Military Technical College
Kobry El-Kobbah
Cairo, Egypt

10th International Conference
On Aerospace Sciences&
Aviation Technology

Secured Communication Technique for Voice Messages

Mahmoud E. Gadallah[*] A. S. Abbas[**]

ABSTRACT:

In this paper, a proposed algorithm to secure a voice message for communication is presented. The proposed approach depends on embedding the voice message in another one. The wavelet transform is used as the tool for the hiding process. The performance of the proposed approach has been tested and evaluated via its application to hide different voice messages and subjectively the transmitted message is listened. The obtained results have shown that this algorithm is promising for secure voice communication.

KEY WORDS:

Secure Communications – Wavelet Transform – Embedding – Detection – Key Message – Secret Message.

I. INTRODUCTION:

The need to protect information in transmission has existed ever since man had a requirement to communicate over distance. The majority of the instances cited are in relation to communications associated with Military campaigns or political power games, however in modern times this will also apply to business and personal communications. The most common form of protection for information in transit currently known is Cryptography. This is the rendering of the information into an unintelligible stream that cannot be deciphered by the casual viewer. This form of protection is only as strong as the crypto key used to scramble the information. No attempt is made to hide the communication and an adversary knows that the communication exist but not what it says. The advent of modern computing techniques is such that computing power is increasing and it is getting easier to decipher encrypted communications using a "Brute Force" attack. This where all possible crypto key permutations are tried until a match is found. In order to combat this stronger crypto keys are being produced. With the latest research into quantum computing, crypto analysis is set to reach a peak where most ciphers will not stand up against the attacks possible [1]. So the researchers moved toward another mechanism, which is data embedding technology. Data embedding is the insertion of information into another piece of data for the purposes of covert communication, establishment and protection of ownership, managing and recording access,

[*] prof. Dr., Armed Forces.
[**] BSc, faculty of computers & information systems, Ain Shams University.

and ensuring data integrity. It is used for a variety of multimedia and text data types, as well as for computer code and file systems. Different types of data embedding are: Stecanography, Digital Watermarking, Digital Fingerprinting, and Digital Verification. Data embedding technology draws from many fields, including signal processing, image processing, communication theory, information theory, data communications, computer data structures, security, cryptography, and even intellectual property law [2].

Techniques for information hiding have become increasingly more sophisticated and widespread [3]. Least significant bit substitution (LSB) is the most common form of data embedding. Digital watermarks technology began humbly around 1993 with the exploration of this technique [4]. This technique exploits the representation of binary information. In such architecture, the bits in each binary word, or byte, are stored in order from the most significant bit (MSB) to the least significant. For images and audio, researchers believe that very little information is conveyed in the LSB and changing it has little effect on the quality of the host file. LSB works by breaking the covert message into individual bits and replacing the LSBs of the pixels are altered. Audio algorithms change the LSBs of samples [2].

Echo embedment hiding of information in a discrete signal by introducing an echo in the cover. The cover signal is divided into blocks before encoding process and consecutive blocks are separated by a random number of unused samples so that the detection and extraction of the hidden data is that bit harder. The block has an echo introduced and the hidden data is introduced by varying the delay between the signal and the echo within the block. The delay duration will denote if the information encoded is a 1 or 0 in binary terms. The delay times are chosen so as not to be noticeable to the human observer [1].

With referring to [5] some audio data embedding approaches are presented. Using a phase-coding approach, data are embedded by modifying the phase values of Fourier transform coefficients of audio segments. Another one is based on replacing the Fourier transform coefficients over the middle frequency bands, 2.4-6.4 kHz, with spectral components from hidden data. The middle frequency band was selected so that the data remain outside of the more sensitive low-frequency range.

One of the well-known data embedding methodology is spread spectrum. This type attempts to insert a signal throughout the spectrum of a broadband noise carrier [2]. There exist a set of techniques that work in the frequency domain which are based on the spread spectrum concepts. One of such techniques is a technique that embeds a spread spectrum signal into the Fourier coefficients of an image carrier. Frequency-based spread spectrum methods appear to be more robust than their spatial counterparts [6].

