Hash Based Data Text Fusion in Speech Signal Using Speech Signal Algorithm

*Madhu, **Anu Aggarwal, ***Anjali Sachdeva
*Deptt of CSE, DIET, Karnal 132001 madhu.wadhwa8@gmail.com
**Deptt. of CSE, DIET, Karnal – 132001
***Deptt of CSE, UGI, Lalru

Abstract
The term "fusion" generally literally means to embed something in some cover field. In the proposed work we are going to hide text data using hash based functionality by finding the non area of interest (NAOI) in the speech signals.
We are going to use .wav file format for speech signals which is to be processed for fusion data into that image.
Data is firstly converted into the ASCII. Data which is going to be hidden taken from any text document stored in our System and then will be fused into that Cover Image.
The next task is to secure the data which is to be fused in to the voice signals that is done with the Concept of HASH KEY, length of the hash key is totally based upon the data which we are going to hide under speech signal.
The term "Decrypt" means to extract something from some cover field. Then we are going to extract text data using hash based functionality from the speech signals. Data which is already hidden taken from any text document stored in our System and then will be read after the decryption process.
Cryptography Algorithm is used to solve out the problem.
Keywords: Speech Signal; Decrypt; PSNR; MSE; NAOI

I INTRODUCTION

Data extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration). The import into the intermediate extracting system is thus usually followed by data transformation and possibly the addition of metadata prior to export to another stage in the data workflow.

This technique has been required and developed for the purpose of security mainly annotation and protection of data or text. Concerning the data hiding performance, not only the imperceptibility of embedding text but also the robustness for the signal processing or intentional attacks is required. Data hiding in audio signals exploits imperfection of human auditory system (HAS) known as audio masking. The present techniques for data hiding within audio signals involve Spread Spectrum (SS), Least Significant Bit (LSB), Phase Encoding (PE), Echo Hiding (EH), Spectrum Transform (ST) and so on.

Perception-based audio data hiding schemes generally exploit the human auditory system (HAS) characteristics such as spectral masking, temporal masking, and inaudibility of phase distortion. Existing audio data hiding schemes can be classified according to the underlying technique used for embedding data. Methods based on least significant bit dithering embed information by replacing the least significant bits of the digital audio samples. Echo hiding methods introduces inaudible echoes in the host audio signal based on the embedding message.

Decryption Algorithm is used to solve out the problem and the whole implementation is on MATLAB.

MATLAB ("MATrix LABoratory") is a tool for numerical computation and visualization. The basic data element is a matrix, so if you need a program that manipulates array-based data it is generally fast to write and run in MATLAB (unless you have very large arrays or lots of computations, in which case you're better off using C or Fortran). If you are doing a computation of any significant length in MATLAB, you will probably want to make an m-file. Anything that you would type at the command prompt you can put in the m-file (for example, "script.m") and then run it all at once (by typing the name of the m-file, e.g. "script", at the command prompt). You can even add comments to your m-file, by putting a "%" at the beginning of a comment line. You can also use m-files to create your own functions.

This paper presents an Decryption Algorithm to decrypt the data so that the data will become secure. The Decryption process is shown below in the Section II. We also calculated the PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) in the Section III.

II   EQUATIONS

The phrase peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is most easily defined via the mean squared error (MSE) which for two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$
$$= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$
$$= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

III   LITERATURE REVIEW

1. Mohamed F. Mansour, et al **"Data Embedding in Audio Using Time-Scale Modification"** 2005 IEEE.
    They propose a new framework for data embedding in audio was proposed in this paper. The basic idea of the algorithm is to change the length of the intervals between salient points of the audio signal to embed data. The intervals are quantized and the data is embedded in the Quantization indices. In this particular implementation, they have used the wavelet extreme of the signal envelope as the salient points. They have proposed novel ideas

for practical implementation that can be used by other data embedding schemes as well. The proposed algorithm is robust to common audio processing operations, E.g.: MP3 lossy compression, low pass filtering, sampling rate conversion, and time-scale modification (TSM). The perceptual quality of the audio signal after embedding the data depends on the technique used for TSM.

