A METHOD FOR ENCRYPTING AND DECRYPTINGWAVE FILES

Mohamad M. Al-laham[1], Mohamad a. Mai'iteh[2], Hasan Rashaideh[3], Ziad Al-Qadi[4]

[1&2]Department of MIS, Al-Balqa Applied University, Jordan
[3&4]Department of computer science, Al-Balqa Applied University, Jordan

ABSTRACT

This paper aims at presenting a novel method for encrypting and decrypting wave files. Basically, the target files are sound files. First, the files are fetched, then a two-dimensional matrix of the double data type is created to maintain the values that correspond to the sample range; these values are placed in a column matrix then they are kept in the two dimensional-matrix already created. The double 2D matrix will be encrypted using matrix multiplication with a private double matrix key [1]. Having been encrypted, the data will be sent in wave file format and decrypted using the same 2D matrix private key.

KEYWORDS

security, encrypting, decrypting, wave files.

1. INTRODUCTION

Waveform Audio File Format (WAVE) is an application of RIFF or Resource Interchange File Format which stores audio bit streams in “chunks”. Linear Pulse Code Modulation (LPCM) format is used to encrypt WAVE [2] [3]. The Sound is a pressure wave or mechanical energy characterized by pressure variance in an elastic medium. The variance propagates as either compression the pressure exceeds the ambient pressure or as reification when pressure is less than the ambient pressure. In the same manner, a WAVE file just represents the sampled sound waves which happen to be above or below the equilibrium or ambient air pressure. In this paper, one and two channels of wave files will be used to show the proposed technique of encrypting the sound file in various matrix formats [4][5]. The most popular characteristics used to analyze wave files are:(1) Estimating the mu of the Population(mu), (2) Estimating Sigma, (3) Peak Factor (Crest Factor), (4) Dynamic Range, (5) Power Spectral Density, and (6) Zero-Crossing Rate.

The rest of this paper are is organized as follows: in section 2 we introduce a basis on how to analyze wave files. Our proposed method is presented in section 3. Section 4 presents the experimental environment. Section 5 presents and discusses the results. Finally, conclusions are drawn in section 6.

2. WAVE FILE ANALYSIS

2.1. ESTIMATING THE MU OF THE POPULATION(MU)

Figure 1 shows an overview of all the relationships. In step 1, in the upper left-hand corner of Figure 1, Sampling Distribution of the Mean (SAQ) is conducted as a normal distribution. In step 2, we do a research project on spatial ability. This is equivalent to taking a sample of size(n)from this population of SAQ scores. So, in step 3 a statistic on the sample data is calculated. Hence, we calculate the mean [6].

The estimate of the population means mu is the sample mean. Unfortunately, it gets messier by estimating population variance as shown in Figure 1.

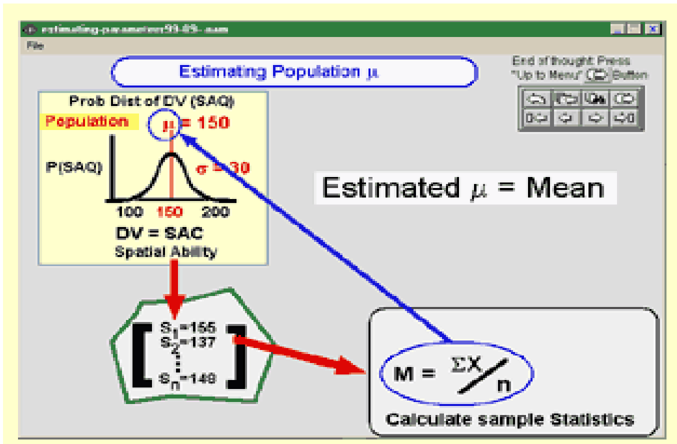

Figure 1. Calculating mu Parameter

2.2. ESTIMATING SIGMA

The standard deviation, sigma, is the next parameter to be estimated. The formula shown in Figure 2 is used to calculate an estimate of the population standard deviation (sigma) from sample [7].

