A Proposed Voice Encryption System Based on off-Line Ica Algorithm

Sattar B. Sadkhan , Nidaa A. Abbas  
University of Babylon, College of Information  
drengsattar@ieee.org  drnidaa_muhsin@ieee.org

Abstract

The voice encryption plays a great role in many important communication systems, such as military communication systems, a bank communication system. This paper proposes the possibility of application of analog voice encryption using adaptive signal processing technique called the Independent Component Analysis (ICA) technique. Practically the device encryption process is implemented using the JADE algorithm that can be considered as an Off-Line mode of ICA technique, and taking into consideration the testability of many input speech signals in Arabic and English. The objective test using LPC and SNR is applied to evaluate the proposed System.

Keywords— Adaptive Signal processing, analog voice encryption, Blind source Separation, ICA, JADE.

1. INTRODUCTION

In many applications, voice can only be transmitted over insecure channels such as telephone links. However, most of these applications require secrecy. In such cases, it becomes imperative to encrypt the voice signal. The voice can be encrypted in two ways: Digital and Analog.

Digital encryption involves digitization of the input voice signal first. The digitized signal is then compressed to produce a bit stream at a suitable bit rate. This bit stream is encrypted and transmitted over the channel using a modem (H. C. Baker and F. C. Piper, 1985). Digital encryption algorithms are cryptanalytically stronger than their analog counterparts. Moreover, they retain a lower residual intelligibility.

On the other hand, in analog voice encryption, also called voice encryption, we act on the voice samples themselves. Any analog voice encryption algorithm needs to satisfy the following requirements:-

1. The voice encryption should be unintelligible.
2. The voice encryption should occupy the same bandwidth as does the original voice signal. That is, the encryption process should be a bandwidth preserving operation.
3. It should be difficult to decrypt, if the decryption key is not available. In other words, it should be cryptanalytically strong or secure.
The communication delay caused by the voice encryption process must be as small as possible. The recovered voice at the receiving end should be of good quality and should preserve both the intelligibility of the voice and the characteristics of the speaker. Voice is highly redundant. For example, it remains intelligible even when subjected to severe amplitude distortion such as infinite peak clipping (A.S. Bopardikar, 2000). Filtering out all frequency components above or below 1.8 kHz still allows 67% of all syllables to be recognized correctly. This makes it all then, are difficult to encryption. These issues have motivated the design of more and more sophisticated voice encryption algorithms. However, analog encryptions do have some distinct advantages. Firstly, no modem or voice compression is required for transmission. Secondly, the quality of the recovered voice is independent of the language. Further, these voice encryption schemes can easily be interfaced with the existing analog channels such as telephone, satellite or mobile communication links.

This paper proposed the possibility of application of analog voice encryption using adaptive signal processing technique which is called the Independent component analysis (ICA) technique. Practically the devoice encryption process is implemented using the JADE algorithm that can be considered as an Off-Line mode of operation in ICA techniques.

The paper contains four sections. Section II introduces the ICA techniques, while section III describes the proposed system. Section IV provides the conclusion.

2. ICA TECHNIQUES

2.1 Blind Source Separation (BSS)

The term “blind” stresses the facts that:

1. The source signals are not observed and
2. No information is available about the mixture.

This is a sound approach when modelling the transfer from the sources to the sensors is too difficult; it is unavoidable when no prior information is available about the transfer. The lack of prior knowledge about the mixture is compensated by a statistically strong but often physically plausible assumption of independence between the source signals.

In most cases, the representation of the data is sought as a linear transform of the observed variables. Using linear transformations makes the problem computationally and conceptually simpler, and facilitates the interpretation of the result (S. I. Amari and A. Cichocki, 1998; J. F. Cardoso, 1998; A. Hyvarinen, 1999).

Several statistical methods have been developed to find suitable linear transformation. These include PCA, Factor Analysis (FA), Projection Pursuit (PP), ICA, and many more. ICA is a statistical method for finding underlying factors or components from multivariate (multidimensional) data, which distinguishes ICA from other methods. It means that it looks for components, that are both statistically independent, and non-Gaussian. ICA is a useful extension of PCA that has been developed in context with blind separation of independent sources for their linear mixtures (J. Karhunen et al, 1997).

