A FOUR LEVEL SPEECH SIGNAL ENCRYPTION ALGORITHM

Harjinder Kaur and Gianetan Singh Sekhon

1M. tech. Student, department of computer engineering, Yadwindra collage of engineering, Punjabi university gurukashi campus, talwandi sabo, Punjab, India, E-mail: s.harjinder04@gmail.com ,
2Department of Computer Engineering, Assistant Professor of Yadavindra College of Engineering, PUGKC, Talwandi Sabo, Punjab, India, E-mail: Gianetan@gmail.com

ABSTRACT

In this paper, we present a novel speech encryption algorithm based on four level of hash based encryption. Our approach integrates a modified time domain scrambling scheme with an amplitude scrambling method which masks the speech signal with algorithmic based noise by specific mixing. In this, we use different algorithm to encrypt the speech signal at different levels i.e. we encrypt the original signal four times using different algorithm at each level. The output of one level makes the input of next level. As a result of this algorithm, the speech signal becomes more and more secure at each level.

Keywords: Encryption, decryption, PSNR value, speech signal, random number generator.

1. INTRODUCTION

Speech is the ability to speak or the act of speaking. Speech signal consists of number of bits. It contains both negative and positive bit values. Speech communications become more and more widely used and even more vulnerable, so the need to providing high level of security is dramatically increasing. To secure the speech signal variety of encryption algorithms are used. There are four speech encryption techniques used for speech security. Time domain scrambling, frequency domain scrambling, amplitude scrambling and two-dimensional scrambling combining frequency and time domain scrambling. Speech signal is encrypted in two forms digital and analogue encryption.

In our approach, we encrypt the speech signal at four levels means four time using different algorithms at each level. Output or encrypted signal of one level becomes the input for next level and so on. At last the encrypted signal of fourth level becomes the final output or encrypted signal for transmission. Last encrypted signal is a constant beep.

The resulting system can securely encrypt the speech files for the purpose of storing speech messages and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that it makes the encrypted speech sound a constant beep. The second advantage is that it does not impose any restriction on the decoding of the specific signal because with every new signal it produces a new hash accordingly. Our system is systematically evaluated, and it shows a high level of security with excellent audio quality. This paper is organized as follows. Section 2 explains the encryption process, Section 3 gives the result and analysis, section 4 gives the performance evaluation and section 5 gives a conclusion.

2. PRESENT WORK

This section presents an encryption of four level speech encryption algorithms. Fig 1 shows a block diagram of four level speech encryption systems.

It shows that input of each level algorithm are the encrypted signal of previous level and the final encrypted signal or encrypted signal of fourth level is the signal to transmit. Explanation of each level algorithm is given below:

2.1. At Level 1

At this level, original speech signal say voice 1 is encrypted using Repositioning of bits. Then encrypted signal of this level becomes the input for second level and so on. At last the encrypted signal of fourth level becomes the final output or encrypted signal for transmission. Last encrypted signal is a constant beep.

The resulting system can securely encrypt the speech files for the purpose of storing speech messages and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that it makes the encrypted speech sound a constant beep. The second advantage is that it does not impose any restriction on the decoding of the specific signal because with every new signal it produces a new hash accordingly. Our system is systematically evaluated, and it shows a high level of security with excellent audio quality. This paper is organized as follows. Section 2 explains the encryption process, Section 3 gives the result and analysis, section 4 gives the performance evaluation and section 5 gives a conclusion.
2.2. At Level 2

To encrypt the signal voice 2, Random Number Generator is used at this level. Steps for this are given below:

(i) For each bit value of voice 2, random number is generated using random number generator.

(ii) Now each bit value is subtracted from random number generated in previous step.

(iii) Resultant value of step 2 is encrypted signal say voice 3 and random number is key for decryption.

Random Number Generator generates values between ranges –32767 to 32767.

If signal bit value is positive then the random no. is generated between 0 to 32767.

Else, the random no. is generated between –32767 to –1.

2.3. At Level 3

Now encrypted signal of level 2 say voice 3 becomes the input for this level. Same random number generator used at level 2 is used at this level. Same algorithm used at level 2 to encrypt the signal, is used at this level to add more security. By doing this, cryptanalysis of the speech signal becomes difficult and the signal becomes more secure to use for military purposes.

Now the encrypted signal say voice 4 of this level using same algorithm, becomes the input for next level.

2.4. At Level 4

Speech signal voice 4 is encrypted using Amplitude Ascending Order at this level. Steps are given below:

(i) Find the minimum value of the signal bits.

(ii) Put it into [row column] matrix.

(iii) Replace the above value in signal find in step 1 with 32767 so that loop not replace for same bit.

(iv) End when all bit values become 32767 and key used for decryption is actual [row column] place of bits.

Encrypted signal of this level say voice 5 is the final output of the system. This signal is more secure than previous signals. This signal is a constant beep.

Reverse procedure is used for the decryption of the signal and at last we get an original speech signal.

3. RESULT AND DISCUSSION

The original Speech signal recorded for duration 5 second. Results shows that, each level encrypted signal is more secure than previous level signal and each encrypted signal is used as input for next level. Fourth level encrypted signal is the final output of the system. This level signal is more secure than previous level signals.

4. PERFORMANCE EVALUATION

At the time of World War 2, when secure communication was paramount to the US armed forces, noise was simply added to a voice signal to prevent enemies from listening to the conversations.
Negative PSNR value indicates noise contaminated data. [9] It means encrypted signal is more secure. The fourth level encrypted signal is more secure than previous encrypted signals. Because it sounds like a beep.

Five different signals are recorded for duration of 5s.

4.1. Noise measurement
There exist no absolute scale for noise but rather all noise is measured relative to the measurement. Signal to noise ratio is used to measure noise in signal. [10]

\[
\text{SNR} = 10 \log_{10} \left( \frac{\sum s^2(n)}{\sum [s(n) - \hat{s}(n)]^2} \right)
\]

4.2. Power Signal to Noise Ratio
PSNR compares the level of desired signal to the level of background noise. Encrypted signal’s sound is very noisy, having a negative PSNR. [9] So the encrypted signal is more secure then original signal.

\[
\text{PSNR} = 10 \log_{10} \left( \frac{\max (A)}{\text{MSE}} \right)
\]

\[
\text{MSE} = \frac{1}{N} \sum \text{err}^2
\]

A = samples of original signal.

Table 1 Shows the Table of PSNR Values of Five Different Signals Recorded for Duration of 5 Second

<table>
<thead>
<tr>
<th>No. of different signals</th>
<th>PSNR at level 1</th>
<th>PSNR 2 at level 2</th>
<th>PSNR 3 at level 3</th>
<th>PSNR at level 4</th>
</tr>
</thead>
</table>

Graph shows that the psnr value at fourth level is lesser than that of level 3. it means the security is increased up to level 3 but dropped at level 4.

4. CONCLUSION
We have described a four level speech signal encryption algorithm. The results show that the proposed algorithm has a high level of security and good audio quality. It encrypts the original signal four times using four different algorithms which makes the cryptanalysis a difficult task and increases the security of the speech signal. Reverse process is used to decrypt the signal and provides a good audio quality after the decryption of encrypted signal.

In other hand, it was observed that the security of the signal improved at every level up to level 3 but at level 4, the security dropped because the PSNR value at this level is lesser than that of the PSNR value at level 3. it was observed for sample of 5 signals of 5 second duration. By this, it can safely be concluded that the encryption be done up to level 3 level four encryption can be left out if there is time constrain.

REFERENCES