On the Effectivity of Different Pseudo-Noise and Orthogonal Sequences for Speech Encryption from Correlation Properties

V. Anil Kumar, Abhijit Mitra and S. R. Mahadeva Prasanna

***Abstract*—We analyze the effectivity of different pseudo noise (PN) and orthogonal sequences for encrypting speech signals in terms of perceptual intelligence. Speech signal can be viewed as sequence of correlated samples and each sample as sequence of bits. The residual intelligibility of the speech signal can be reduced by removing the correlation among the speech samples. PN sequences have random like properties that help in reducing the correlation among speech samples. The mean square aperiodic auto-correlation (MSAAC) and the mean square aperiodic cross-correlation (MSACC) measures are used to test the randomness of the PN sequences. Results of the investigation show the effectivity of large Kasami sequences for this purpose among many PN sequences.**

***Keywords*—Speech encryption, pseudo-noise codes, maximal length, Gold, Barker, Kasami, Walsh-Hadamard, autocorrelation, crosscorrelation, figure of merit.**

I. Introduction

WHILE transmitting information (speech, image or other data) through insecure channels, there might be unwanted disclosure as well as unauthorized modification of data if that is not properly secured. Therefore, certain mechanisms are needed to protect the information within insecure channel. One way to provide such protection is to convert the intelligible data into unintelligible form prior to transmission and such a process of conversion with a key is called encryption [1]-[3]. At the receiver side, the encrypted message is converted back to the original intelligible form by the reverse process of the encryption called decryption. Cryptographic techniques are mainly classified as private key cryptography and public key cryptography [2],[3]. In private key cryptography, also called symmetric key cryptography, same key is used for both encryption and decryption. In public key cryptography, on the other hand, different keys are used for encryption and decryption and it is thus called an asymmetric key cryptography. The main disadvantage of private key encryption technique is the distribution of key to authorized users but it is faster when compared with public key cryptography.

Security is needed against two types of attackers, namely casual listeners and professional attackers termed as cryptanalysts. The strength of a cryptographic system [4],[5] is measured in terms of time and the resources required to break the system for getting back the message in intelligible form. Removing the intelligibility of a message that is to be transmitted is sufficient to provide security against a casual listener, but cryptanalysts would need strong cryptograms.

In this paper, a symmetric key encryption technique for speech samples based on the simple XOR operation with different PN sequences is used to test the performance of the sequences for speech encryption, and the residual intelligibility present in the encrypted speech using different sequences is observed by informal listening tests and by signal inspection methods. This encryption scheme is easy to implement, less complex and it provides better security against casual listeners.

Usually, speech encryption techniques using PN sequences make the speech signal unintelligible by removing the correlation between the samples of the speech signal. The sequences used for the encryption, in any case, should not portray the statistical properties of the transmitted signal so that the attacker cannot use statistical analysis to attack the system. PN sequences [6]-[8] have noise like properties; these sequences are statistically independent and uniformly distributed. XOR operation of these sequences with the speech samples makes the speech signal a *noise-like* signal, and the encrypted speech signal sounds like a random noise signal. The PN sequences which have good auto-correlation and cross-correlation properties remove the correlation among the speech samples and results in an encrypted signal of less residual intelligence. The randomness of binary sequences is measured by mean square aperiodic auto-correlation (MSAAC) and mean square aperiodic cross-correlation (MSACC) measures [9],[10]. The sequences which have better random noise properties will have less MSAAC and MSACC values.

This paper is organized as follows: in Sections 2 and 3, we briefly deal with different types of PN and orthogonal sequences. Section 4 describes the techniques to measure the correlation or randomness of the PN sequences. Section 5 narrates the speech encryption using PN sequences and the main obtained results along with the comparison of the different PN sequences are given in Section 6. The paper is concluded by summarizing the present work in Section 7.

II. Different PN Sequences for Speech Encryption

PN sequences are streams of 1's and 0's. Here, the waveform is taken as a *random-like*, meaning that it can be generated by mathematically precise rules, but statistically it satisfies the requirements of a truly random sequence in the limiting sense. These pseudo-random or pseudo-noise (PN) properties include, among other properties, (a) balance, (b) run and (c)

Manuscript received May 31, 2007; revised September 07, 2007.

