CM-2 | 439

MILITARY TECHNICAL COLLEGE

CAIRO - EGYPT

A Practical Limit for the Validity Time of a Cipher System Base Key

By

Y.A.Abou Kerisha and M.N.Saleh

ABSTRACT

Key Management is a vital procedure for the appropriate performance of any cipher system. Of key management sub-items is the key change policy that arouses a quest about the limitations of time interval elapsed before necessitating the replacement of the secret base key.

This paper discusses the problem of the base key validity time for two distinct cipher systems ;namely the straight forward(synchronous) and the cipher feedback(self-synchronous) stream cipher systems. Its result is depicted as a graph aiding to either choose number of bits for some key parameters in system design forgiven validity interval duration or to evaluate an already implemented system.

I. Introduction and Problem Definition

In cipher systems, secret keys are those variable parameters used to control their performance. The base key is that one that constitutes all portions of secret keys which can, hardly, be changed neither per message nor per transmission session. This is simply because, base key change requires an arduous procedure and dedicated resources imposing to keep the base key valid for certain number of messages (message interval) or for certain time period (time interval).

For optimizing key management procedure we have to define a limit for the validity interval of a base key on practical basis other than the validity interval defined by the time of executing an exhaustive search attack for secret base key. This latter limit is excluded as being irreasonable to be admitted today, since designers of cipher systems were aware enough for that type of attacks by increasing the length of base key expressed in bits. Consequently the up to date cipher systems can not be easily cracked by trying all possible keys and such brute force attack entails time amount approaching several years even with very fast trials of one nanosecond per key.

In this work, we consider the aspect of message key which is an akin to straight-forward stream cipher systems and the aspect of cover time for cipher feedback systems for the purpose of defining a practical limit for base key retention or replacement. In section 2, we use the message key principle in conjunction to straight-forward cipher system to attain our objective and this section includes deduction of the base key

- Y.A.Abou Kerisha (Armed Forces ,Signal Corps)
- M.N.Saleh (Faculty of Engineering ,Ain Shams University)

message interval and its practical interpretation. In section 3, we discussed the cryptanalysis principle applied cipher feedback systems and this section includes deduction of base key time interval and its practical application. Finally, conclusions are given.

II. Key Validity Time in Straight-Forward Cipher Systems

In these systems, a message key is associated with the base key. Such message key is a subset including certain number of bits ranging to about one fourth of the base key length. Message key has the task of randomizing the starting point of the enciphering sequence of the stream cipher key sequence generator. At the start of enciphering each message; a message key is generated usually using a true random bit generator and send to the deciphering side ahead of the enciphered message [1]. The message key is then mixed with the base key, in some way or another, the mixture is used to initialize the enciphering algorithm (the key sequence generator algorithm).

II.1. Evaluation of the Validity Time

To avoid having two sequences enciphered by the same enciphering sequence, a distinct message key is used for each enciphered message. For a message key with L bits, the pool of message key has a number M of key possibilities given by :

$$M = (2^L - 1)$$

The probability of having distinct message keys for a number R of messages is given by :

$$P = (1-1/M)\ (1-2/M)\ \ldots\ (1-(R-1)/m) \qquad (1)$$

where;

R is the number of enciphered messages.
M is the number of different possibilities of the message key.

Equation (1) can be reformulated as :

$$P \simeq M!/(M^R).(M-R)! \qquad (2)$$

Using Strling formula which is given by:

$$N! \simeq (N/e)^N.(2\pi N)^{1/2}$$

Where e.... is the natural base.
Equation (2) will be :

$$P = (1-\theta)^{[-M(1-\theta)\ -\ 0.5]}.e^{(-M^{\theta})} \qquad (3)$$

Where $\theta = R/M$

The base key of a stream cipher system can be retained as long as it affords high probability of distinct message keys, i.e the base key can be retained for a message interval comprises a number of messages under condition of satisfying the accepted probability figure for distinct message keys.
Taking p = 0.999, specific values for message interval are computed as 2,11,46,259 or 1466 for L of 10,15,20,25 or 30 respectively.

II.2. An Application Example

Illustrative examples for use of the derived validity time will be taken from domains of application of cipher systems over telephone communication (speech encryption) and teletype and facsimile encryption (data encryption).

In telephone networks, the so called common user telephone is assigned practically a traffic occupancy of 0.25 erlangs for the purpose of traffic analysis. The most important factor, for the case of key management, is the average holding time of telephone call[8]. A value of 3 minutes is an acceptable practical average holding time, accordingly, an average of 120 calls per day is implied. Considering the 120 calls per day as the rate of messages we get the corresponding base key retaining interval shown in fig.1 for various applications. Thus, if the common user telephone subscriber uses a voice encryption equipment which implements a straight-forward stream cipher system with a message key length of30 bits; the user can retain his base key for 7 days safely.

Another telephone subscriber is the so called sole user, he is assigned a larger traffic occupancy of 0.6 erlangs, accordingly an average of 288 calls per day is implied for the 3 minute average holding time of the call, its corresponding base key retaining interval is shown in Fig.1 as a result, if the sole user subscriber uses the same voice encryption equipment of the 30 bits message key he can retain his base key for 2 days only.

For dial up TTY and FAX, they are both assigned 0.25 erlangs practically, but with 1 minute average holding time. This willimply an average of 360 calls per day, consequently thecorresponding base key retaining interval is plotted in Fig.1.

III. Key Validity Time in Cipher Feedback Systems

In these systems, the intruder is interested in finding the key stream which is function of the base key and the feedback ciphertext register. This intruder needs a time to collect all the different states of the feedback register (cover time) to get the corresponding key stream bits.