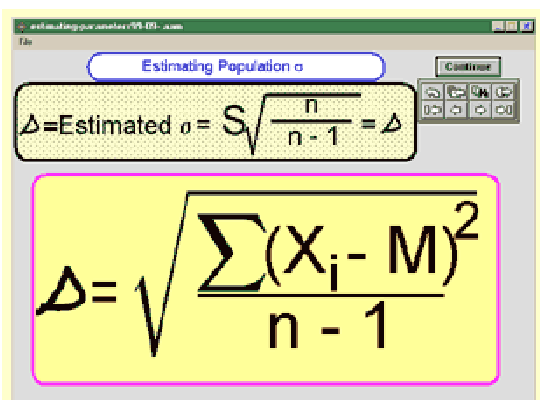

Figure 2. Calculating Sigma Parameter

2.3. Peak Factor (Crest Factor)

The crest factor of an audio signal is defined as the dB difference between the peaks and the Root Main Square (RMS) value of the signal. The RMS is defined as the "heating value" of the signal- the voltage that would generate the same heat as a DC (Direct Current) signal- over the same time [8]. RMS value of a complex signal must be read with an RMS voltmeter. Alternatively, the signal can be digitally sampled, and the samples are summed to yield the RMS value. Furthermore, the RMS value of a complex signal can be calculated from the "area under the curve" of a signal.

2.4. Dynamic Range (DR)

DR, or DNR, is defined as the ratio between the largest and smallest possible values of a changeable quantity, such as in signals like sound and light. It is measured as a ratio, or as a base-10 (decibel) or base-2 (doublings, bits or stops) logarithmic value [9].

2.5. Power Spectral Density (PSD)

For continuous signals that describe, for example, stationary physical processes, it is more convenient to define a Power Spectral Density (PSD). It describes how the power of a signal or time series is distributed over different frequencies, as given in the previous simple example. Also; here, power can be the real physical power, or more often, for convenience with abstract signals, can be defined as the squared value of the signal [10][11].

2.6. Zero-Crossing Rate

The Zero-Crossing Rate is defined as the rate of sign-changes along a signal, i.e., the rate at which the signal changes from positive to negative or vice versa. This feature has been heavily used in both speech recognition and music information retrieval; being a main feature to classify percussive sounds [12].

3. The Proposed Technique to Wave Files Encryption/ Decryption

Wave files can be treated as one column matrix (mono sounds: one channel) or two columns matrix (stereo sounds: two channels). The proposed technique is based on this idea and consists of two phases: Phase 1: Encryption and Phase 2: Decryption.

3.1. Encryption Phase

This phase will be implemented as shown in figure 3 by applying the following steps:

I. Capture the original wave file.
II. Calculate the wave file size.
III. If the wave file size is not a square number, increase the size to the nearest square number.
IV. Pad zeros to the wave file if the size is increased.
V. Convert the wave file to a 2D square matrix.
VI. Generate a 2D double matrix to be used as a private (secret) key.
VII. Apply matrix multiplication to get the encrypted matrix.
VIII. Resize the encrypted matrix, and then change the2D matrix to a1D matrix to get the encrypted wave file.

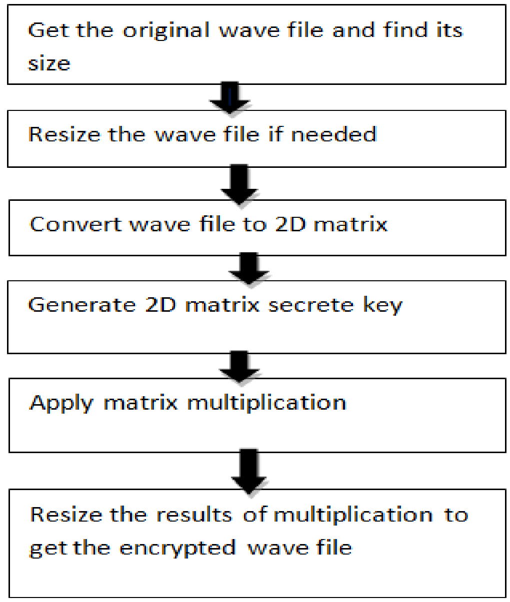

Figure 3. Encryption Phase

3.2. Decryption Phase

This phase will be implemented as shown in figure 4 by applying the following steps:

I. Get the encrypted wave file.
II. Calculate the encrypted wave file size.
III. If the decrypted wave file size is not a square number, increase the size to the nearest square number.
IV. Pad zeros to the encrypted wave file if the size is increased.
V. Convert the encrypted wave file to a2D square matrix.
VI. Use the inverse of the secret key as a private key.
VII. Apply matrix multiplication to get the decrypted matrix.
VIII. Resize the decrypted matrix, and then change the2D matrix to a1D matrix to get the decrypted original wave file.