The basic linear model relates the unobservable source signal and the observed mixtures: 

\[ x(t) = As(t) \]  

(1)
Where $s(t) = [s_1(t), ..., s_m(t)]^T$ is a $m \times 1$ column vector collecting the source signals, similarly vector $x(t)$ collects the $n$ observed signals, $A$ is a $n \times m$ matrix of unknown mixing coefficients, $n \geq m$, and $t$ is the time index. This model is instantaneous (or memoryless) because the mixing matrix contains fixed elements, and also noise-free.

If noise is included in the model, it can be treated as an additional source signal or as measurement noise. In the case the model becomes:

\[ x(t) = As(t) + n(t) \]  

(2)

Where the noise vector $n(t)$ is of dimension $n \times 1$. The mixing matrix may be constant, or can be with the time index $t$. In the time-varying case, $A$ becomes $A(t)$ (P. Comon, 1994).

In order to recover the original source signals from the observed mixtures, we use a simple linear separating system (J. F. Cardoso, 1998):

\[ y(t) = Bx(t) \]  

(3)

Where $y(t) = [y_1(t), ..., y_n(t)]^T$ is an estimate $s(t)$, and $B$ is a $n \times n$ (assume $n=m$) separating matrix, as shown in Fig. 1.

**Figure 1.** Mixing and separating. Unobserved signals; observations $x(t)$, estimated source signals $y(t)$.  

### 2.2 Independent Component Analysis (ICA)

ICA defines a generative model for the observed multivariate data, which is typically given as a large database of samples. In the model, the data variables are assumed to be linear or nonlinear mixtures of some unknown latent variables, and the mixing system is also unknown. The latent variables are assumed non-Gaussian and mutually independent and they are called the independent component (IC) of the observed data. These independent components are also called sources or factors that can be found by ICA (A. Hyvarinen and E. Oja, 2000).

ICA severs from two ambiguities, there are:

1. The variances (energies) of the independent components cannot be determined.
2. The order of the independent components cannot be determined.

There are mainly two distinct approaches towards computing the ICA, off-line (batch) processing, and on-line algorithms. In this paper we concentrate on batch algorithm. This approach (batch algorithm) employs high order cumulants and is found mainly in the statistical signal processing literature. A standard approach for batch ICA algorithms is the following two stages procedure (P. Comon and C. Jutten, 2010): -
1. Decorrelation or whitening. This stage seeks to diagonalize the covariance matrix of the input signals. It is implemented by computing the sample covariance matrix, giving the second order statistics of the observed output. From this, a matrix is computed by eigen decomposition which whitens the observed data.

2. Rotation. This stage minimizes a measure of the higher order statistics which will ensure that the nonGaussian output signals are as statistically independent as possible. It can be shown that this stage can be carried out by a unitary rotation matrix (J. F. Cardoso and A. Souloumiac, 1993), to provide the higher order independence. It is implemented by finding a rotation matrix which jointly diagonalizes eigenmatrices formed from the fourth order cumulants of the whitened data. The outputs from this stage are the independent components.

This approach is sometimes referred to as “decorrelation and rotation”, and relies on the measured signals being nonGaussian. For Gaussian signals, the higher order statistics are zero already and so no meaningful separation can be achieved by ICA methods. For nonGaussian random signals the implication is that not only should the signals be uncorrelated, but that the higher order cross-statistics (e.g., moments or cumulants) are zero (Tianbao Dong et al, 2012).

3. PROPOSED SYSTEM

We use Joint Approximate Diagonalization of Eigen-matrices (JADE) algorithm to test the samples of voice signals. Fig. 2, represent the proposed system.