To devoid the cryptanalytical attack, the validity time will betaken less than the time required for completing the aimed attack.The cover time [3] will be taken as the basis for the required calculation Practically, the cover time must be related to a specific attack against the cipher system, so we will adopt the related cover time analysis of the proposed cryptanalytical attack given in [4].

It has been shown [4] that the most significant time component of the cover time is that time component related to constructing the equivalent table, i.e the only significant time is that required for gathering the plain text-ciphertext pair of length (2 ^ L) at the actual transmission rate of the cipher system. The other two time components of cover time, namely the look up time into the table and the deciphering time of a cipher bit by modular addition of two bits, are highly dependent upon practical realization technology used, more over, according to todays technology, these times are extremely short w.r.t the significant time component for gathering the plain text-ciphertext pair.

Let the transmission rate of the cipher system is B bits per second, consequently, the base key retaining interval, K, is given by:

$$K \leq 2^N / B$$

where
N is the number of feedback cipher bits.
B is the actual transmission rate.

Figure-2 shows the plotting of the base key retaining interval K, versus the number of feedback bits N for different practical transmission rates.

IV. Conclusions

The key point in base key retaining interval in straight-forward stream cipher system is the message key length, while in cipher feedback system the key point is the length of the feedback ciphertext register.

Practically, it is preferable to have message key of length more than 30 bits in straight-forward stream cipher system while in cipher feedback systems the length of feedback ciphertext register is preferable to be more than 40 bits.

The comparison between straight-forward stream cipher and feedback cipher system can be a different subject of another aspects in addition to the base key retaining interval.

References

[1] Y.A.Abou Kerisha and T.A.EL-Garf,"Maximum Time Before Base Key Variation Depending on the Message Key Length", Proceedings of the Eighth National Radio Science Conference, Cairo, 1991.

[2] Y.A. Abou Kerisha and N.H. Shaker, " Cryptanalyzing Cipher Feedback Systems", Proceedings of the Eighth National Radio Science Conference, Cairo, 1991.

[3] H.J. Baker and F.C.Piper, " Cipher Systems, The Protection of communication " Northwood Publication, 1982.

[4] N.H.Shaker, " Cryptanalysis of Ciphertext Auto-Key Cipher Systems", M.Sc.Thesis, Faculty of Engineering, Ain Shams University, 1990.

[5] T.A.EL Garf, " Analysis of Straightforward Stream CipherSystems", M.Sc.Thesis, Faculty of Engineering, Ain Shams university, 1990.
[6] H.J.Beker, "Cryptography -Modern Cipher Systems", NewElect.13(23), pp. 29-33, 1980.
[7] C.E.Shannon, " Communications Theory of Secrecy Systems", Bell Syst. Tech.J.28, pp. 656-715, 1949.
[8] Bellamy, John, "Digital Telephony", John Wiley & Sons Inc, 1982.

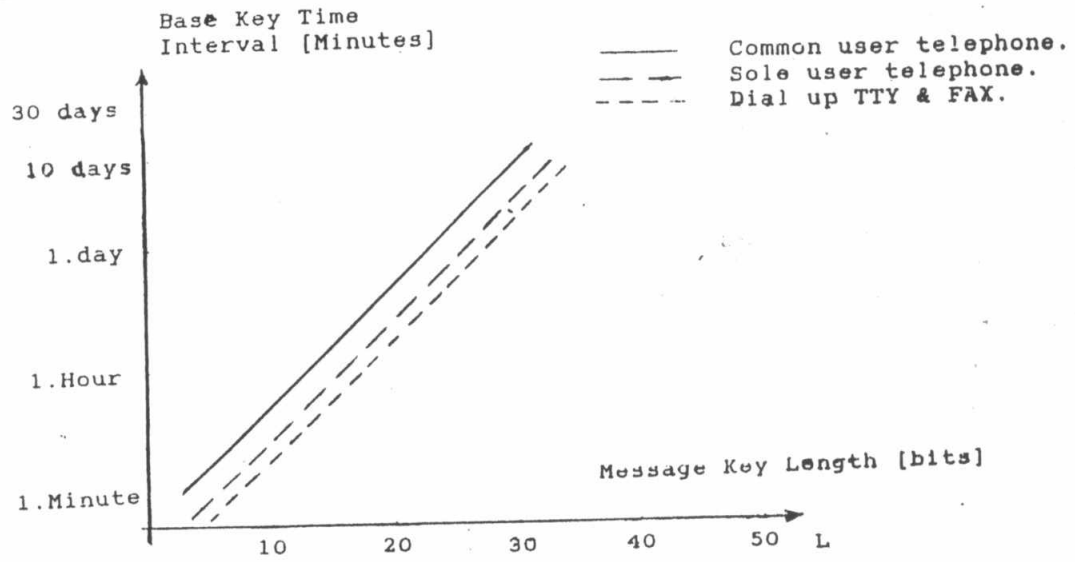


Fig-1 Base Key Time Interval
Versus Message Key Length.

