International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 6 ǁ 2021 ǁ PP. 01-09

Speech Encryption Using Meitei Lock Sequence Generated from Standard Hash Functions

Yumnam Kirani Singh
C-DAC Silchar, Ground Floor, IIPC Building, NIT Silchar Campus, Assam, India

Abstract
Proposed here is a secure and fast speech encryption scheme based on generalized Vigenere cipher and Meitei Lock Sequence (MLS) generated from standard hash functions. An MLS is a random like sequence of any desired length generated from a chosen fixed length password. Use of MLS as key stream enhances the tightness or the search space of the key. Encryption and decryption are performed using the random look-up tables of the generalized Vigenere Cipher and are very fast. We consider random encryption and decryption of generalized Vigenere ciphers of size 266x256, 512x512, 1024x1024 to encrypt digital speech signal of 8-bit, 9-bit and 10 bit resolutions. To test the tightness of the encryption scheme, we compute the correlation coefficients between the original signal and the encrypted signals using different passwords. Also, the correlation coefficients between the original signal and signals decrypted with slightly different passwords. The correlations are found to be negligibly small indicating that there are no trace of similarity between the original signal and the encrypted signals, original signal and the decrypted signals with wrong passwords. In other words, the proposed scheme is a secure speech encryption scheme.

Keywords: *Correlation Coefficients, Generalized Vigenere Cipher, Hash Functions, MD5, SHA-1, SHA256, SHA512, Meitei Lock Sequence, Signal Distorter, Speech Encryption, Symmetric Cryptography*.

Date of Submission: 25-05-2021 Date of acceptance: 07-06-2021

I. INTRODUCTION

Encryption is the process of encoding information in unintelligible form so that only authorized people can render it intelligible through a process called decryption. Encryption and decryption is performed with the help of a key or keys. If the same key or keys are used for both encryption and decryption process, the cryptosystem is known as symmetric key crypto system. If the key or keys used for encryption is or are different from the key or keys used for decryption process, the cryptosystem is known as asymmetric key crypto system. Security of a cryptosystem is dependent on the difficulty of guessing or derivability of the key. The more the search space of the key, the more secure is the cryptosystem. For example, 128-bit key cryptosystem is considered less secure as compared to 512-bit or 1024-bit key cryptosystem because the key search space is more for longer keys. There are numerous standard encryption schemes such as DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), AES (Advanced Encryption Standard) for encrypting textual information. But these symmetric key cryptosystems are not suitable for suitable for encrypting highly correlated data like images and speech signals [4]. Also, the public key cryptosystems such as RSA or Elliptic Curve Cryptography (ECC) are not suitable for encryption of speech signals because they are too slow to be used in encryption of large volumes of data contained in a speech signal. Another problem for public key cryptosystem is that the volume of data becomes tremendously large after encryption. In speech encryption the main problem is that trace of original speech waveform remains intact in the encrypted signal or in the signal decrypted with wrong passwords. As a result, when such a signal is heard original content of the sound can be also heard embedded in noise. The main objective of the most of the speech encryption scheme to generate the encrypted signal without residual intelligibility. In order to encrypt a speech signal, the correlation of the speech samples in the original signal need to be reduced significantly before applying any encryption scheme or during the encryption process. That is, speech encryption requires an effective distorter function or scrambler [3, 5] to de-correlate the sample data in a speech signal. Several reversible transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [23], Discrete Wavelet Transform (DWT) [4], etc. are used as a distorter function for speech encryption. But the problem of using these reversible transforms as distorter functions is that trace of original signal appears even when decryption passwords are quite different from encryption password. Many researchers suggest the use of different chaotic mapping functions as distorter for speech encryption. In [6], Hato and Shihab used three dimensional chaotic maps of the Lorenz and Rossler chaotic system to generate a keystream. The actual encryption is done using substitution and permutation process based on the generated keystream. As compared to one-dimensional logistic map, it has

more parameters to generate the keystream as a result key search space is more. In [7], two different chaotic maps are used- Arnold cat map for sample permutation and Henon map for key generation which in turn generate a key mask and used in substitution of samples. In [8], Zhao H, et al. suggested speech encryption scheme based on dual random key streams in which one-time pad signal and another random signal generated from Chen Lee chaotic system are used to generate encrypted signal by mixing the three signals i.e., speech signal, one time-pad signal and signal from Chen Lee chaotic system. For decryption it used BSS method to approximate the speech signal. In [10], speech encryption using one-time pad signal and decryption using BSS method is proposed. Liu et al., [9] proposed encryption scheme using confusion and diffusion based on multi-scroll chaotic system. In [11] a new stream key generator Hybrid Discrete Continuous Chaotic System (HDCCS) based on continuous and discrete chaotic systems is proposed and provides an easy and robust chaos synchronization while decrease the degradation due to finite precision during a digital implementation and claimed that proposed speech cryptosystem is highly secure and has a very powerful diffusion and confusion mechanisms widely used in conventional cryptograph. In [13] circle Map and modified rotation equations are used for generating pseudo random numbers and then use permutation and substitution of speech samples based on the generated random numbers. Logistic Map, Henon Map and Baker Map chaotic functions [14] are used in combination with DCT or DST to develop a speech encryption scheme. Sathiyamurthi and Ramakrishnan [16] used Bernoulli's chaotic map for constructing encryption algorithm. In [19] original speech is encoded using a nonlinear function of the chaotic states of Lorenz map - use two channels to transmit the cipher texts and the synchronization signal separately.