Another set of techniques depends on masking phenomenon ([2], [5], and [6]). Frequency Masking is well-known technique that uses the masking as abase for the embedding process. It is based on the signal redundancies and the irrelevancies of the human auditory system. The term psychoacoustics describes the characteristics of the human auditory system on which the technique is based. The sensitivity of the human auditory system for high frequencies is between 2.5 and 5khz. This sensitivity decrease above and below this frequency band to a threshold where any tone above and below this threshold will not be perceived. For every tone in the audio signal there is a masking threshold that can be calculated. If another tone lies below this threshold it will be masked by the louder tone and remain inaudible. By knowing where these thresholds are the technique is to hide the secret data within these inaudible thresholds [1].

Jonathan Foote and John Adcock proposed a method that is called Time Base Modulation. The method is based on subtly and inaudibly compressing or expanding time regions of an audio file. By comparing the altered file with a reference copy, compressed and expanded regions can be detected. This method was used in watermarking [7].

A simple technique uses the DC level of the audio signal as a way to embed the bits of information such as product id [8]. Also, this method was used in watermarking.

With the introduction of the wavelets, new techniques appeared that depend on it. One of them use the nature of the wavelet coefficients, by finding the coefficients whose values are below a specified threshold and replacing them with the bits of data to be hidden [9].
Embedding data in a transformed content is not restricted to the obvious transforms that are widely used for compression as DCT (Discrete Cosine Transform), wavelet and fractal transforms [10].

The paper is organized as follows: In section (II) the wavelet transform is introduced, and then in section (III) the proposed approach is presented. Section (IV) is dedicated to a discussion on some important aspects of the proposed approach, and then section (V) shows the experiments and tests. Finally section (VI) gives the conclusions and the future work.

II. WAVELET ANALYSIS:

In signal processing there are numerous examples of the benefits of working in the frequency domain. Fourier analysis remains a powerful technique for transforming signals from the time domain to the frequency domain. However, time information is hidden in the process. In other words, the time of a particular event cannot be discerned from the frequency domain view without performing phase calculations, which is very difficult for practical applications.

The Fourier transform was modified to create the Short-Time Fourier Transform (STFT) in an attempt to capture both frequency and time information. The STFT repeatedly applies the Fourier transform to disjoint, discrete portions of the signal of constant size. Since the time window is constant throughout the analysis, a signal can be analyzed with high time precision or frequency precision, but not both. As the window gets smaller, high frequency, transitory events can be located, but low frequency events are not well represented. Similarly as the window gets larger, low frequency events are well represented, but the location in time of the interesting, high frequency events becomes less precise. Wavelet analysis offers more flexibility because it provides long time windows for low frequency analysis and a short time window for high frequency analysis. As a result, wavelet analysis can better capture the interesting transitory characteristics of a signal.
A wavelet is a waveform of limited duration with an average value of zero. One-dimensional wavelet analysis decomposes a signal into basis functions, which are shifted and scaled versions of a *mother* wavelet. Wavelet coefficients are generated and are a measure of the similarity between the basis function and signal being analyzed. To scale a wavelet is to compress or extend it along the time axis. A compressed wavelet will produce higher wavelet coefficients when evaluated against high frequency portions of the signal. Therefore, compressed wavelets are said to capture the high frequency events in a signal. A smaller scale factor results in a compressed wavelet because scale and frequency are inversely proportional [11].

Since a wide range of signals can be classified into piecewise polynomial, Wavelet transform has become an essential tool for many applications [12]. Wavelet analysis is capable of revealing aspects of data that other signal analysis techniques miss aspects like trends, breakdown points, discontinuities in higher derivatives, and self-similarity. Furthermore, because it affords a different view of data than those presented by traditional techniques, wavelet analysis can often compress or de-noise a signal without appreciable degradation. Indeed, in their brief history within the signal-processing field, wavelets have already proven to be an indispensable addition to the analyst's collection of tools and continue to enjoy a burgeoning popularity today [13].
The continuous and discrete wavelet transforms are given in equations (1), (2) respectively [14]:

$$T_\psi f(b,a) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} f(t)\psi\left(\frac{t-b}{a}\right)dt \tag{1}$$

$$T_\psi f(b,a) \approx \frac{1}{\sqrt{a}} \sum_{n} f(n)\psi\left(\frac{n-b}{a}\right) \tag{2}$$

In digital signal and image processing, the discrete wavelet is closely related to filter banks. A typical two-channel decomposition and reconstruction structure is given in Fig. (1).