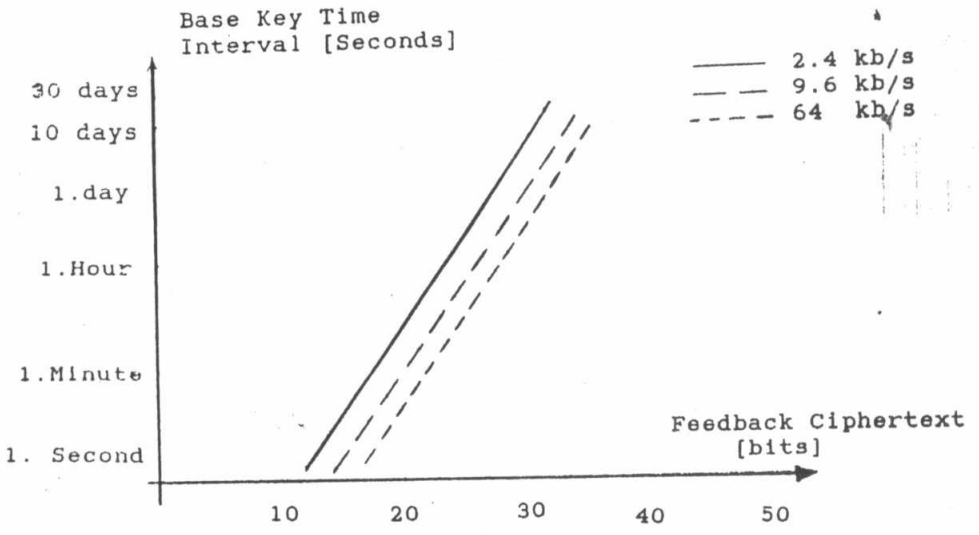
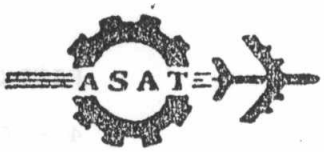


Fig.2 Base Key Time Interval Versus Feedback Ciphertext Length.

CM-3 445



MILITARY TECHNICAL COLLEGE

CAIRO - EGYPT

Improvement of the Linear Predictive Coding of Noisy Speech by a Pre-processing Technique.

Mahmoud E. Gadallah
Lecturer, Dpt. of Electronic Securing,
Military Technical College,
Cairo, Egypt.

ABSTRACT

In this paper, a technique for pre-processing speech signals before the linear predictive coding (LPC) of speech signals, spoken in a noisy environment, is proposed. The pre-processing technique introduced here depends on the use of median filter. The effect of applying this technique as a pre-processing stage on speech signals enhancement and consequently on the performance of the LPC analysis is studied. The use of median filter to enhance speech before the LPC analysis shows considerable reduction for the prediction error. The pre-processing technique introduced here is compared with the spectral subtraction technique which is used for speech enhancement. Median filtering the speech signals results in better performance as a speech enhancement technique than the spectral subtraction method when speech is corrupted by Gaussian noise. This result has been confirmed for different speech frames with different signal to noise ratios.

1. INTRODUCTION

One of the most powerful speech processing and coding techniques is the method of LPC. This method has become the predominant technique for estimating the basic speech parameters, e.g., pitch, formants, spectra, and vocal tract functions. LPC is used also to code speech for low bit rate transmission or storage. The importance of this method lies both in its ability to provide extremely accurate estimates of the speech parameters and in its relative speed of computation, [1]. The appeal of LPC as applied to speech, however, is not only its predictive function but also the fact that it gives us a very good model of the vocal tract. In other words, LPC can be interpreted as a spectrum matching process to produce the model that best matches the spectrum of the input signal.

From the discussion above, it is clear that if the input speech to the LPC is corrupted by any type of noise, the resultant model will match the spectrum of the distorted speech. In this case,

the estimated speech parameters will have a considerable error. Moreover, if the model estimated by the LPC is used for speech synthesis, the produced speech will be distorted. In a study for the effect of different types of noise on the LPC, introduced in [2], the authors have shown that LPC is susceptible to degrading effects in the case of noisy speech.

The study of reducing the effect of noise on the performance of the LPC is very important. This is true especially when the speech applications are used in a real noisy environment (e.g., aircrafts, cars, factories, etc.). In this paper, a pre-processing technique is introduced to reduce the effect of the random Gaussian noise on the LPC analysis.The noises studied here are the background noise of a computer room and an additive white Gaussian noise. The pre-processing technique proposed here depends on using median filter to enhance speech signal before applying the LPC.

One of speech enhancement techniques is the spectral subtraction method [3]. The pre-processing technique, introduced in this work, is compared with spectral subtraction to enhance speech signal corrupted with a white Gaussian noise.

The paper is organized as follows: In section 2, the application of median filter to improve the LPC performance is introduced. In the same section, the effect of median filter as an enhancement technique for noisy speech is tested for white Gaussian noise. In section 3, the idea of spectral subtraction technique is given and also its effect on a speech signal corrupted with a white Gaussian noise is tested to be compared with the median filter as a speech enhancement technique. Finally, a conclusion for this research is given in section 4.

2.APPLICATION OF MEDIAN FILTER AS A PRE-PROCESSING STAGE TO IMPROVE THE LPC OF SPEECH SIGNALS.

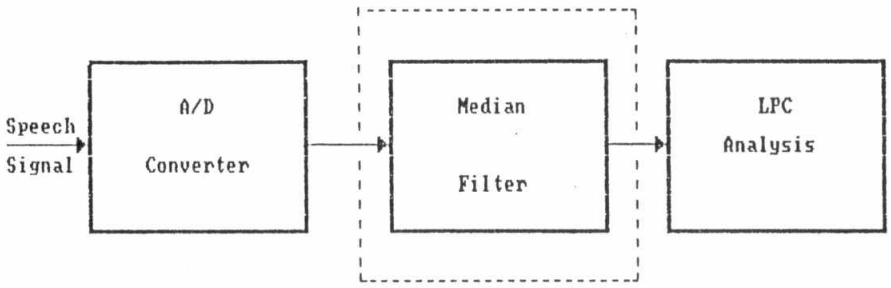


Figure 1. Pre-processing by median filter.