The authors are with the Department of Electronics and Communication Engineering, Indian Institute of Technology (IIT) Guwahati, India. E-Mail: (v.anil, a.mitra, prasanna)@iitg.ernet.in.

auto-correlation properties [8]. These three properties make PN sequences efficient for speech encryption. However, due to the third property, adjacent bits correlation becomes considerably less, thereby making the PN sequences more effective for speech encryption when compared with data encryption due to high adjacent correlation present in the speech signals. Therefore, PN sequences that are useful for speech encryption must have very good auto-correlation and cross-correlation properties as well as maintaining some randomness properties. Below, we briefly describe different PN sequences useful for speech encryption. Note that in some cases we shall represent binary sequences using zeros and ones and in other cases +1's and -1's. The appropriate mapping is that the zeros are mapped to +1's and ones are mapped to -1's.

A. Maximal Length Sequences

The Maximal length sequence (m-sequence) generator is usually constructed with linear feedback shift registers (LFSR) [11],[12]. The m-sequences are, by definition, the largest codes that can be generated by a given shift register of given length with feedback. The feedback function, also called as characteristic polynomial, determines the length and type of the sequence generated.

B. Gold Sequences

Gold sequences are generated by the modulo-2 operation of two different m-sequences of same length. Any two m-sequences are able to generate a family of many non-maximal product codes, but a preferred maximal sequences can only produce Gold codes [7], [8].

C. Gold-Like Sequences

There exists a class of sequences which has parameters similar to those of Gold sequences except that it is obtained from a decimated sequence. Let u be an m-sequence of length $N = 2^n - 1$ generated by a primitive polynomial of degree n and let q be an integer such that $\gcd(q, N) = 3$. Also, let $v^{(k)}$, $k = 0, 1, 2$, denote the sequences obtained by decimating $T^k u$ by q. In that case, the new sequences formed by different combinations of u and v are called Gold-like sequences [13].

D. Barker Sequences

Barker sequences are short length codes that offer good correlation properties. A Barker code is a sequence of some finite length N such that the absolute value of discrete auto-correlation function $|\mathbf{r}(\tau)| \leq 1$ for $\tau \neq 0$ [14], [15]. Barker sequences have many advantages over other PN sequences. These sequences have uniformly low auto-correlation side-lobes ($\leq$1), but the size of these families is small.

E. Barker-Like Sequences

Barker sequences have good correlation properties with the peak correlation value being bounded by 1. The number of existing Barker sequences, however, are very less. We can generate more number of sequences by making certain relaxation on the peak value of the correlation function along with a maximum allowed shift between the sequences. This newly generated sequences are called Barker-like sequences [16].

F. Kasami Sequences

Kasami sequences are also PN sequences of length $N = 2^n - 1$, which are defined for even values of n [13],[17]. There are two classes of Kasami sequences: (i) small set of Kasami sequences, (ii) large set of Kasami sequences.

Small set of Kasami sequences are optimal in the sense of matching Welch's lower bound for correlation functions. A small set of Kasami sequences [13] is a set of $2^{n/2}$ binary sequences. Fig. 1 shows the block diagram representation for the generation of small set of Kasami sequences, each of length 63 bit.

Small set of Kasami sequences are optimal sequences and have better correlation properties compared to Gold sequences. But the set contains less number of sequences. For the shift register of length n the number of possible sequences for the small Kasami sequence set is only $2^{n/2}$ sequences, whereas Gold code set contains $2^n + 2$ sequences. The number of sequences can be increased by making some relaxation on the correlation values of the sequences. The resulting set of sequences is called large set of Kasami sequences [13],[17].

III. Different Orthogonal Codes for Speech Encryption

Two sequences are said to be orthogonal when the inner product between them is zero, i.e., $\langle \mathbf{c}_i(k\tau), \mathbf{c}_j(k\tau) \rangle = 0$ where $\mathbf{c}_i(k\tau)$ and $\mathbf{c}_j(k\tau)$ are the i^{th} and j^{th} orthogonal members of an orthogonal set, respectively, M is the length of the set and τ is the symbol duration. There are two kinds of orthogonal codes: fixed- and variable-length. Fixed length orthogonal codes include Walsh Hadamard (WH) and modified WH (MWH) codes. Among variable length codes, orthogonal Gold codes and orthogonal variable spreading factor (OVSF) codes are mentionable.

WH codes are orthogonal codes possessing low auto-correlation properties. The WH sequences [18],[19] of length N are defined with a class of orthogonal matrices $\mathbf{H}_N$, called Hadamard matrices, as $\mathbf{H}_N \mathbf{H}_N^T = N\mathbf{I}_N$ where $\mathbf{H}_N^T$ is the transposed Hadamard matrix of order N, and $\mathbf{I}_N$ is the $N \times N$ unity matrix.