A broad review of the chaotic map cryptosystems has been provided in [12], in which the author has the opinion that all chaos-based cryptographic algorithms use dynamical systems defined on the set of real numbers, and therefore are difficult for practical realization and circuit implementation. Some others methods have also been suggested for speech encryption. Abdalla [1] suggested a speech encryption method based on bit shuffling of the audio samples. In [2], segments of analog speech samples are distorted using principal component analysis as a process of encryption and the decryption is the approximation of the signal by finding the inverse of the eigen values. Public Key cryptography schemes – RSA [24] and Elliptic Curve [18] have also been used for encryption of speech signal. In [25] a Linear Feedback Shift Register is used to generate pseudo random numbers as key stream and encrypt the speech samples by using XOR operation as distorter function. Many other recent methods or approaches of speech encryption are discussed in [15].

In this paper, an encryption scheme for speech or audio signal is proposed which is simple fast and secure. The encryption scheme does not require any distorter function or chaotic mapping. It is based on generalized Vigenere cipher [22] which uses random look-up tables for encryption and decryption. This makes the decryption process as fast as encryption process. The random lookup table of the generalized Vigenere cipher acts as distorter. Moreover, it uses MLS (Meitei Lock Sequence) [20], [21], [22], which can be considered as one-time pad lock to secure the encryption scheme. An MLS is a random sequence of any desired length generated from a positive array having two or more elements. The MLS's can be generated from the recursive call of hash functions from any randomly chosen password. As SHA function can take any size input, the search space for password is infinitely large. This will make the brute force search for password impossible because the password length is not fixed. In most of the papers on speech encryption, more attention has been given on the correlation between the encrypted and original signal, which is important from the eavesdropping point of view. But the analysis on decrypted signals with passwords closely similar to the encryption password is also equally important. If the trace of the original signal is present in the signal decrypted for some different passwords, then encryption scheme is no longer secure. The security of an encryption scheme also depends on the traceability of the original speech sound from the decrypted speech for different keys. The proposed encryption scheme has been tested for traceability of the original speech signal from the decrypted signals by using decryption passwords which are slightly different from the encryption password. It is found that there is no trace of original speech in the decrypted speech when there is any slight difference in the password. The correlation coefficients of the original speech and decrypted speeches of wrong passwords have been computed and they are found to be negligibly small. This indicates that the proposed encryption scheme is secure in which getting the original speech from the encrypted speech is only possible when the decryption password is exactly same as the encryption password.

II. GENERATION OF MLS FROM HASH FUNCTIONS

Meitei Lock Sequence (MLS) is a random like sequence of any desired length which can be generated from a positive array having two or more elements. The randomness of the MLS has been tested in [20] to find any periodic repetition of any part of the sequence. It was found that no periodic repetition occurred in a generated MLS from any given password array. As MLS can be of any length, it can be used in combination with Vigenere Cipher to provide a secure encryption scheme. The weak point of Venenere Cipher was the use of periodic key sequence. As a result, periodic patterns appear in the cipher text from which tracking of the

encryption key or the deciphering of the cipher text is possible. Using MLS as key string in Vigenere Cipher removes its weakness [21]. In a cryptographic system if the password can be guessed or traced through mathematical or statistical analysis, it cannot be considered as a secure encryption scheme. Hash functions such as MD5, SHA1, SHA256, SHA512 [26] which generate hash code of particular length from a given input can be used to generate a secure password string like MLS from which tracing of input is impossible. In this paper, we are using MD5 and the SHA algorithms SHA1, SHA256 and SHA512 by recursively calling them to generate an MLS of desired length. These hash functions take an input of any length and gives an output of fixed length known as hash value or message digest. When there is any slight change in the input, the generated hash value is drastically changed. This property is used to check for message or data integrity. This property is desired to generate an MLS. Although, MD5 and SHA1 are considered for now insecure for used as message digest, both can be securely used for MLS key stream generation. Because in MLS, longer sequences are generated from shorter sequence and hence there is no issue of collision of generated hash codes. More information hash functions and message authentication can be found in [27]. Unlike hash value, the length of an MLS is not fixed which may be as long as the length of the signal to be encrypted. So, to generate MLS from hash function, we first generate a hash value from a hash function using an input of shorter length known as password. The whole hash value or some portion of it is then used as input to generate next hash values. The process continues until the combined length of the generated hash values becomes equal to or greater than the desired length. The steps for generating an MLS sequence from a hash function is given below.

Steps for generating MLS from a Hash function

1. Compute M, the number of data samples in the speech signal
2. Find L, the length of the hash code generated by the hash function
3. Find N =Ceiling(2*M/L), the number of times a hash function is to be repeated to generate at least M random values.
4. Choose an input password array P of length 2 or more
5. Assign K to an empty array to hold the generated MLS
6. Generate the hash code of a particular hash function from the password array P
7. Convert the hash code to integer sequence by taking two successive characters
8. Concatenate the integer sequence to K
9. Use hash code integer sequence or some elements of the sequence as next password array P
10. Repeat step 6 to 9 for N times

The generated key sequence K will have length equal to M or more. If length of the sequence K is more select only the first M or last M samples so that it length becomes equal to the length of the input sequence. The generated MLS will have the range 0 to 255 as two hash code characters are combined to form a random sample in K.