Figure 1 shows the configuration of speech processing system with

applying the median filter for noise reduction. Median filter is a known smoothing technique. It is applied in the field of image processing as a noise reduction technique [4]. The explanation of the theory of the median filter can be found in [1] and [4]. The main idea of median filter is that it separates signals based on whether they can be considered smooth or rough (noise-like). If we consider a signal x(n) that can be represented as:

$$x(n) = S[x(n)] + N[x(n)] \qquad (1)$$

Where **S[x]** is the smooth part of the signal **x** and **N[x]** is the noise like part of **x**, the median filter separates **S[x]** from **N[x]**. The median filter is applied and tested in the following cases:

2.1 Speech Uttered in a Computer Room:

This experiment is conducted using a speech signal uttered in a PDP-11 computer room to test the effect of median filtering speech signal before the LPC analysis on the prediction error as a measure for LPC accuracy. The noise in the room is clear from figure (2.a) which shows the word *"right"* . The effect of median filtering the signal of the same word is shown in figure (2.b). In this filtering, the window size (w) of the median filter was 3. Figure (2.c) shows the effect of applying the median filter of window sizes 3 and 5 as a pre-processing stage before the LPC analysis on the normalized mean square prediction error. This error is defined as [1]:

$$V_n = \prod_{i=1}^{p} (1-k_i^2) \qquad (2)$$

Where k_i, i=1,2,...p are the reflection coefficients calculated using the LPC and p is the order of analysis. The LPC analysis is applied here using lattice method [1], [3], [5]. From the figure, it is clear that there is a reduction in the normalized prediction error obtained when applying the median filter for noise reduction in most of the signal interval. Also, it can be noticed that only in regions where the signal strength is high, the error increases. This can be interpreted as the weak effect of noise at such regions. On the other hand; the reduction in the prediction error is considerable where the speech signals are weak. From figure 2.c, although a median filter with window size 5 results in more reduction for the prediction error in the weak signal intervals than the case when w=3, it causes considerable increase in this error in the regions of strong signals. This result is expected because when w=5, more smoothing is introduced which is desired in regions of weak signals at which noise level relative to speech level is high. For this reason, it is decided to use median filter with w=3 only for the next tests.

2.2 Speech Corrupted by White Gaussian Noise:

In this experiment, a random Gaussian noise has been generated and added to a 20 msec.speech frame. Tests have been done for different signal to noise ratios (S/N), namely, 5,11,17,23,26,29,35,41,47,53,and 59dB. The original speech frame, its spectrum and its spectrum envelope (calculated using LPC) are shown in figure 3. The effect of adding the Gaussian noise to the same frame , for the case when the S/N ratio is 11dB (one of the tested cases as an example), is shown in figure 4 which illustrates this effect in both time and frequency domains. Also, from this figure, the effect of noise on the spectrum envelope (i.e. the effect on the LPC accuracy) can be seen, especially on the high frequency components.

The median filter is applied to the same speech frame and the median filtered output is shown in figures 5.a. From this figure, the amount of noise reduced due to median filtering is clear. The spectrum of the median filtered frame is calculated and the LPC analysis is also applied to calculate the spectrum envelope. This is shown in figure 5.b. Also, from this figure, the effect of median filter for noise reduction can be noticed.

3. COMPARISON BETWEEN MEDIAN FILTER AND SPECTRAL SUBTRACTION FOR SPEECH ENHANCEMENT

The technique of spectral subtraction has been applied in many researches for noisy speech enhancement [6] and [7]. The main idea of spectral subtraction can be found in [3]. The procedure of this technique is shown in figure 6. In the work reported in this paper, this technique is applied and tested for the purpose of comparison with the proposed median filter technique from the point of view of speech enhancement and consequently on the improvement of the LPC analysis.

In this experiment, the same Gaussian noise ,used in subsection 2.2, has been generated with different levels and the spectrum of a 20 msec. frame of it is calculated and used as an estimate for the noise spectrum. Other frames of this noise are added to two speech frames with different signal levels. The first speech frame used is the one shown in figure 4 and the other one is shown in figure 7. The purpose of using different frames with different signal levels is to test the dependence of the technique on the frame location. The added noise to the speech frames have been studied for S/N ratios 5,11,17,23,26 and 29dB for the first frame which corresponds to S/N ratios -9,-3,3,9,12 and 15dB respectively for the second frame. The distorted frames have been used as an input to both the median filter and the spectral subtraction techniques. The resultant enhanced frames are shown in figure 8 for the case when the S/N ratio is 5dB for the first frame and in figure 9 for the case when S/N ratio is 3dB for the second frame. These tested cases are shown as some

examples because of the limited allowed size of the paper.Figures 8.a and 9.a show the distorted frames, figures 8.b and 9.b show the enhancement effect by median filter and figures 8.c and 9.c show the enhancement effect by spectral subtraction . As it is clear, the enhancement by median filter is better than that achieved by spectral subtraction especially for low S/N ratios. Thus, it can be said that enhancing speech by median filtering is suitable for the applications where the noise level is high (e.g. aircrafts, cars,...etc.). Another and important advantage of median filter over spectral subtraction is that it is time domain filtering technique. This means that median filtering is preferred in the applications in which the processing time should be as minimum as possible (e.g. recognition, synthesis).

4. CONCLUSIONS

If it is required to analyze the speech signals using the LPC technique, it is important to reduce the interfered noises before the analysis. Median filter, as a smoothing technique, can be used to reduce the effect of the wideband noise (random Gaussian noise). This technique has shown better performance as an enhancement technique for speech signals (with different S/N ratios) than spectral subtraction method.