MWH codes are generated by multiplying the Hadamard matrix $\mathbf{H}_N$ by a diagonal matrix $\mathbf{D}_N$ of same order [19],[20] such that $\mathbf{W}_N = \mathbf{H}_N \mathbf{D}_N$.

WH codes and MWH codes are fixed length orthogonal codes; the dot product of any two sequences is zero. Variable length orthogonal codes $\mathbf{c}_k(i)$, $i = 1, 2, \ldots, 2^k$, are those with different lengths satisfying the orthogonal property [7]. The codes are taken from a code tree and this orthogonal variable spreading factor (OVSF) tree generation algorithm is similar to the recursive generation of the Walsh codes by means of the Hadamard matrices. New levels in the code tree are generated by concatenating a root codeword with a replica of itself.

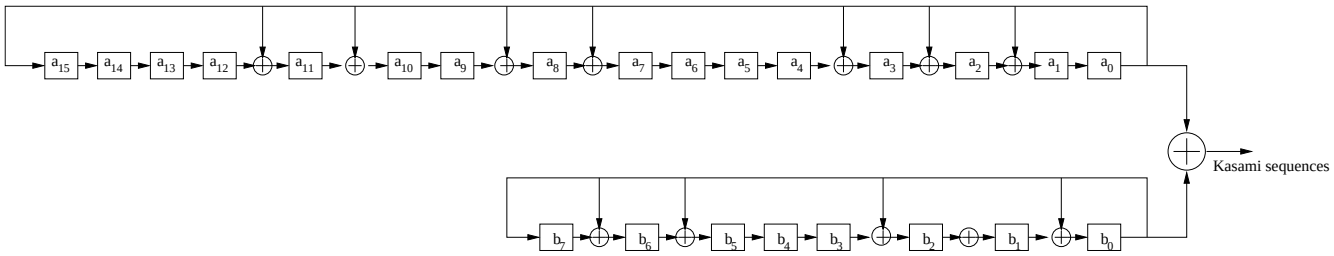

Fig. 1. An example of 63 bit small set of Kasami sequence generator.

One can find that many cross-correlation values of Gold codes are -1. By padding one zero to the original Gold codes, it is possible to make cross-correlation values to 0 at no shift among the two sequences. In fact, $2^n + 1$ orthogonal codes can be obtained by this simple zero padding. These codes are called orthogonal Gold codes.

A detailed discussion on all these PN and orthogonal codes can be found in [21].

IV. Mean Square Correlation Measures

The performance of the different PN sequences are evaluated by mean square aperiodic auto-correlation R_{AC} (MSAAC) and mean square aperiodic cross-correlation R_{CC} (MSACC) measures [20]. These correlation measures have been introduced by Oppermann and Vucetic [10]. If $\mathbf{c}_i(n)$ represents non-delayed version of $\mathbf{c}_k(i)$, $\mathbf{c}_j(n+\tau)$ represents the delayed version of $\mathbf{c}_k(j)$ by 'τ' units and N is the length of the sequence $\mathbf{c}_i$, then the discrete aperiodic correlation function is defined as

$$\mathbf{r}_{i,j}(\tau) = \frac{1}{N} \sum_{\tau=1-N}^{N-1} \mathbf{c}_i(n)\mathbf{c}_j(n+\tau). \tag{1}$$

The mean square aperiodic auto-correlation value for a code set containing M sequences is given by

$$R_{AC} = \frac{1}{M} \sum_{i=1}^{M} \sum_{\tau=1-N,\tau\neq 0}^{N-1} |\mathbf{r}_{i,i}(\tau)|^2 \tag{2}$$

and a similar measure for the mean square aperiodic cross-correlation value is given by

$$R_{CC} = \frac{1}{M(M-1)} \sum_{i=1}^{M} \sum_{j=1,j\neq i}^{M} \sum_{\tau=1-N}^{N-1} |\mathbf{r}_{i,j}(\tau)|^2. \tag{3}$$

Auto-correlation refers to the degree of correspondence between a sequence and phase shifted replica of itself, whereas cross-correlation is the measure of agreement between two different codes. These two measures have been used as the basis for comparing the sequence sets in this paper. The sequences which have good auto-correlation properties will have poor cross-correlation properties, and vice-versa, and they have wide and flat frequency spectrum. The sequences which have less MSAAC values removes the correlation among the bits with in a sample, and the sequences which have less MSACC values removes the sample to sample correlation, and make the speech signal less intelligible.