The MLS generated from hash functions are quite random in nature and there is no trace of periodicity in the generated MLS. The waveforms of the MLS sequences generated from the same password 11111 from four different hash functions MD5, SHA1, SHA256 and SHA512 are shown in Fig. 1, Fig.2, Fig.3 and Fig.4 respectively.

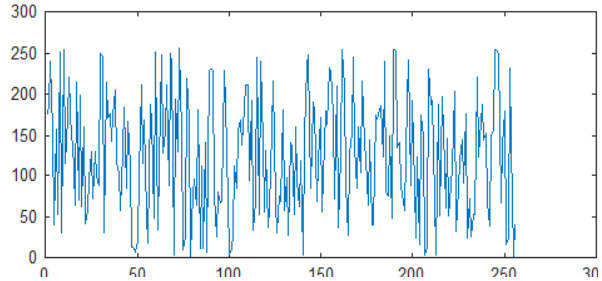

Figure-1: MLS MD5 using password 11111

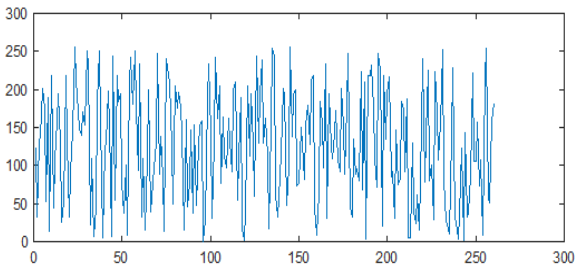

Figure-2: MLS from SHA1 using password 11111

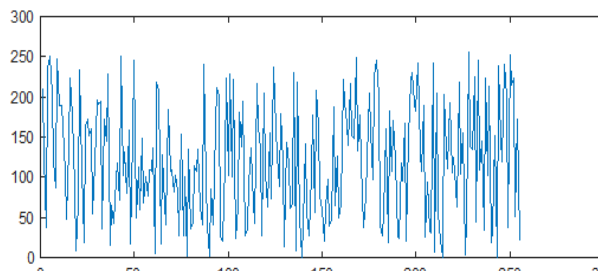

Figure-3: MLS from SHA256 using password 11111

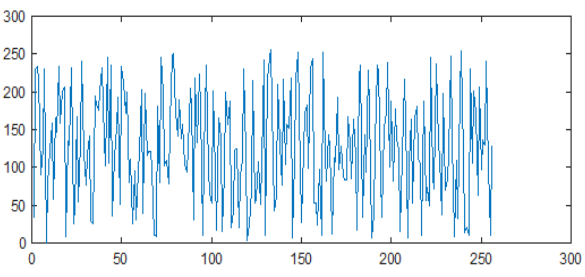

Figure-4: MLS from SHA512 using password

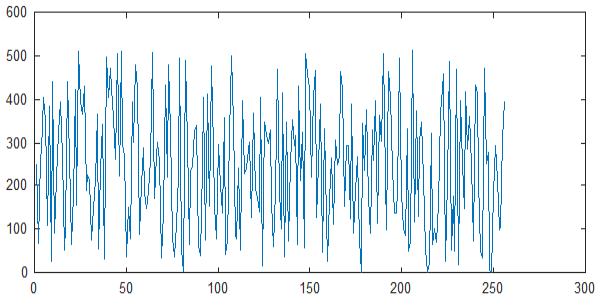

Figure-5: MLS of SHA1 with range 1 to 512 generated by range normalization of Figure-1.

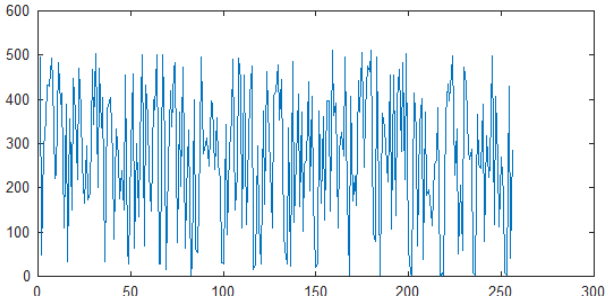

Figure-6: MLS of SHA1 with range 1 to 512 generated by combining 9-successive bits.

From the figures, it is clearly seen that the generated sequences from the same password 11111 are random in nature and there is no trace of periodic repletion in any part of the generated sequence. Such feature is desirable for generating a key sequence for use in a secure encryption scheme.

Usually, the generated MLS having 8-bit random values are suitable for encrypting 8-bit or lower data samples. The quality of speech in 8-bit resolution is considered poor. Good quality speech data samples are coded in higher resolutions such as 9-bit, 10-bit or higher. To encrypt such speech samples in higher resolution, the generated MLS should also be in that range. That is, for 9-bit speech samples has the range is 1 to 512, so MLS to encrypt such speech samples should have the range 1 to 512. Similarly, to encrypt speech samples in 10-bit resolution, the generated MLS will have the range 1 to 1024.