References:

1. L.R. Rabiner, and R.W. Shafer, *"Digital processing of speech signals"*, Prentice-Hall, Inc., 1978.

2. M.R. Sambur and N.S. Jayant, *"LPC analysis/synthesis from speech inputs containing quantizing noise or additive white noise,"* IEEE Trans. vol. ASSP-24, no. 6, pp 488-494, Dec., 1976.

3. T.W. Parsons, *"Voice and speech processing"*, McGraw-Hill Book Comp., 1987.

4. R.C. Gonzalez and P. Wintz, *"Digital image processing"* , Addison-Wesley publishing comp., 1987.

5. S. Satio and K. Nakata, *"Fundamentals of speech signal processing"*, Academic Press, 1985.

6. S.F. Boll, *"Suppression of acoustic noise in speech using spectral subtraction"*, IEEE Trans., vol., ASSP-27, no. 2, pp. 113-120, April, 1979.

7. M.Berouti et al.: *"Enhancement of speech corrupted by acoustic noise"*, ICASSP-79, pp. 208-211, 1979.

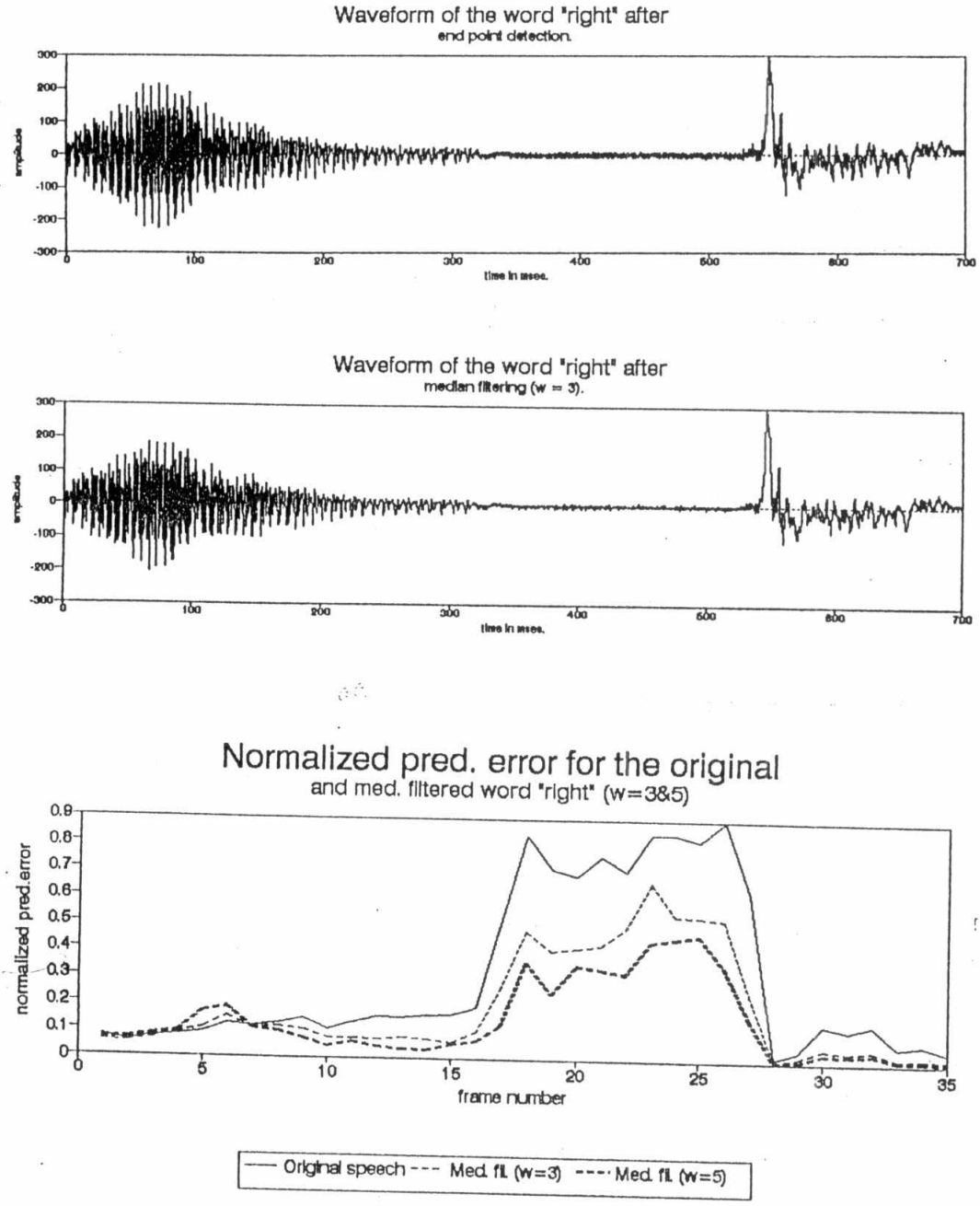


Figure 2. The effect of median filtering speech signal of the word "right"