A. Figure of Merit

As has been mentioned, the price for being able to select good cross-correlation properties will be a degradation in the auto-correlation properties of the set of sequences. A degradation of the auto-correlation properties has a direct relation on the frequency spectrum of the sequences in the set. If the R_{AC} values are poor, the spectrum of the sequence will not be wide-band and flat. In order to determine quantitatively how significant this degradation is for a given set of sequences, a Figure of Merit (FoM) is required to judge the suitability of the frequency characteristics of the sequences. Sequences with low FoM has narrow flat spectrum and they are neither suitable for CDMA nor for speech encryption. The FoM for a sequence, $\mathbf{c}_i(n)$, of length N having the auto-correlation function $\mathbf{r}_i(\tau)$ is given as:

$$F_x = \frac{\mathbf{r}_{i,i}^2(0)}{\sum\limits_{\tau\neq 0} |\mathbf{r}_{i,i}(\tau)|^2} = \frac{N^2}{2.\sum\limits_{\tau=1}^{N-1} |\mathbf{r}_{i,i}(\tau)|^2}. \tag{4}$$

This is nothing more than the inverse of the MSAAC value for a given sequence. In our case, this FoM may be extended to the whole sequence set as each sequence in the set has the same absolute value of auto-correlation value. Thus we may use the inverse of the value calculated for the R_{AC} as the FoM.

V. Speech Encryption using PN Sequences

Speech signal can be viewed as sequence of samples and each sample can be viewed as a sequence of bits. Speech signal can be encrypted, by removing the correlation between speech samples, by the XOR operation of speech sample with a PN sequence selected at random from a table of PN sequences. Pseudo random index generators (PRIG) [11] are used to select a specific PN sequence from a given list of sequences. The block diagram of PRIG is similar to that of m-sequence generator. The decimal index value is generated by converting the binary output of each shift register in to decimal value by using a binary to decimal converter. The PN sequence corresponding to this decimal index value is taken from the table and XOR operated with the bits of the each speech sample to get the encrypted speech sample. At the receiver side same operation is performed to get the decrypted speech signal. The performance of the different PN sequences is compared by analyzing the encrypted speech signal in time domain and the spectrum of the encrypted speech signal.

VI. Results and Discussions

The above proposed techniques, MSAAC, MSACC measures and speech encryption using different PN sequences, are implemented in MATLAB.

A. Correlation Measures

PN sequences and orthogonal codes of desired length are generated as described in Sections 2 and 3, and the MSAAC and MSACC measures are computed for the code sets. Table I shows the correlation measures for PN sequences of length 63 bits. From the results, among all PN sequences, m-sequences and Barker sequences have low MSAAC values since these sequences have single peak auto-correlation function and all sidelobes amplitudes are very less. The FoM of these sequences is also high for which these sequences have flat power spectrum. These sequences, however, are not suitable for speech encryption since there is only one possible sequence for given LFSR length and given primitive polynomial, and the security provided by these sequences is thereby less. Note here that the circular shifted sequences of original sequences are not taken as different sequences. The Gold and Gold-like sequences have four valued auto-correlation and three valued cross-correlation functions with the maximum cross-correlation of $t(n)/N$ [e.g., for $n = 6$, the maximum correlation value is 0.2698]. However, the FoM of Gold-like sequences is more than that of Gold sequences and the number of codes that can be generated is also similar, therefore these sequences are more preferable than Gold sequences. The correlation values of Barker-like sequences depend on the value of m, i.e., the upper bound on the peak correlation function. For Barker sequences of length $N = 63$ and for $m = 15$, the obtained MSAAC and MSACC values are shown in Table I. These sequences have less auto-correlation values and therefore high FoM value. As has been mentioned, the auto-correlation value decreases with the increment of cross-correlation values. Barker-like sequences also have less auto-correlation values. Although small Kasami sequences have less auto-correlation values too and hence more cross-correlation values but the number of sequences that can be generated are less. Thus the security provided by these sequences is less compared to Barker-like sequences. The small set of Kasami sequences have less MSAAC value making the FoM of these sequences high. On the other hand, the large set of Kasami sequences have many unique features. The FoM of these sequences is similar to that of Barker-like sequences. The maximum cross-correlation value of large set of Kasami sequences is same as that of Gold sequences. The possible number of large Kasami sequences for a given structure are more when compared with all other PN sequences. All these features make large Kasami sequences effective for speech encryption.