There are two possible ways to increase the range (from 1 to 256) of MLS generated from hash function to higher range. One way is to extend the range directly using range normalization method. Another method is to convert the MLS to binary string and then combine k successive bits to get k-bit resolution data of MLS. If can of rang normalization, the waveform is similar to that of 8-bit sequence and in the case of combining successive bits, the generated waveforms are different from the 8-bit sequence. Fig.5 shows the MLS having the range 1 to 512 by normalizing the range of MLS of SHA1 shown in Fig.2. It can be seen that the two have similar waveform patterns except the difference in the range. Another MLS having the range 1 to 512 by combining successive 9 bits from the MLS of Fig.2 is shown in Fig.6. It can be clearly seen that the waveform of MLS in Fig.6 is very different from the waveform of Fig.2 from which it is generated. We will be using successive bit combination method for range enhancement for generating higher range MLS for encryption of speech samples greater than 8-bit. It may be noted that when using bit combination method to generate MLS of higher resolution, the length of the sequence should be adjusted appropriately.

III. GENERATION OF RANDOM ENCRYPTION AND DECRYPTION TABLES

In original Vigenere cipher which was developed as polyalphabetic cipher to encrypt textual data uses a 26x26 square of 26 alphabets (i.e, A-Z) shifted sequentially and the same table is used for encryption as well as decryption. The encryption process is quite fast but decryption is quite slow because during decryption search or matching operation is performed. Another problem in the Vigenere cipher was the use of periodic sequence as password. This caused periodic patterns appear in the cipher text and gave clue to determining password length and tracing of the password. To strengthen the Viginere cipher keeping its simplicity intact, generalized vigenere cipher was proposed [22], in which random tables and non-repeating password strings are used. Use of random tables in encryption and decryption strengthen and fasten the encryption and decryption process. In addition, use of MLS for generating random password string enhances the tightness of security significantly. The beauty of the generalized Vigenere cipher is that the size and the content of the random tables used for encryption are not fixed. Any square matrix whose rows or columns are unique can be used as encryption table and the decryption table can be easily obtained from it by finding the invertible matrix as described in [22], which is as follows.

Suppose, E is the encryption table having the size QxQ whose rows are unique.

Then, the decryption table D can be generated from E as

D(I, E(I,J))=J

Where I=1, 2, 3 , …, Q and J=1, 2, 3, …, Q.

Similarly, we can easily obtain decryption tables from the encryption tables whose columns are unique.

For image encryption, we can use a random table of size 256x256, where each row is unique and consists of integers from 1 to 256 in random order. For speech signal, we may also use 512x512 and 1024x1024 random square matrices as encryption tables in which each row or column is unique and consists of 1 to 512 and 1 to 1024 random orders. The random table 256x256 can be used for encryption of 8-bit resolution speech samples and the quality of the speech may be poor. For encryption 9-bit and 10-bit speech samples, the random

tables of 512x512 and 1024x1024 need to be used. For encryption of higher-bit speech resolution, appropriate random tables having higher range must be used.

Fig.7 shows the random encryption table of size 256x256 and the corresponding decryption table is shown in Fig.8. From these two tables, it can be seen that the contents in the tables are totally random and there is no trace of periodicity in either of the tables. When the 8-bit speech samples are encrypted using the random encrypted table in Fig.7, the encrypted speech signal becomes a random signal without any trace of the original speech waveform. Similar is the case for decryption. When an encrypted signal is decrypted with different password sequence using the random decryption table in Fig.8, the decrypted signal becomes unintelligibly random. For other random tables, 512x512 and 1024x1024, they cannot be displayed as a gray scale image as their ranges are much beyond 8- bit gray scale image and hence they are not shown. However, the encryption table of 512x512 table having range 1-to 512 is shown in figure-9 as gray scale image to show the randomness of the table.

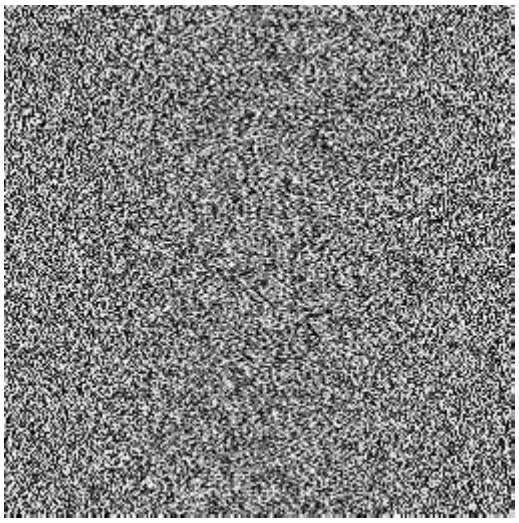

Figure-7: Random Encryption Table (256x256)

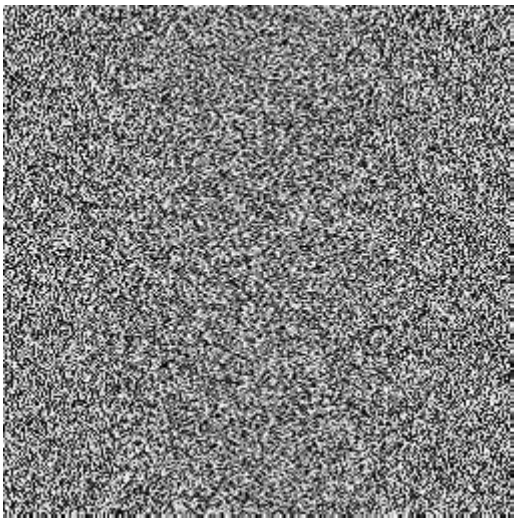

Figure-8: Random Decryption Table (256x256)