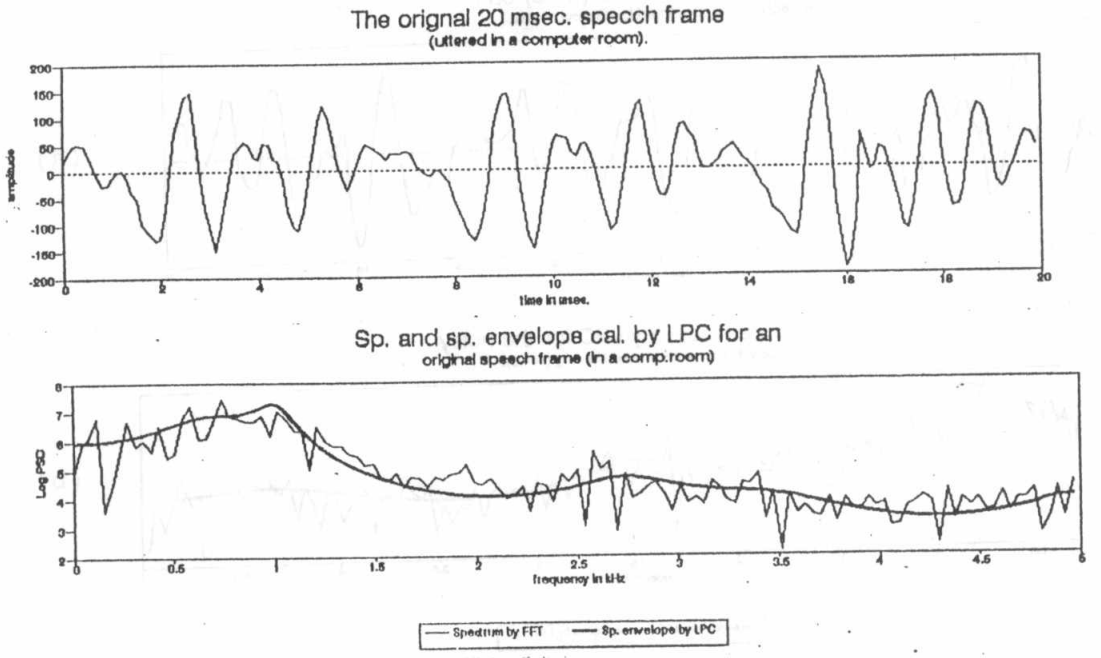


Figure 3. The original 20 msec. speech frame, its spectrum and spectrum envelope calculated using LPC analysis.

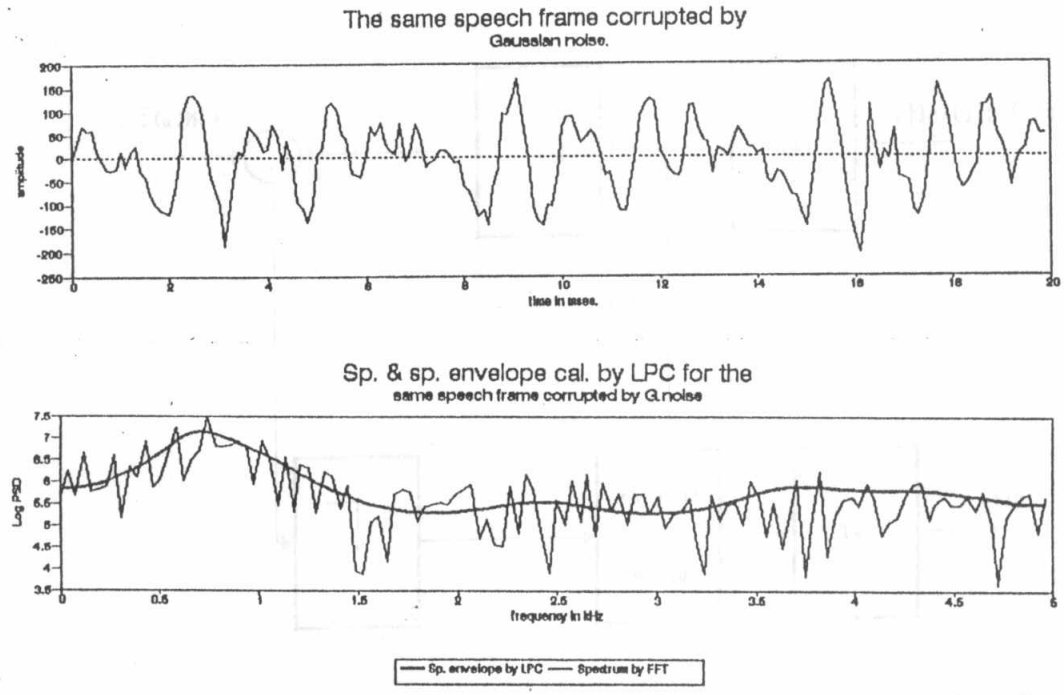


Figure 4. The effect of adding Gaussian noise to the speech frame of figure 3 such that S/N=11dB.