Table II shows the correlation measures for 64-bit length orthogonal codes. Orthogonal codes have zero cross-correlation when there is no time shift between the two sequences but the correlation values are high when there is a shift between the sequences. The correlation values of orthogonal codes are high compared to that of PN sequences. The auto-correlation values of WH codes are very high and the FoM value is less so the spectrum of these sequences is not so wide and flat. However, the MWH codes have less correlation values compared to WH codes making the cross-correlation values of these codes high. The correlation functions and the MSAAC and MSACC values of OVSF codes are almost same as that of MWH codes. The correlation values of OVSF codes depends on the repetitive sequence. In Table II the correlation values of OVSF codes are for the repetitive sequence $\{1, 1, 1, -1\}$ and it is seen that with this repetitive sequence the obtained OVSF codes have less correlation values. The orthogonal Gold codes have the correlation values similar to that of original Gold codes.

TABLE I
Aperiodic Correlation Measures for PN Sequences of Length 63 Bits

Sequence	MSAAC	MSACC	FoM	Max-CC
Maximal	0.4429	–	2.2577	–
Gold	0.9750	0.9849	1.0256	0.3333
Gold-Like	0.9227	0.9859	1.0838	0.2857
Barker (13 bit)	0.0710	–	14.0833	–
Barker-Like	0.6547	1.0546	1.5274	0.9841
Small Kasami	0.7604	0.9098	1.3151	0.2222
Large Kasami	0.9148	0.9979	1.0932	0.9524

TABLE II
Aperiodic Correlation Measures for Orthogonal Codes of Length 64 Bits

Sequence	MSAAC	MSACC	FoM	Max-CC
Walsh Hadamard	10.3906	0.8531	0.0962	0.9844
MWH	5.3281	0.9154	0.1877	0.9531
OVSF	5.3281	0.9154	0.1877	0.9844
Orthogonal Gold	0.9739	0.9848	1.0268	0.3438

Correlation measurements of encryption with different 31/32 bit sequences are provided in Table III which can be compared with Tables I and II. Also, correlation measures for different repetitive sequences of OVSF code set of length 16 and 32 are provided in Table IV from which one can choose the optimum sequence according to the requirement.

B. Speech Encryption with PN Sequences

Speech signal sampled at 8 kHz is quantized with 2^{16} levels, and it is encrypted with the above PN sequences as described in Section 5 and the residual intelligibility within the encrypted speech signal is observed. Fig. 2(a) shows the time domain representation of 30 ms voiced speech segment taken from the speech utterance */vande mataram/* and Fig. 2(b) is its spectrogram representation computed by 512 point fast Fourier transform (FFT). The encrypted speech signal and its spectrum by using all the sequences are compared with

TABLE III
CORRELATION MEASURES OF A FEW PN/ORTHOGONAL SEQUENCES OF LENGTH 31/32 BITS

Sequence	MSAAC	MSACC
m-sequences (31 bits)	0.4807	-
Gold Codes (31 bits)	0.6866	0.7451
Barker Sequence	0.8127	01.0505
WH Codes	6.5938	0.7873
MWH Codes	3.2188	0.8962

TABLE IV
CORRELATION MEASURES FOR OVSF CODE SET OF LENGTH 16 AND 32 BITS

Repetitive Sequence	$N = 16$		$N = 32$	
	MSAAC	MSACC	MSAAC	MSACC
$(-1,-1,-1,-1)$	4.0625	0.7292	6.5937	0.7873
$(-1,-1,-1,1)$	1.8125	0.8792	3.2188	0.8962
$(-1,-1,1,-1)$	1.8125	0.8792	3.2188	0.8962
$(-1,-1,1,1)$	4.0625	0.7292	6.5938	0.7873
$(-1,1,-1,-1)$	1.8125	0.8792	3.2188	0.8962
$(-1,1,-1,1)$	4.0625	0.7292	6.5937	0.7873
$(-1,1,1,-1)$	4.0625	0.7292	6.5938	0.7873
$(-1,1,1,1)$	1.8125	0.8792	3.2188	0.8962
$(1,-1,-1,-1)$	1.8125	0.8792	3.2188	0.8962
$(1,-1,-1,1)$	4.0625	0.7292	6.5938	0.7873
$(1,-1,1,-1)$	4.0625	0.7292	6.5937	0.7873
$(1,-1,1,1)$	1.8125	0.8792	3.2188	0.8962
$(1,1,-1,-1)$	4.0625	0.7292	6.5938	0.7873
$(1,1,-1,1)$	1.8125	0.8792	3.2188	0.8962
$(1,1,1,-1)$	1.8125	0.8792	3.2188	0.8962
$(1,1,1,1)$	4.0625	0.7292	6.5937	0.7873