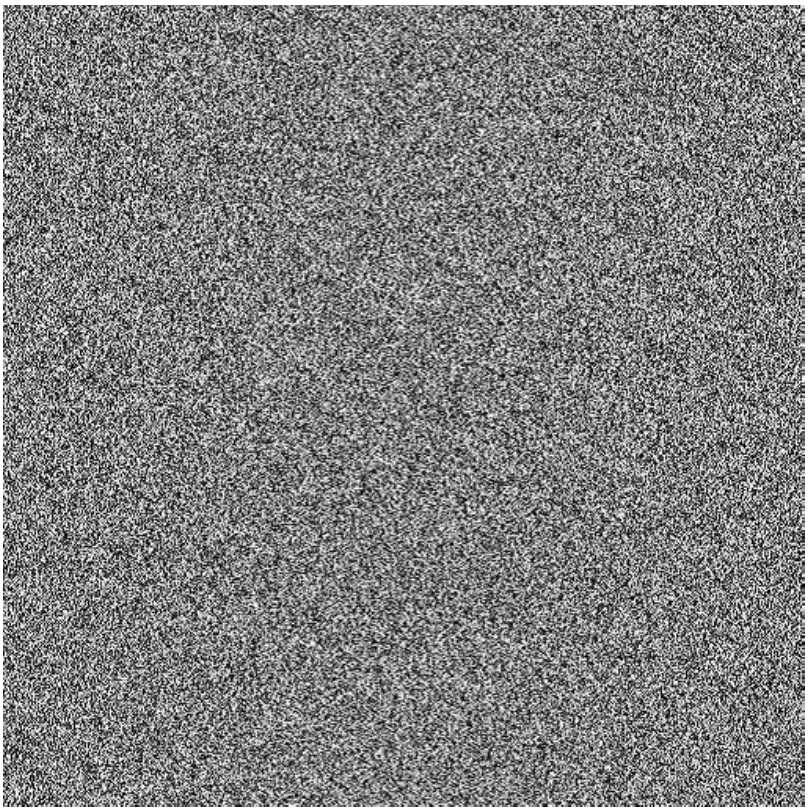

Figure-9: Random Encryption table (512x512)

IV. SPEECH ENCRYPTION AND DECRYPTION USING MLS

Here, we will be using generalized Vigenere cipher [22] for encrypting and decrypting speech or audio signal. As speech signals are highly correlated data, we need to use a highly randomized encryption and decryption table along with the MLS key stream generated from the hash functions. In generalized Vigenere cipher, any random table whose rows or columns are unique can be used as encryption table. We can generate infinitely many such random tables which once generated cannot be generated again. For image encryption, the random table of size 256x256 is sufficient but for speech encryption the size of the random table may be larger depending on how many bits are used to represent a speech sample, i.e., 512x512, 1024x1024 for 9- and 10-bits speech samples. Once the size of the encryption table is fixed and the corresponding random table is generated, then the encryption is performed based on this random table but not from the speech samples. In other words, the encrypted speech data are formed by the values of the random encryption table. So, there is hardly any correlation between original speech and encrypted speech, i.e., there is no visible or distinguishable speech waveform of the original speech in the encrypted speech. This avoids the necessity of using any distorter function or chaotic map in the speech encryption using generalized Vigenere cipher. The process of encryption using Vigenere cipher is very simple, just like using a look-up table. This makes the encryption scheme very fast as in the original Vigenere cipher.

It may be noted that encryption table has a specified range. The original speech signal must also be mapped in that range. For using 256x256 random encryption and decryption tables, the speech signal must be mapped to 1 to 256. Similarly, for using 512x512 and 1024x1024 random tables, the speech signal must be mapped respectively to 1 to 512 and 1 to 1024. The encrypted and decrypted signal will also be in the range of random encryption and decryption tables used. To play the sound the encrypted and decrypted signals, they must be converted in the range of -1 to 1.

Let E be the encryption table, S is the speech signal of length M mapped in the range of E, K is the key sequence generated from a password P. Then, the encrypted speech C, is obtained as

K=MLS(M, HashName, P)

C=E(S,K)

Where MLS is the Meitei Lock Sequence algorithm, HashName is the name of the hash function i.e., MD5, SHA1, SHA236 or SHA512 which will be used in generating the key sequence K.

The process of decryption is also very simple and fast. It uses a decryption table D derived from the encryption table E. The process how the decryption table is derived from encryption table is described in [22]. These two tables (E and D) are cryptographically inverse to each other. That is, any one of them can be used for encryption or decryption. When one is used for encryption, the other must be used for decryption. So, if D is the decryption table corresponding to the encryption table E, then the original signal S can be obtained from encrypted speech C using the following relation.