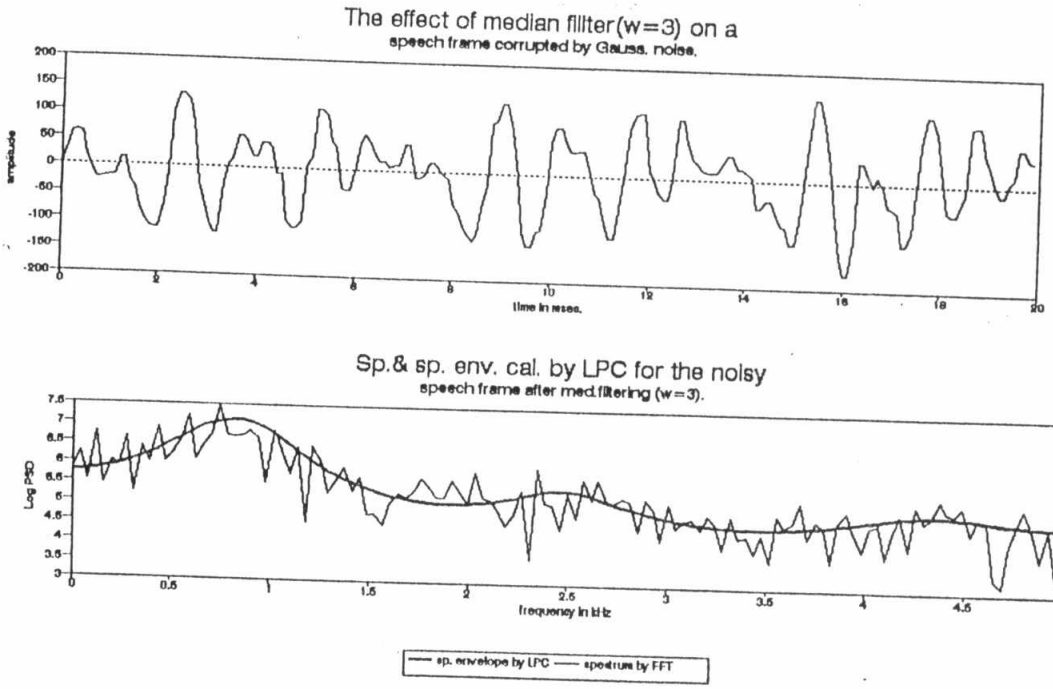


Figure 5. The effect of median filtering the speech frame of figure. 4 on its LPC analysis.

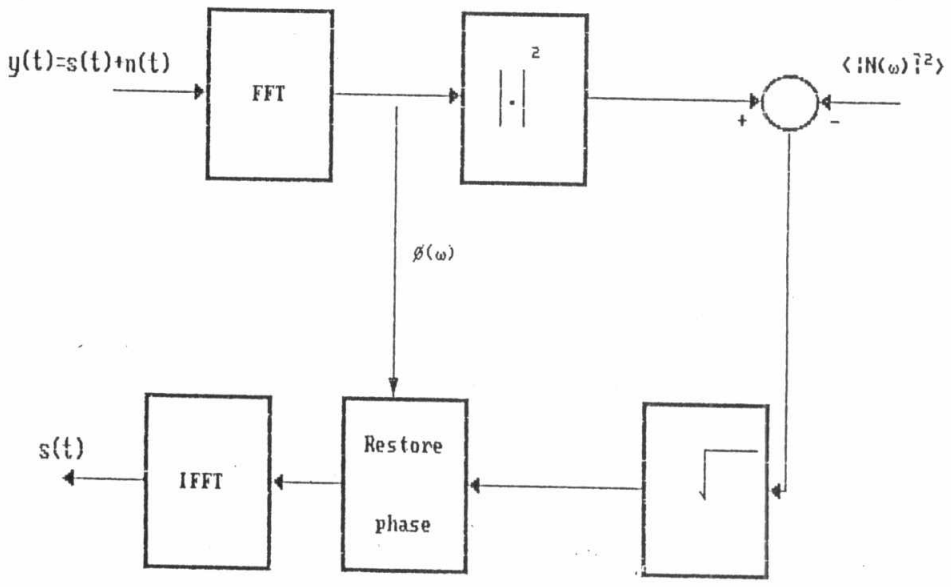


Figure 6. Spectral subtraction technique.

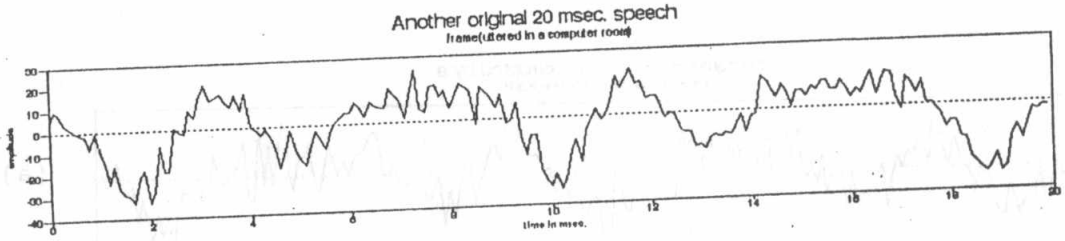


Figure 7. 20 msec. speech frame of weak signal level (the second frame).