this voiced speech segment. If we encrypt each sample of the speech signal with a different binary sequence, the residual intelligibility is less as compared with the encrypted speech signal with a single sequence. The code set which have more number of sequences with good correlation properties have better performance and the encrypted speech signal sounds like a noise signal.

1) m-Sequences: Speech encryption using m-sequences reduces the residual intelligibility of the encrypted speech but they are not suitable for real time applications since, there is only one possible sequence of given length. Fig. 2(c)-(d) shows the encrypted speech waveform and its spectrogram representation using m-sequence of length 63 bits. From the Fig. 2(c) we can observe that the periodicity of the speech signal is retained in the encrypted signal.

2) Gold Sequences and Gold-like Sequences: The performance of Gold sequences is similar to that of the Gold-like sequences The performance of the gold sequences is good compared to m-sequences since, by using different Gold sequences the sample to sample correlation is also reduced. The size of these families is large, but practically gold codes are more suited for speech encryption. Fig. 2(e)-(f) shows the encrypted speech signal and its spectrum using Gold sequences and Fig. 2(g)-(h) are the encrypted speech and its spectrogram representations for Gold-like sequences.

3) Barker Sequences: Barker sequences of some length only are existing and the number of known Barker sequences are also less, so these sequences are not suitable for speech encryption. Fig. 2(i)-(j) shows the encrypted speech signal and its spectrum using Barker sequence of length 13 bits. Most of the information is present in the encrypted speech signal using Barker sequences.

4) Barker-like Sequences: Barker sequences gives better performance compared to other sequences. The residual intelligibility of the encrypted speech signal using Barker sequences is very less, it sounds like a noise signal. Fig. 2(k)-(l) shows the encrypted speech signal and its spectrum using Barker sequences. From the figure, we can observe that there is no periodicity preserved in the encrypted signal, the signal looks like a random noise signal and the spectrum of the encrypted signal is flat, the formant peaks are suppressed in the spectrum.

5) Kasami Sequences: The correlation values of small set of Kasami sequences is less but the number of sequences in the set is less, so the residual intelligibility of the encrypted speech is somewhat high as compared with the Barker sequences. Large set of Kasami sequences have better performance compared with the all other sequences since the number of large Kasami sequences are more, so the residual intelligibility is less. If the number of sequences are more, by encrypting each sample with different sequences the sample to sample correlation in speech signal is better removed, so the residual intelligibility of the encrypted signal is less. Fig. 2(m)-(n) are the time domain and spectrogram representations for encrypted speech signal using small set of kasami sequences and Fig. 2(o)-(p) shows the encrypted speech signal and its spectrum using large set of Kasami sequences.

C. Speech Encryption with Orthogonal Codes

Orthogonal codes of length 64 bits are generated and each sample of the coded speech sample is XOR operated with the orthogonal codes to get encrypted speech sample. Each sample of the speech signal is represented with 16 bits, and four samples of the original speech signal are XOR operated with the 64 bit sequence to get four samples of the encrypted speech signal.

1) Walsh Hadamard Codes: WH codes satisfies the orthogonal property but they have poor correlation properties and the residual intelligibility present in the encrypted speech signal is also more. Fig. 3(a)-(b) are the waveform of encrypted speech signal and its spectrogram representation using WH codes.

2) Modified Walsh Hadamard Codes: Fig. 3(c)-(d) shows the encrypted speech signal and its spectrogram representation using MWH codes. The performance of MWH codes is good compared with the WH codes because these codes have better correlation properties compared to WH codes. The residual intelligibility of the encrypted speech signal is also less compared to WH codes.

3) Variable Length Orthogonal Codes: Fig. 3(e)-(f) shows the encrypted speech signal and its spectrum using OVSF codes with repetitive sequence $\{1, 1, 1, -1\}$. The MSAAC and MSACC values for this repetitive sequence are less and the residual intelligibility of the encrypted speech signal is also less.