S=D(C, K)

It may be noted as D and E cryptographically inverse to each other that the role of D and E may be exchanged to perform encryption and decryption in generalized Vigenere cipher. That is, D can be used for encryption and E for decryption. So, the encrypted signal C can be obtained from D as

C=D(S, K)

And the original signal S can be obtained C by using E as

S=E(C,K)

This exchangeability of encryption and decryption scheme can be expressed as

S=D(E(S,K),K)

S=E(D(S,K),K)

That is, either of D, or E can be used for encryption or decryption. If one is used for encryption the other should be used for decryption.

Another important feature that makes the proposed encryption scheme highly secure is the use of MLS key string K as the key for encryption. The MLS key string K is generated from a password of any desired length greater than 1.i.e., there is no upper bound of the length of the key. So, the key search space is infinitely large and this makes it extremely difficult to apply brute force to search the password or tracing the password from the encrypted signal.

V. EXPERIMENTAL RESULTS

For experimentation, we consider the chirp signal available in MATLAB. The reason for choosing the signal is that the signal has periodic waveforms coresponding chirping frequency. Such a signal is difficult to encrypt to hide the visible of highly correlated regions . For experimentation, the original signal is mapped to 1 to 256, 1 to 512 or 1 to 1024 depending on whether the range of encryption table has range 1 to 256, 1 to 512, or 1 to 1024. Four different MLS's are generated from password 11111 using hash functions MD5, SHA1, SHA256 and SHA512 to encrypt the speech signal. The encrypted speech waveforms using these MLS's are

unintelligibly different from the original signal. The encrypted signal is a like a random noise signal in which no trace of the original signal is present. Fig.10 shows the original chip signal mapped 1 to 256 as 8-bit audio signal. This signal can be encrypted using encryption table 256x256 or larger. The encrypted speech signals in 8-bit, 9-bit and 10 bit samples using MLS key streams generated from MD5 hash function are shown respectively in Fig.11, Fig.12 and Fig.13. From these figures, it is seen that the original waveform is lost in the encrypted signal and there is no trace of intelligible information present in the waveform of the any of the encrypted signals. Similar is the case for the encrypted signals of 8-bit, 9-bit and 10-bit encrypted speech signals generated using MLS key streams generated from the hash functions SHA-1, SHA-256 and SHA512. The encrypted signals generated from SHA functions are not shown to save space in the paper. To measure the similarity between original speech i.e. chirp signal and the encrypted signals generated by different hash function, we compute the correlation between the mapped original signal of a particular bit resolution and encrypted signals generated by using the MLS key streams from different hash functions with same password. The password can be any alphanumeric string of any length greater than 1 including space. For the experimental purpose, we use simple password of five ones as for generating key streams from hash functions. This will enable us to find the decryption passwords close to the encryption password and analyze similarity between the original signal and the decrypted signals with close passwords. Table -1 shows the result of the encryption and decryption performed using the 256x256 random encryption table shown respectively in Fig.5 and Fig.6. The correlation coefficients between the mapped original signal and the encrypted signals generated with different hash functions are shown in the second column of Table-1. It is observed that correlation coefficients are negligibly small indicating that there is not much or any similarity between the original signal and the encrypted signals. The encrypted signals are then decrypted with passwords which are close to the encryption password 11111 to test whether any trace of intelligible sound of the original signal becomes apparent in the decrypted signals. The correlation coefficients are computed between the mapped original signal and the decrypted signals with MLS key streams generated from MD5, SHA1, SHA256, and SHA512 using passwords 11, 111, 1111, 11101, 111011 and 10111 are shown in 3rd to 9th columns of Table-1. It is seen that the correlation coefficients are negligibly small which indicate that there is no trace of information in the decrypted signals when there is any difference between the decryption and the encryption passwords.