It is well-known that the filter banks will provide perfect reconstruction (i.e., in Fig. (1)) if they satisfy (3) and (4) [14]:

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 2 \tag{3}$$

$$H_0(-z)G_0(z) + H_1(-z)G_1(z) = 0 \tag{4}$$

Very important classes of filter banks are orthonormal filter banks. For two-channel, orthonormal, FIR, real-coefficient filter banks (T.O.F.R.FB.), (3) and (4) are equivalent to equations (5)–(7) [14]:

$$G_0(z)G_0(z^{-1}) + G_0(-z)G_0(-z^{-1}) = 2; \tag{5}$$

$$G_1(z) = -z^{-2k+1}G_0(-z^{-1}), \qquad k \in Z; \tag{6}$$

$$H_i(z) = G_i(z^{-1}), \qquad i \in \{0,1\}. \tag{7}$$

III. THE PROPOSED ALGORITHM:

The proposed approach is divided into two parts: the embedding algorithm and the detection algorithm. These two algorithms are described in the following subsections.

a) The Embedding Algorithm:

Let x and y be the secret message and host signals respectively. The signal y , will be the key of the detection process. The two signals are passed through the discrete wavelet transform

(W) with one level decomposition. This process yields four components (2 approximations and two details), which are $x_a, y_a, x_d, and\ y_d$ respectively. Then the approximation of the transformed secret message signal is multiplied by the detail of the transformed host signal, and the approximation of the transformed host signal is multiplied by the detail of the transformed host signal. By this way, the four components are merged into two new components $z_a\ and\ z_d$. This process can be expressed as follows:

$$z_a = x_a * y_d \qquad (8)$$

$$z_d = x_d * y_a \qquad (9)$$

Finally the resulting components are used as an approximation and detail to generate a new signal z by using the inverse wavelet transform W^{-1}, this can be expressed as:

$$z = W^{-1}(z_a, z_d) \qquad (10)$$

The resulting signal will be the transmitted, which carry the secret information embedded in it. The flow chart of the embedding process in an abstract view is shown in Fig. 2.

b) The Detection Algorithm:

The detection process works in the same fashion of the embedding process. First the received signal (the secured) is passed through the 1-level wavelet transform as following:

$$(z_a, z_d) = W(z) \qquad (11)$$

Also the key signal which must be available at the detector is transformed in the same manner as:

$$(x_a, x_d) = W(x) \qquad (12)$$

Then the approximation and detail of the secret message signal is obtained as:

$$y_a = z_d / (x_d + C) \qquad (13)$$

$$y_d = z_a / (x_a + C) \qquad (14)$$

Where C is a very small constant that is used to avoid the problem of dividing by zero. Lastly the obtained approximation and detail are used to get the secret speech signal as:

$$y = W^{-1}(y_a, y_d) \qquad (15)$$

The flow chart of the detection process in an abstract view is shown in Fig. (3):

IV. Discussions for the proposed approach:

In this section some important aspects of the proposed algorithm are discussed. The first point is the use of the multiplication process for embedding. The reason for this is that the approximation coefficients have larger amplitudes compared to the detail coefficients. By multiplying the approximation coefficients with the detail coefficients, a noise-like signal results (when both the secret key signal and secret signal are speech signals). This process results in hiding the secret signal in the secret key signal. The addition operation has been experimented as well instead of multiplication. In this case, a part of the secret message signal has been detectable. This result was expected because the transmitted message, in this case, consists of the approximation coefficients of the two signals (the dominant large amplitudes).

Second, the approximation of one signal is multiplied by the detail of the other one in the embedding process (not the approximation by the approximation and the detail by the detail). The discussion of the first point above interprets this choice.

Third, the proposed algorithm has been tested to recover the secret message signal using a signal that is not the key signal, which was used in the embedding process. In this case, the result has been impressive because the secret signal couldn't be detected. This is an important aspect in the hiding process to achieve the security because this means that only one signal that can work correctly with the decoder to get the secret signal, which is the key signal.

Fourth, it should be noted that, for proper operation of the proposed approach, the key signal must be long enough (long than the secret message signal) to hide the entire secret message signal. Otherwise part of the secret message signal will be audible.

Fifth, the proposed algorithm can be realized for real time environments; this is due to the simple operation on which it is based. The wavelet transform is realized as a QMF (Quadrature Mirror filter bank), and the multiplication/division as a simple register.