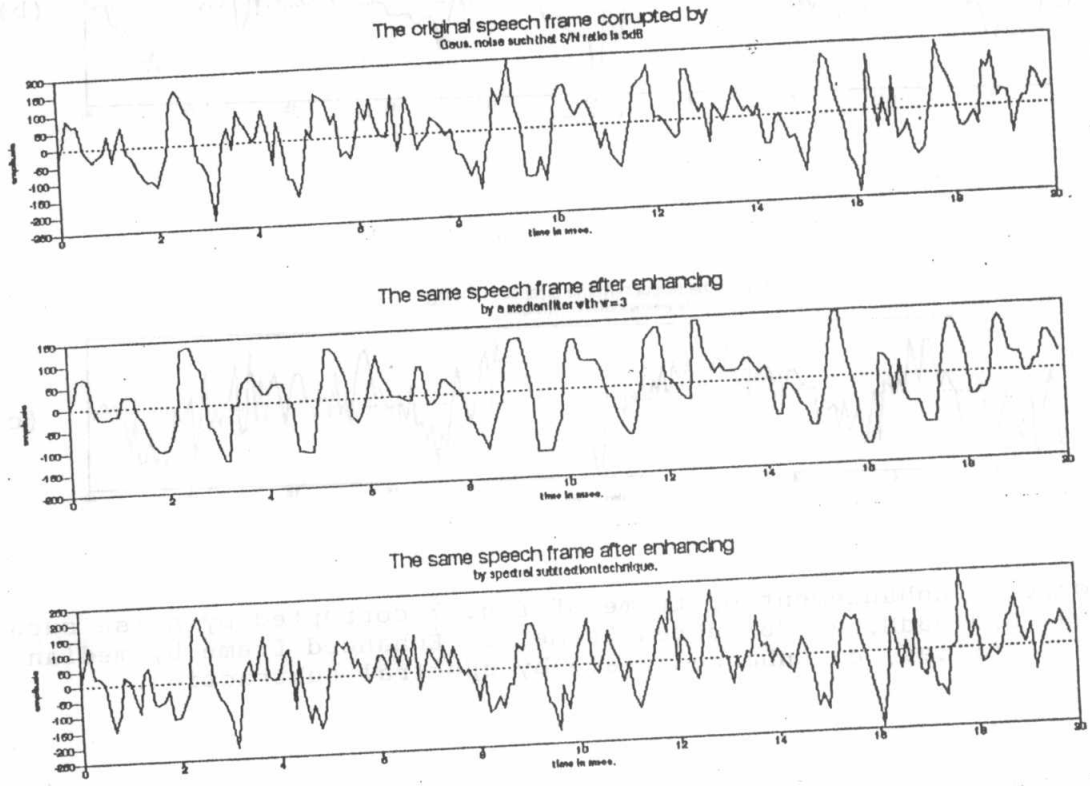


Figure 8. Enhancement of frame of fig. 3 corrupted by noise such that S/N =5dB, a. Corrupted frame, b. Enhanced frame by median filter, c. Enhanced frame by spectral subtraction.

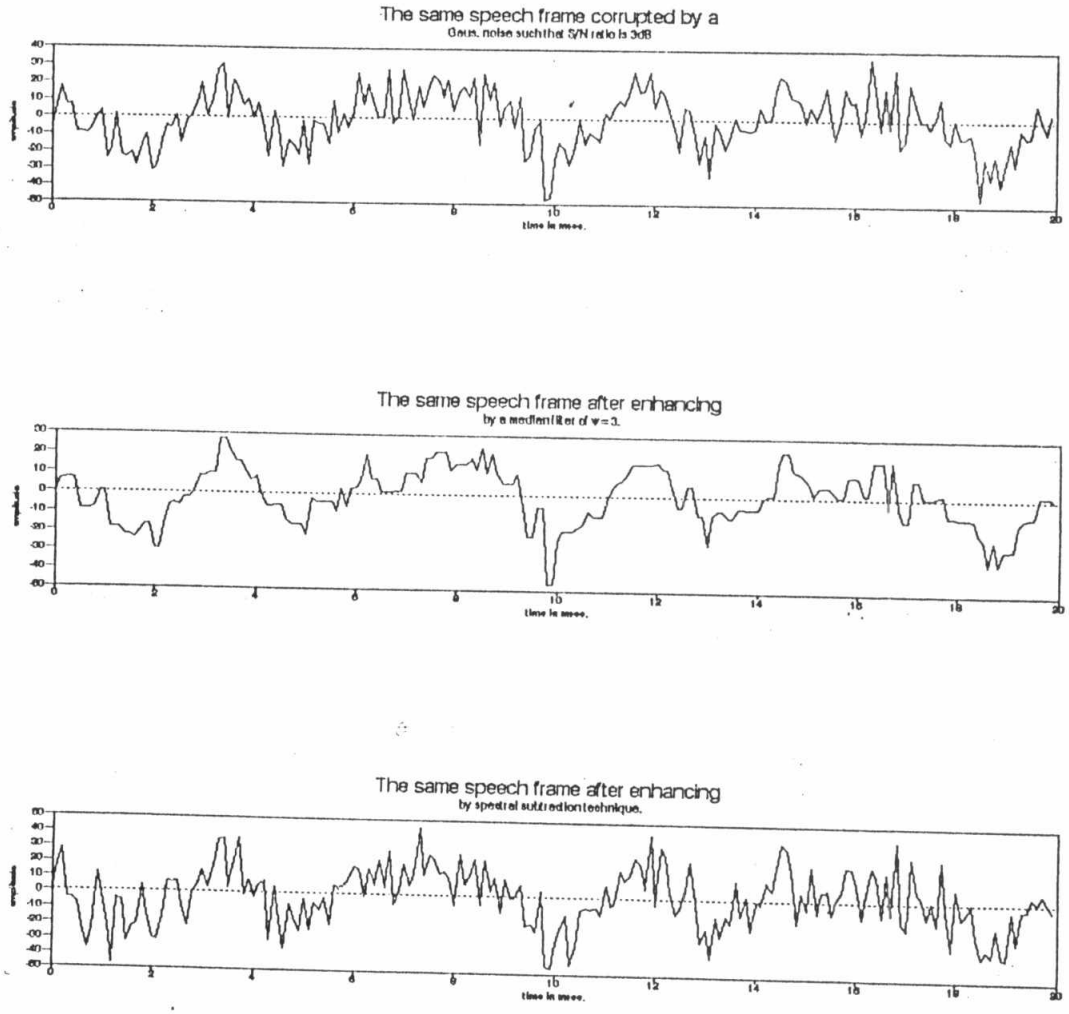


Figure 9. Enhancement of frame of fig. 7 corrupted by noise such that S/N =3dB, a. Corrupted frame, b. Enhanced frame by median filter, c. Enhanced frame by spectral subtraction.