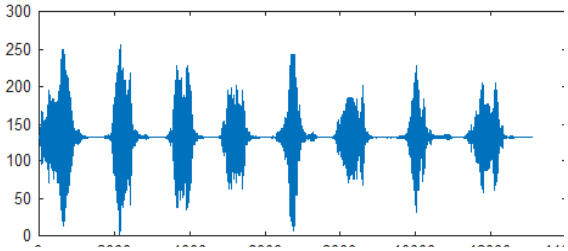

Figure-10: Original Chirp Signal

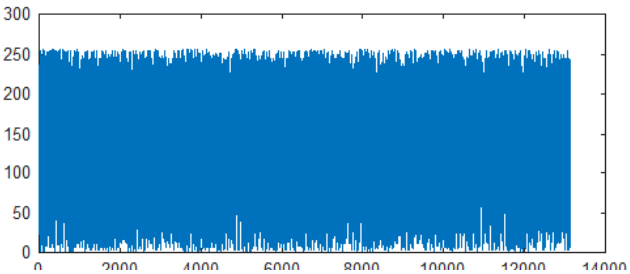

Figure-11: Encrypted Chirp signal in 8-bit samples

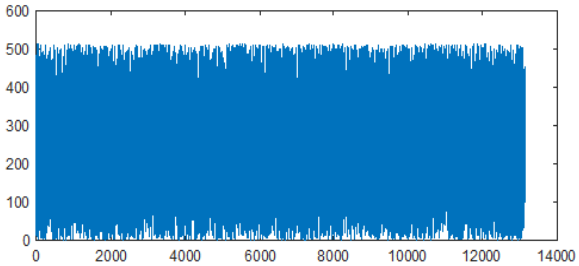

Figure-12: Encrypted signal in 9-bit samples

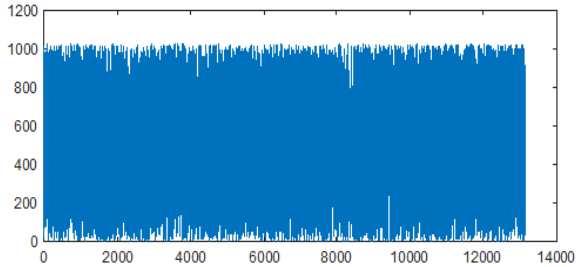

Figure-13: Encrypted Signal in 10-bit samples

Similar analysis conducted for encryption of 9-bit and 10 bit-speech samples (i.e., charp signal) when encrypted with 512x512 and 1024x1024 random encryption and decryption tables using the same encryption and decryption passwords in case of Table-1. The correlation coefficients between 9-bit and 10-bit audio samples and the encrypted and decrypted signals are shown respectively in Table-II and Table-III.

Table-1: Correlation coefficients of encrypted speeches and decrypted speeches using 256x256 random generalized Vigenere square.

MLS from Hash function	Correlation Coefficients between original speech and							
	Encrypted speech with password	Decrypted speeches with passwords						
	11111	11	111	1111	11110	11101	11011	10111
MD-5	0.0120	0.0103	-0.0061	0.0151	0.0064	-0.0118	-0.0080	0.0058
SHA-1	-0.0165	-0.0103	0.0198	0.0141	0.0121	0.0078	-0.0014	0.0033
SHA-256	-0.0048	-0.0122	-0.0044	0.0026	0.0041	0.0152	-0.0080	0.0073
SHA-512	0.0023	0.0037	-0.0109	0.0025	-0.0138	0.0227	-0.0066	0.0091

Table-1I: Correlation coefficients of encrypted speeches and decrypted speeches using 512x512 random generalized Vigenere square.

MLS from Hash function	Correlation Coefficients between original speech and							
	Encrypted speech with password	Decrypted speeches with passwords						
	11111	11	111	1111	11110	11101	11011	10111
MD-5	-0.0039	-0.0020	0.0064	-0.0040	-0.0066	0.0086	0.0052	0.0046
SHA-1	-0.0263	0.0055	-0.0016	0.0030	-0.0133	0.0060	-0.0099	-0.0099
SHA-256	0.0040	-0.0014	0.0095	0.0157	-0.0035	-0.0175	-0.0046	-0.0023
SHA-512	-0.0250	0.0003	-0.0006	0.0141	-0.0017	-0.0124	0.0145	-0.000043

Table-1II: Correlation coefficients of encrypted speeches and decrypted speeches using 1024x1024 random generalized Vigenere square.

MLS from Hash function	Correlation Coefficients between original speech and							
	Encrypted speech with password	Decrypted speeches with passwords						
	11111	11	111	1111	11110	11101	11011	10111
MD-5	0.0152	0.0137	-0.0160	-0.0058	0.0009	0.0123	0.0164	-0.0078
SHA-1	-0.0033	0.0006	-0.0044	-0.0053	0.0046	-0.0149	-0.0124	0.0090
SHA-256	0.0137	0.0035	0.0151	0.0008	-0.0029	-0.0028	0.0120	0.0026
SHA-512	-0.0054	0.0026	0.0131	-0.00011	0.0055	0.0036	-0.0125	-0.0103

From tables II and III, it is seen that the correlation coefficients between the original mapped signal and the encrypted signals are negligibly small indicating that there is hardly any similarity between the original signal and the encrypted signal. Also, the correlation between the original signal and the decrypted signal with close passwords are also negligibly small which indicates that there is hardly any similar trace of the original signal in the decrypted components with wrong passwords. We also computed the correlation coefficients between the original signal and the encrypted or decrypted signals after mapping them to -1 and 1, the correlation coefficients remain almost the same. The sound produced by the encrypted signals and decrypted signals from wrong passwords are just random noise of hissing sound without any trace original speech sound. So, without knowing the exact encryption password, there is hardly any possible way of tracing the original signal from the encrypted signal.

VI. CONCLUSIONS

A secure speech encryption scheme based on generalized Vigenere Cipher and Meitei Lock sequences generated from four standard hash functions has been described. The proposed scheme uses random encryption and decryption tables of generalized cipher which is more powerful than confusion and diffusion technique used in a secure encryption scheme and hence does not require any distorter function or chaotic map to de-correlate speech samples for encryption. The encryption scheme also uses MLS key strings generated from SHA functions, which significantly enhances the security level. Also, the use of random encryption and decryption tables makes the encryption and decryption processes very fast. As the encryption is based on random tables and random key sequence, the encrypted signals are random signals with no trace of intelligible sound of the original signal. Similarly, the decrypted signals become unintelligibly random when there is slight change in the decryption password. This makes the known cryptographic attacks such as cipher text only attack, chosen plain text attacks etc. impossible. Moreover, the search space for password is infinitely large which makes the brute force attack next to impossible. In short, the proposed signal encryption scheme is a simple, fast and secure encryption scheme.

REFERENCES

[1]. Tamimi, A.A.; Abdalla, A.M. An Audio Shuffle-Encryption Algorithm. In Proceedings of theWorld Congress on Engineering and Computer Science, San Francisco, CA, USA, Vol. 1, pp. 22–24 October 2014.