V. RESULTS:

The proposed approach has been evaluated by applying it to hide many voice messages and detecting them. As an example for these tests is the following experiment. In this experiment, 3 speech massages: the secret message signal, the key signal, and a false key signal, respectively are used. Fig. (4) Shows the embedding process and the detection process.

Fig. (5) shows the result of detection when a false key signal has been used in the detector (which happen in real situations by the attackers). It is clear that the detected signal in this case is not the secret signal. This experiment confirms that the key signal is necessary to detect the secret message.

VI. CONCLUSIONS:

In the work reported in this paper, an algorithm to hide a voice message in another voice message has been introduced. The algorithm has shown that the wavelet transform is a powerful technique to achieve this purpose. This work is considered as a starting step towards developing a robust technique for securing voice communication. The authors are continuing to develop and improve the introduced algorithm. Also, a hardware implementation is the final objective of this work.

VII. REFERENCES:

[1] - R .A. Isbell, "Steganography hidden menace or hidden saviour", LIRIC Associates Ltd, 2002.

[2] - Erich J. Smythe, "Data embedding for information assurance", state-of-the-art-report, Information Assurance Technology Analysis Center, 1999.

[3] - Hany Farid, "Detecting hidden messages using higher-order statistical models",International conference on Image Processing, Rochester, Ny, 2002.

[4] - Christoph Busch, Wolfgang Funk, and Stephen Wolthusen, "Digital Watermarking: From Concepts to Real-Time Video Applications", IEEE Computer Graphics and Applications, vol. 19 no. 1 pp. 25–35, Jan./Feb., 1999.

[5] - M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data-embedding and watermarking technologies", Proceedings of the IEEE, vol. 86, no. 6, June 1998.

[6] - Jiri Fridrich,"Applications of data hiding in digital images", ISPACS'98, 1998.

[7] - Jonathan Foote and John Adcock, "Time base modulation: a new approach to watermarking audio and images", Proc. ICME 2003.

[8] - Umut Uludag and Levent M. Arslan, "Audio watermarking using dc level shifting", EE 683.01 Advanced Topics in Speech Processing project report, 2001.

[9] - Han-Yang Lo, Sanjeev Topiwala, and Joyce Wang," Wavelet based steganography and watermarking", Cornell University, CS 631 1998.

[10] - R. J. Anderson and F. A. P. Petitcolas,"On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 474–481, Special issue on copyright & privacy protection, May 1998.

[11] - Jacob T. Jackson, Gregg H. Gunsch, Roger L. Claypoole, and Jr., Gary B. Lamont, "Blind Steganography Detection Using a Computational Immune System Approach: A Proposal", Air Force Institute of Technology, Aproposal,2002.

[12] - Junhui Qian, "Denoising by wavelet transform", Department of electrical engineering, 4100 south main, st. Houston,2001.

[13] - Michel Misiti, Yves Misiti, Georges Oppenheim, and Jean-Michel Poggi,"Wavelet Toolbox User's Guide", MathWorks, Inc., 2000.

[14] - Yiwei Wang, John F. Doherty, and Robert E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE transactions on image processing, vol. 11, no. 2, February 2002.

