain: a stream cipher for constrained environments. IJWMC. 2007;2(1):86-93.

[16] Dalai DK. On some necessary conditions of Boolean functions to resist algebraic attacks, Theses of Doctorat. Applied Statistics Unit Indian Statistical Institute Kolkata, India August; 2006.

[17] Edwin L. Key. An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Transactions on Information Theory. 1976;22(6):732-736.

[18] Amparo FS, Pino CG. On the linear complexity of nonlinearly Filtered Pn-Sequences, In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, Advances in Cryptology, ASIACRYPT'94, LNCS 917, 1995, 8090. Springer Verlag.

[19] Biryukov A, Shamir A. Cryptanalytic Time/Memory/Data tradeoffs for stream Ciphers. Asiacrypt 2000, Springer Verlag, LNCS. 1976;1-13.

Appendix

In this section we provide few basic concepts and definitions introduced in this paper. By F_2 we denotethe the set $\{0, 1$ and we denote by F_2^n the set of all n-tuples from F_2. A Boolean function on n-variable may be viewed as a mapping from F_2^n in to F_2. The Hamming weight $wt(f)$ of a Boolean function f on F_2^n is the size of its support$\{x \in F_2^n;\ f(x) = 1\}$.

An n-variable Boolean function f has a unique algebraic normal form (A.N.F):

$$f(x_1, \cdots, x_n) = a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{1 \leq i \prec j \leq n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\ldots n} x_1 x_2 \cdots x_n$$

, where the coefficients a_0, a_i, $a_{i,j}, \cdots a_{1,2,\ldots,n}$ belong to F_2.

The algebraic degree, deg(f), of Boolean function f, is the number of variables in the highest order term with non zero coefficient. The Walsh transform of an n-variable Boolean function f computed as

$$\widehat{\mathrm{f}}(u) = \sum_{x_2^n} (-1)^{f(x) \oplus u \cdot x}. \tag{7.1}$$

where $u \cdot x = u_1 x_1 \oplus \cdots \oplus u_n x_n$, denotes the usual scalar product of vectors u and x. A Boolean function f on F_2^n is balanced if and only if $wt(f) = 2^{n-1}$. A function f is m-th order correlation immune if and only if its Walsh transform of f satisfies: $\widehat{\mathrm{f}}(u) = 0$, for $1 \leq wt(u) \leq m$, where $wt(u)$ denotes the Hamming weight of u, and f is balanced if moreover $\widehat{\mathrm{f}}(0) = 0\ \forall u \in F_2^n, 0 \leq wt(u) \leq m$. A balanced m-th order correlation immune function is called m-resilient. The nonlinearity $\mathcal{N}(f)$ of an n-variable Boolean function f, can be written as:

$$\mathcal{N}f = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |\widehat{\mathrm{f}}(u)|. \tag{7.2}$$

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=1069&id=5&aid=8546