[2]. N. Abbas, "Speech scrambling based on principal component analysis," MASAUM Journal of Computing, Vol. 1, No. 3, pp. 452-456, Oct. 2009.

[3]. D.S. Anjana and M. Kuriakose, "Frequency speech scrambler based on hartley transform and OFDM algorithm," International Journal of Computer Applications, Vol. 61, No. 8, pp. 36-40, Jan. 2013.

[4]. A. S. Bopardikar, V. U. Reddy, "Speech Encryption Using Wavelet Packets". Bangalore, Indian Institute of Science, October 2005.

[5]. Yaoyao Chen, "End-to-end speech encryption algorithm based on speech scrambling in frequency domain", PLA Equipment Academy, Beijing, China, 101416 ; Jianhua Hao ; Jianbiao Chen ; Zibo Zhang Published in: Third International Conference on Cyberspace Technology (CCT 2015) Page(s):1 – 5

[6]. Hato, E.; Shihab, D. "Lorenz and Rossler Chaotic System for Speech Signal Encryption". Int. J. Comput. Appl., Vol 128, No. 11, pp. 25-33, 2015.

[7]. M. F. Abd-Elzaher, M. Shalaby, S. H. El-Ramly, "Securing modern voice communication systems using multilevel chaotic approach", International Journal of Computer Applications, Vol. 135, No. 9, pp. 17—21, 2016.

[8]. Zhao H, He S, Chen Z, Zhang X "Dual key speech encryption algorithm based underdetermined BSS", The Scientific World Journal 2014. doi: 10.1155/2014/974735

[9]. Liu, H.; Kadir, A.; Li, Y. Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. Optik , Vol. 127, pp. 7431–7438, 2016.

[10]. Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang,"A Blind Source Separation Based Method for Speech Encryption", IEEE Transactions On Circuits and Systems, Vol. 53, No. 6, pp. 1320-1328, ,June 2006.

[11]. Azzaz, M. S., Tanougast, C., Sadoudi, S., & Bouridane, A. "Synchronized hybrid chaotic generators: application to real-time wireless speech encryption". Elsevier: Communications in Nonlinear Science Numerical Simulation, Vol. 18, pp. 2035–2047, 2013.

[12]. Ljupco Kocarev, "Chaos-based cryptography: a brief overview", IEEE Circuits and Systems Magazine", Vol.1, No. 3, pp 6-21, 2002.

[13]. Krasimir Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution" Architecture, Electronics, Vol. 8, No. 5, 2019 https://doi.org/10.3390/electronics8050530

[14]. Alzharaa Mostafa, Naglaa F Soliman, Mohamoud Abdalluh, Fathi E Abd El-samie, "Speech encryption using two dimensional chaotic maps", IEEE Xplore, 11th International Conference on Computer Engineering (ICENCO), Feb 2016

[15]. S.Rajanarayanan and A. Pushparaghavan, "Recent developments in signal encryption- A critical survey"; International Journal of Scientific and Research Publications, Vol. 2, No. 6, pp. 1-7, 2012.

[16]. P. Sathiyamurthi, S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication", EURASIP Journal on Audio, Speech and Music Processing, December 2017, doi https://doi.org/10.1186/s13636-017-0118-0

[17]. Mohammed, R. S., & Sadkhan, S. B., "Speech scrambler based on proposed random chaotic maps", IEEE International Conference on Multidisciplinary in IT and Communication Science and Applications, Baghdad, pp. 1–6, 2016.

[18]. Priyanka, S. and Hemalatha, B. "Speech Data Encryption and Decryption Using Elliptic Curve Cryptography", International Journal of Research in Computer Science, Vol. 3, Issue 1, pp. 48-53, 2016.

[19]. Long Jye Sheu, "A speech encryption using fractional chaotic systems", Nonlinear Dynamics, vol 65, pp. 103-108, 2011.

[20]. Y. K. Singh, S.K. Parui, "Simplet and Its application in Signal Encryption", Multidimensional Systems and Signal Processing, Vol. 15, No. 4, pp. 375-394, October 2004.

[21]. Y. K. Singh, A Simple, fast and secure Cipher, ARPN Journal of Engineering and Applied Sciences, Vol. 6, No. 10, pp. 61-69, Oct. 2011.

[22]. Y. K. Singh, "Generalization of Vigenere Cipher", ARPN Journal of Engineering and Applied Sciences, Vol 7, No. 1, pp. 39-44. January, 2012.

[23]. Dalila Slimani, Fatiha Merazka, "Encryption of speech signal with multiple secret keys", Procedia Computer Science, Vol. 128, pp. 79–88 , 2018.

[24]. Sura F. Yousif, "Encrynption and Decryption of Audio Signal Based on RSA Algorithm", International Journal of Engineering Technologies and Management, Vol. 5, No. 7, July 2018.

[25]. Tin Lai Win, and Nant Christina Kyaw, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR) ", World Academy of Science, Engineering and Technology ,Vol. 48 , pp.462, 2008.

[26]. MD5, SHA-1, SHA256 and SHA512 generator https://passwordsgenerator.net/sha1-hash-generator/

[27]. Hashing for Message Authentication https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture15.pdf