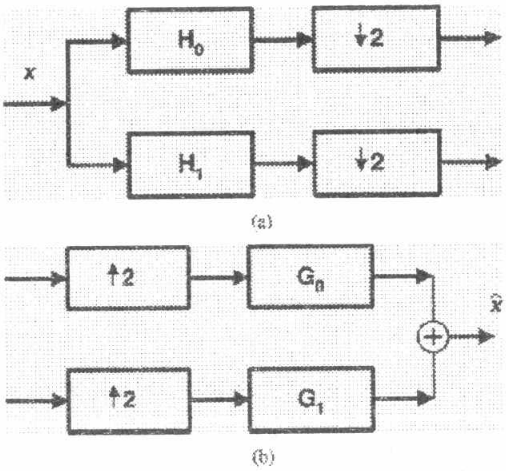

Fig. 1 Two-channel decomposition and reconstruction structure

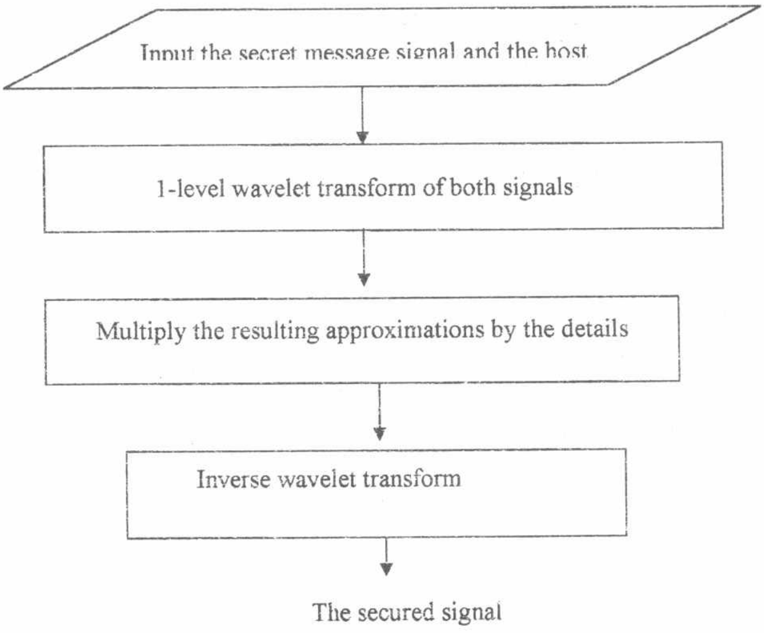
Input the secret message signal and the host
1-level wavelet transform of both signals
Multiply the resulting approximations by the details
Inverse wavelet transform
The secured signal

Fig. 2 The embedding process

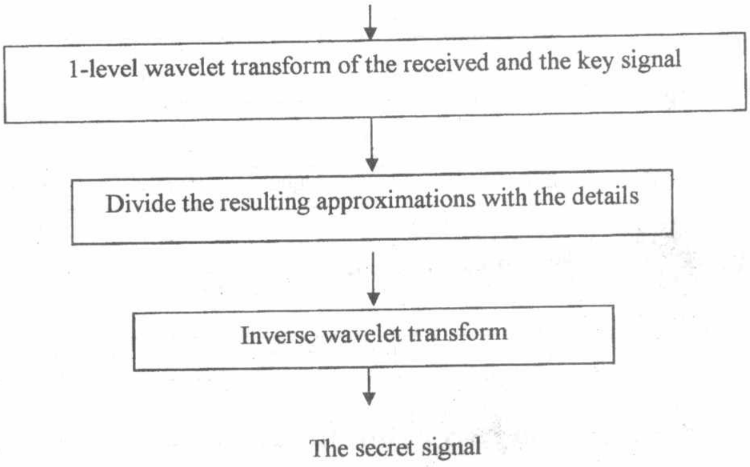
1-level wavelet transform of the received and the key signal
Divide the resulting approximations with the details
Inverse wavelet transform
The secret signal