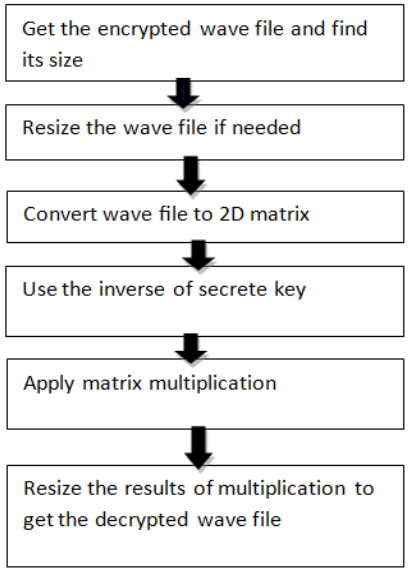

Figure 4: Decryption Phase

4. EXPERIMENTAL ENVIRONMENT

To analyze the proposed technique, the following tools are used:

- The Personal computer (i7 processor with 4Gbyte RAM)
- MATLAB package.
- MATLAB programs and functions to be used for variant methods of analysis and for encryption and decryption.

5. EXPERIMENTAL RESULTS

During the implementation, we focus on the issues in the following subsections.

5.1 ACCURACY:

Accuracy means approaches zero error between the original wave file and the decrypted one to make sure that there is no loss of information during the process of encryption-decryption. The proposed technique is implemented and tested several times using deferent wave files with deferent sizes and channels. Each time of testing, the correlation coefficient among the original wave file and the decrypted one and the value of the correlation coefficient is always zero, which means that the decrypted wave file 100% matches the original wave file.

Table 1 shows some sample values of the original, encrypted and decrypted files:

Table 1. Sample Values of the Wave File

Original	Encrypted	Decrypted
0	0.2587	0.0000
-0.0078	0.8213	-0.0078
-0.0078	0.6926	-0.0078
-0.0078	-0.0491	-0.0078
-0.0078	-1.1681	-0.0078
-0.0078	-1.7954	-0.0078
-0.0078	-1.8709	-0.0078
-0.0078	-1.7097	-0.0078
-0.0078	-1.6803	-0.0078
-0.0078	-1.8099	-0.0078
-0.0078	-1.1020	-0.0078
-0.0078	0.0670	-0.0078
0	1.3161	-0.0078
-0.0078	1.6382	-0.0078
-0.0078	0.8977	-0.0078

The original wave file and the decrypted one are graphically represented using deferent forms and Figures 5 and 6 show that the original file and the decrypted one are the same.