2. Deng Lixin **"A new approach of data hiding within speech based on Hash and Hilbert Transform"**
In this paper, an approach for data hiding within speech signals based on Hash and Hilbert Transform (HT) has been proposed. The secret data is firstly pre-processed by Hash to enhance its security. Then, exploiting the orthogonality of HT and insensitivity of human perception to the phase of speech, then embeded processed secret data into a speech signal by using the HT They have propose in this paper both blind and non-blind methods to extract embedded data along with experimental results demonstrates transparent, secure and robust data hiding performances.

3. Hafiz M.A. Malik,,Rashid Ansari, Ashfaq A. Khokhar" **Robust Data Hiding in Audio Using All pass Filters**"
2000 IEEE.
This paper proposes a data hiding technique where digital audio exploits the low sensitivity of the human auditory system to phase distortion. Inaudible but controlled phase changes are introduced in the host audio using a set of all pass filters (APFs) with distinct parameters of all pass filters, i.e., pole-zero locations. The APF parameters are chosen to encode the embedding information. During the detection phase, the power spectrum of the audio data is estimated in the -plane away from the unit circle. The power spectrum is used to estimate APF pole locations, for information decoding. Experimental results show that the proposed data hiding scheme can effectively withstand standard data manipulation attacks. Moreover, the proposed scheme is shown to embed 5–8 times more data than the existing audio data hiding schemes while providing comparable perceptual performance and robustness.

4. Mohamed Waleed Fakhr,**"A Novel Data Hiding Technique for Speech Signals with High Robustness"** 2000 IEEE.
A novel data hiding technique for robust watermarking is proposed. The technique is given the name **"Segment-Difference Classification" (SDC),** and is applied on speech signals. Each block of speech is divided into segments, and the weighted sum of each segment is calculated, where a secret set of random weights is used. The segments' weighted-sums are sorted by amplitude.

5. Jing Liu, Fei Gao, Haiyan Ma "**A Speech Chaotic Encryption Algorithm Based on Network**" 2007 IEEE.
Considering chaotic synchronization, the TCP protocol is usually adopted to transport encrypted data on networks at present. A block encryption algorithm is proposed to digital speech codes in this paper. The proposed method uses the UDP protocol to cipher text. It partially solves the problem of decryption for receiver when some data packages are lost during transportation. It encrypts message with chaotic sequences which randomly come from chaos model database, so the randomness of chaotic sequence is enhanced greatly. Furthermore, it can overcome the disadvantages of short period when data amount is great. The algorithm is testified with testing program written by the authors.

6. Marina Ponomar **"On Acceptable Modification Limits of Electroacoustic Speech Signals for Data Hiding"** 2009 IEEE.

This paper focuses on crypto security for data hiding in electro acoustic speech signals, and an example of data hiding in a speech signal based on segment fundamental frequency modification is described. In the process of embedding of data into speech artificial distortions can be perceivable for human ear. The author sets a task to determine acceptable limits of modification to maintain optimal security level and natural speech communication.

IV REFERENCES

[1] Marina Ponomar "On Acceptable Modification Limits of Electroacoustic Speech Signals for Data Hiding" 2009 IEEE.

[2] Deng Lixin "A new approach of data hiding within speech basedon Hash and Hilbert Transform"

[3] Jing Liu, Fei Gao, Haiyan Ma "A Speech Chaotic Encryption Algorithm Based on Network" 2007 IEEE

[4] Mohamed F. Mansour, Senior Member, IEEE, and Ahmed H. Tewfik, Fellow, IEEE "Data Embedding in Audio UsingTime-Scale Modification" 2005 IEEE.

[5] Hafiz M. A. Malik,,Rashid Ansari, Ashfaq A. Khokhar" Robust Data Hiding in Audio Using All pass Filters" 2000 IEEE.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Mohamed Waleed Fakhr,"A Novel Data Hiding Technique for SpeechSignals with High Robustness"2000IEEE