Fig. 3 The detection process

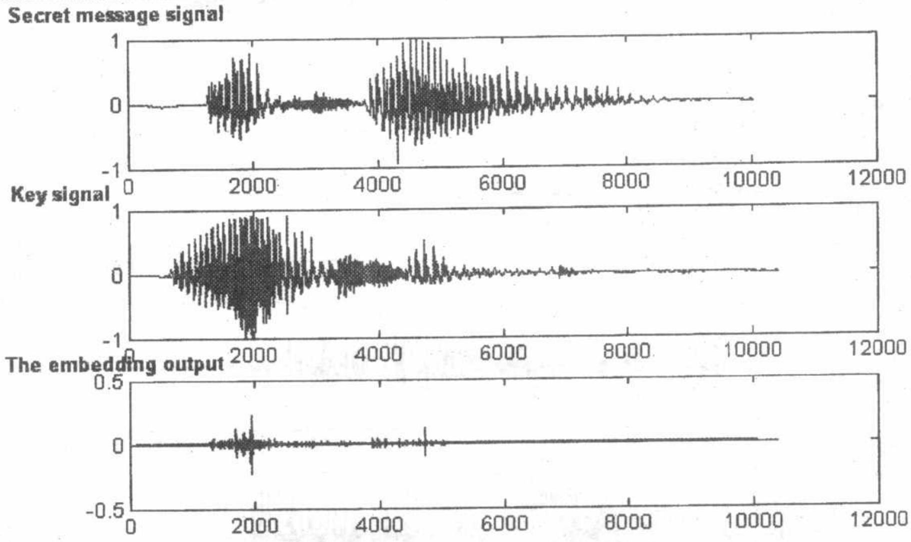

Fig. 4(a) The Embedding Process

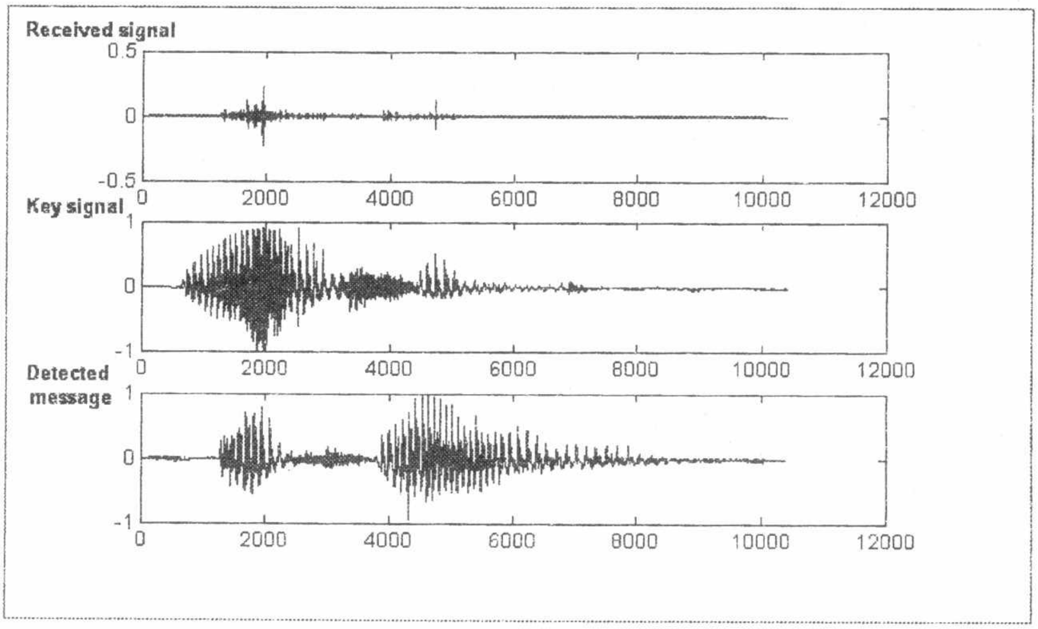

Fig. 4(b) The Detection Process with correct key signal

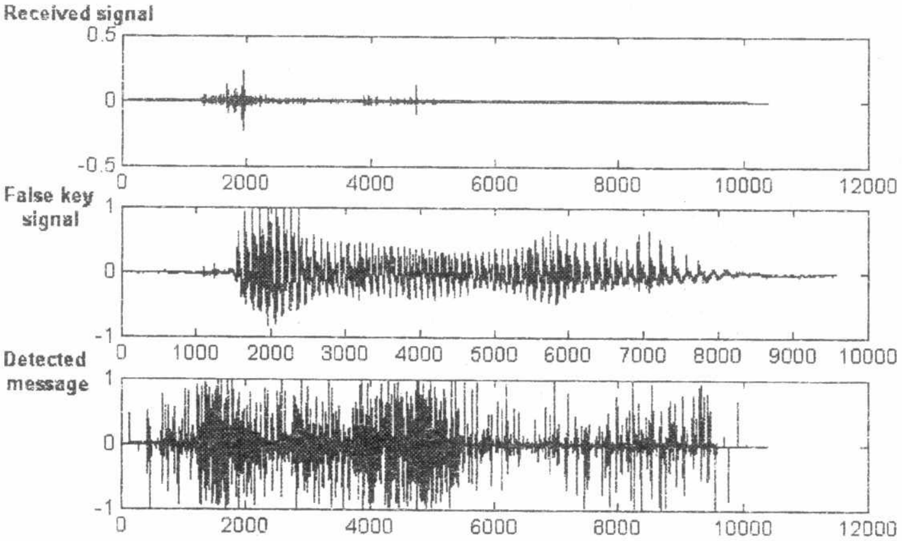

Fig. 5 The Detection Process with wrong key signal