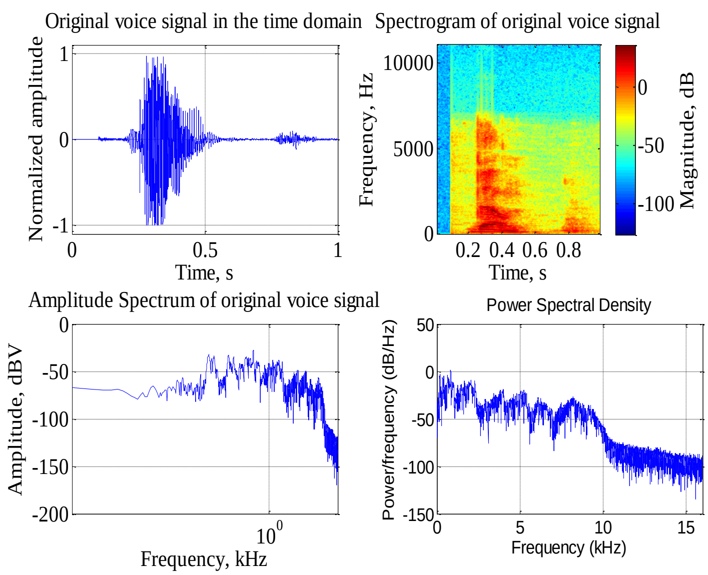

Figure 5. Representation of the original wave file

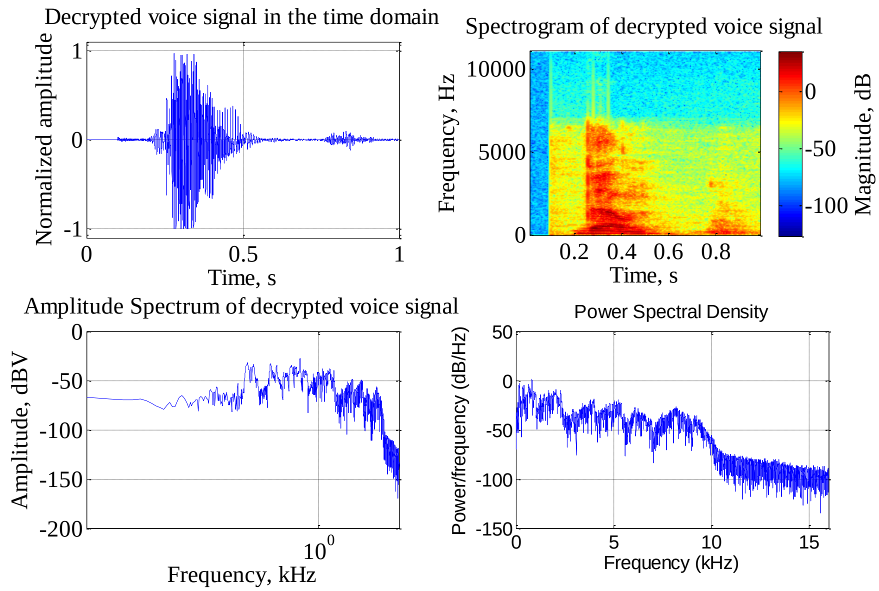

Figure 6. Representation of the Decrypted Wave File

The most popular characteristics of the wav file are calculated for the original file and the decrypted one and they are always the same. Table 2 shows sample:

Table 2. Sample of Wave File Characteristics

File	Sigma	Mu	Peak (crest) Factor Q	Dynamic Range D	psdl	Zero Crossing
Original Wave	0.18886	1.9571e-05	14.477 dB	90.2216 dB	0.0063	700
Decrypted Wave	0.18886	1.9571e-05	14.477 dB	90.2216 dB	0.0063	700

5.2 Security

Information Security is the process of protecting data from unauthorized access, disclosure, destruction, modification and disruption. The common goals of information security are: protecting the confidentiality, integrity, and availability of information. However, there are some slight differences between them. The proposed technique uses a very huge 2D matrix with double values as a private (secret) key for encryption and decryption. This key will be generated randomly and saved, and it is very difficult, or even impossible, to hack or guess it as shown in the next example:

Hacking Time Calculation Example:

Suppose we have the following random double matrix to be used for encryption-decryption:

```
PrivateKey =

    0.8147    0.9134    0.2785
    0.9058    0.6324    0.5469
    0.1270    0.0975    0.9575
```

- The probability of guising each digit (P) $=1/10^4$
- The probability of guising the 9 digits (PP) $=1/10^{4\times 9}=10^{-36}$
- For the best case: the number of guising = 10^{36}
- For the worst case: the number of guessing=1
- The average number of guessing=$(1+10^{36})/2 \sim 5 \times 10^{35}$
- Suppose the matrix multiplication requires 10^{-9} seconds, so the hacking time will be:

$5 \times 10^{35} \times 10^{-9} = 5 \times 10^{26}$ sec $= 5 \times 10^{26}/60 = 8.3333\times10^{24}$ min$= 8.3333\times10^{24}/60=1.3889\times10^{23}$ hours $= 1.3889\times10^{23}/24= 5.7871 \times10^{21}$ days$=5.7871 \times10^{21}/365.25=1.5844\times10^{19}$ years

The calculation results lead us to conclude that it is impossible or even very hard to hack the key which is always greater than 3 by 3 random matrix.

5.3 Efficiency

The proposed technique is implemented using different wave files with different sizes. Each time the encryption/decryption time is calculated, and some samples of time calculation are listed in table 3:

Table 3. Encryption-Decryption Time

Wave File Size(MB)	Encryption\Decryption Time (Millisecond)
0.022051	15
0.589824	168
18.690480	6194
1.214400	294
5.400000	854
10.00000	1281
20.00000	7105
30.00000	11237

From the results in Table 3, we find out that the results of the different sizes of wave files vary proportionally to the size of wave file. Encryption time increases as the file size increases in multiples of file size. The implementation results are compared with the results in [13] as shown in Table 4 and Figure 7.

Table 4:Encryption Time Comparisons

File Size(MB)	Proposed Technique	DES(1)	Blowfish(2)
10	1281	7566	34010
20	7105	10424	64195
30	11237	15211	82230

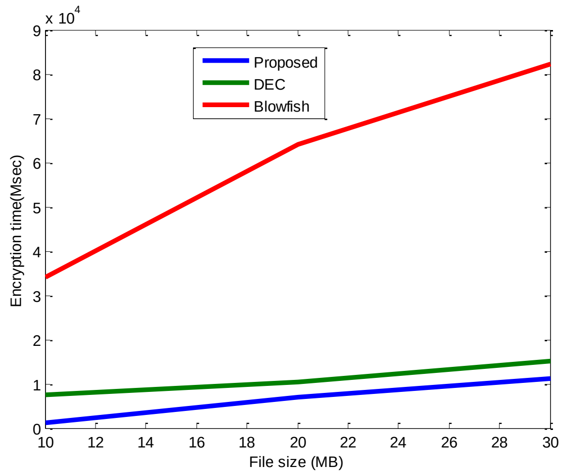

Figure 7. Comparison Results

From table 4, we can compare the proposed technique results with the results of the other two methods by calculating the speedup as shown in table 5:

Table 5:Speedup Calculation

File Size(MB)	**Speedup with (1)**	**Speedup with (2)**
10	5.9063	26.5496
20	1.4671	9.0352
30	1.3537	7.3178
Average Speedup	2.9090	14.3009

6. CONCLUSIONS

An efficient and secure technique for wave file encryption- decryption is proposed, implemented, tested and compared with the other method of encryption-decryption and from the obtained results we can conclude the following:

- The proposed technique can easily be used to encrypt-decrypt both mono and stereo wave files with any size.

- The proposed technique is very secure and it is hard or even impossible to hack the private key.

- The proposed technique provides zero error; thus, there is no loss of information during the process of encryption-decryption.

- The proposed technique is very efficient being compared with other techniques and satisfies a high-speed up.

REFERENCES

[1] Dastoor, Sarosh. "Comparative Analysis of Steganographic Algorithms Intacting the Information in the Speech Signal for Enhancing the Message Security in Next Generation Mobile Devices", IEEE Xplore Digital Library, in proceedings of The World Congress on Information and Communication Technologies. Mumbai, India, 11-14 Dec.2011: pp. 279-284.

[2] Dey, Sandipan, Ajith Abraham, and SugataSanyal. "An LSB Data Hiding Technique Using Natural Numbers", in proceedings of IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IIHMSP, Nov. 26-28, 2007, Kaohsiung City, Taiwan, vol.2: pp. 473-476.

[3] Nosrati,Masoud, RonakKarimi, HamedNosrati and Ali Nosrati, "Taking a Brief Look at Steganography: Methods and Approaches", Journal of American Science, vol.7, no. 6, 2011: pp. 84-88.

[4] SandipanDey, Ajith Abraham, BijoyBandyopadhyay and SugataSanyal. "Data Hiding Techniques Using Prime and Natural Numbers", Journal of Digital Information Management, vol. 6, no. 3, pp. 463-485, 2008.

[5] Stern, Richard M. Fu-Hua Liu, Yoshiaki Ohshima, Thomas M. Sullivan, and AlexAcero, "Multiple Approaches to Robust Speech Recognition", in proceedings of DARPA Speech and Natural Language Workshop, Feb. 1,1992: pp.274-279 .

[6] Chatzimisios, P., Verikoukis, C., Santamaria, I., Laddomada, M., Hoffmann, O. (eds.). Mobile Lightweight Wireless Systems. In proceedings of The Second International ICST Conference, Mobilight, May 10-12, 2010, Barcelona, Spain, Revised Selected Papers. Springer. p. 164.

[7] Wu, Bin, Jianwen Zhu and FaridNajm, "Dynamic-Range Estimation". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 25, Issue 9, Sept. 2006, pp.1618-1636.

[8] Wu, Bin, Jianwen Zhu and FaridNajm, "An Analytical Approach for Dynamic-Range Estimation", inProceedings of the 41st DAC AnnualDesign Automation Conference, San Diego, California, USA, June 7-11, 2004: pp. 472-477

[9] Wu, Bin, Jianwen Zhu and FaridNajm, "Dynamic Range Estimation for Nonlinear Systems."IEEE/ACM. In proceedings of the International Conference on Computer-Aided Design(ICCAD-04), San Jose, California, Nov. 7-11, 2004.

[10] Miller, Scott and Donald Childers. Probability and Random Processes: With Applications to Signal Processing and Communications.USA, Academic Press, 2012: pp. 370–375.

[11] Gouyon, F., Pachet, F., Delerue, O., "Classifying Percussive Sounds: A Matter of Zero-Crossing Rate", in Proceedings of the COST G-6 Conference on Digital Audio Effects (DAFX-00), Verona, Italy, Dec. 7–9, 2000.

[12] B.L,Srinivas, Anish Shanbhag and Austin Solomon D'Souza , "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, vol.2, Special Issue 5, Oct., 2014:pp.77-88.

[13] J. Nadir, A. Abu Ein and Z. Alqadi, " A Technique to Encrypt- decrypt Stereo Wave Files", International Journal of Computer and Information Technology, ISSN: 2279 -0764, Volume 05 Issue 05, September2016

[14] M. Kaur and S. Kaur, "Survey of Various Encryption Techniques for Audio Data", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, pp. 1314-1317, 2014