![Diagram of the proposed system]

To test the validity of the above proposed system, we take the voice signal with the variety of intervals of random mixing matrix, samples, and frequency samples. Two measures are used for the original and encryption voice, these are: SNR,

\[
SNR = 10 \log_{10} \frac{\sum_{n=-\infty}^{\infty} s^2(n)}{\sum_{n=-\infty}^{\infty} (s(n) - \hat{s}(n))^2} (dB) \tag{4}
\]
Where \( n \) is the number of samples, \( s(n) \) is the amplitude of the input voice signal and \( \hat{s}(n) \) is the amplitude of the reconstructed voice signal, and LPC distance

\[
d_{\text{LPC}}(c, e) = \ln \left( \frac{a_c R_e a_c^T}{a_e R_c a_e^T} \right)
\]

(5)

Where \( R_c \) is the autocorrelation matrix of the clear voice block, vector \( a_c \) contains the LPC coefficients for the clear voice block and vector \( a_e \) containing the LPC coefficients for the voice encryption block.

3.1 Steps of the Proposed System

The steps of the proposed system are:

1. Input the original signal
2. Split the original signal into segments, where every segment has an equal number of samples, and independent from each other to ensure the successful using ICA.
3. Choose an interval from the random mixing matrix.
4. The result is the encryption voice, as in (1). Where the steps from 2-4 represent the encryption voice process.
5. The decorrelating process is called whitening using Principal Component Analysis (PCA); this can be accomplished by scaling the vector elements by the inverses of the eigenvalues of the correlation matrix. The whitened data have the form:

\[
\tilde{x}(t) = D^{-1/2} E^T x(t)
\]

(6)

Where \( \tilde{x}(t) \) is the whitened data vector, \( D \) is a diagonal matrix containing the eigenvalues of the correlation matrix and \( E \) contains the corresponding eigenvectors of the correlation matrix as its columns. One of benefits of whitening is noise reduction, as the data not contained in the \( n \) first components may be mostly due to noise (J. F. Cardoso and A. Souloumiac, 1993).

Using a JADE algorithm (J. F. Cardoso and A. Souloumiac, 1993). The result is the decryption voice, as in (3). Due to the ICA ambiguity, the order of ICs doesn't determine, hence we reorder the ICs to obtain the decryption d voice.

3.2 Experiments

Through tests we implement the experiments on different separate English letters and different English and Arabic words. Hence we choose on this paper (for clarification) only the word MASSA and the letter C. Fig. 3 up to Fig. 8 provides the original, encryption and decryption forms of the tested signals. While the table I provide the performance parameters (SNR and LPC distance) measured at different sampling frequencies. It is evident from this table as the sampling frequency increased the SNR decreased and LPC increased.
### TABLE I
**PRONOUNCE OF WORDS MASAA AND LETTER C.**

<table>
<thead>
<tr>
<th>Voice</th>
<th>LENGTH OF SEGMENTS</th>
<th>Fs</th>
<th>SNR</th>
<th>LPC Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MASAA</td>
<td>2000</td>
<td>44100</td>
<td>6.8266</td>
<td>0.1796</td>
</tr>
<tr>
<td>C</td>
<td>500</td>
<td>8000</td>
<td>27.4534</td>
<td>0.0637</td>
</tr>
</tbody>
</table>

---

**Figure 3.** The Original MASAA Signal.

**Figure 4.** The encryption MASAA Signal.

**Figure 5.** The Decryption MASAA Signal, after reordering.

**Figure 6.** The Original C Letter Signal.

**Figure 7.** The encryption C Letter Signal.

**Figure 8.** The Decryption C Letter Signal, after reordering.

---

### 4. CONCLUSION

From the evaluation tests performed on the encryption and voice decryption (letters and words), we conclude that the new proposed voice encryption algorithm satisfies the followings:

1. Unintelligibility of the tested encryption voice.
2. The proposed voice encryption process is bandwidth preserving operating.
3. It is very difficult to decrypt. Hence it is cryptanalytically strongly or secure.
4. Communication delay caused by voice encryption process was small.
5. The recovered voice signal at the receiving side was of better quality (through hearing) and preserves both the intelligibility of the voice and the characteristics of the speaker.
5. References