4) Orthogonal Gold Codes: The performance of Orthogonal Gold codes is same as that of original Gold codes since both have similar correlation values and the number of sequences are also nearly equal. Fig. 3(g)-(h) are the time

domain and spectrogram representations for encrypted speech signal using orthogonal Gold codes.

VII. Conclusion

In this paper, we have investigated different PN and orthogonal sequences that are appropriate for speech encryption by the correlation measures to test the randomness of these binary sequences. The sequences which have less correlation values have more noise like properties and make the speech signal less intelligible by reducing the correlation among successive speech samples by encrypting the speech signal with those sequences. The security offered by the system depends on the number of PN sequences present in the code set. Also, the residual intelligibility is very less if each sample of the speech signal is encrypted with different sequence instead of using same sequence for each sample therefore, the signal is better encrypted if the code set contains more number of sequences. Among all the sequences, m-sequence and Barker sequences have very less auto-correlation values and high FoM values but these sequences are not suitable for encryption since there is only one possible sequence for a given shift register length. The security offered by these sequences is thus less. Barker-like sequences have better auto-correlation properties and the residual intelligibility within the encrypted speech signal is less but generation of these sequences is complex when compared with other sequences. The large set of Kasami sequences have good correlation values, high FoM value and these sequences have wide flat spectrum which makes these better suited for speech encryption. The encrypted speech signal using large Kasami sequences sounds as a noise like signal. For a given shift register length the number of possible large Kasami sequences are also large so the security offered by these sequences is also large. The generation of these sequences is also easy when compared with Barker like sequences. These sequences are therefore effective for speech encryption. The WH, MWH and orthogonal Gold codes have zero cross-correlation when there is no shift in the sequences. They have, however, very high correlation values if there is any shift in the sequences. These sequences thus may not serve as a good option for speech encryption.

References

[1] H. J. Beker and F. C. Piper, *Secure Speech Communications*, London: Academic Press, 1985.

[2] W. Stallings, *Cryptography and Network Security*, Englewoods Cliffs, NJ: Prentice Hall, 2003.

[3] W. Diffe and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, pp. 644-654, Nov. 1976.

[4] N. S. Jayant, B. J. McDermott, S. W. Christensen and A. M. Quinn, "A comparison of four methods for analog speech privacy," *IEEE Trans. Commun.*, vol. COM-29, pp. 18-23, Jan. 1981.

[5] B. Goldburg, S. Sridharan and E. Dawson, "Design and cryptanalysis of transform based speech scramblers," *IEEE J. Selected Areas Commun.*, vol. 11, no. 5, pp. 735-744, June 1993.

[6] R. L. Pickholtz, D. L. Schilling and L. B. Milstein, "Theory of spread spectrum communications — A tutorial," *IEEE Trans. Commun.*, vol. COM-30, no. 5, May 1982.

[7] E. H. Dinan and B. Jabbari, "Spreading codes for direct sequence CDMA and wideband CDMA cellular networks," *IEEE Commun. Magazine*, vol. 36, no. 4, pp. 48-54, Sep. 1998.

[8] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd Ed., NJ: Prentice Hall, 2001.

[9] J. H. Lindholm, "An analysis of the pseudo randomness properties of the subsequences of long m-sequences," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 569-576, July 1968.

[10] I. Oppermann and B. S. Vucetic, "Complex spreading sequences with a wide range of correlation properties," *IEEE Trans. Commun.*, vol. COM-45, pp. 365-375, March 1997.

[11] L. T. Wang and E. J. McCluskey, "Linear feedback shift register design using cyclic codes," *IEEE Trans. Comput.*, vol. 37, pp. 1302-1306, Oct. 1988.

[12] A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes," *Theoretical Computer Science*, vol. 259, pp. 679-688, May 2001.

[13] D. V. Sarwate and M. B. Pursley, "Correlation properties of pseudo random and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593-619, May 1980.

[14] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. IT-11, no. 4, pp. 533-537, Oct. 1965.

[15] D. G. Luenberger, "On Barker codes of even length," *Proc. IEEE,* vol. 51, pp. 230-231, Jan. 1963.

[16] C. K. Chan and W. H. Lam, "Generalised Barker-like PN sequences for quasisynchronous spread spectrum multiple access communication systems," *IEE Proc. Commun.*, vol. 142, no. 2, pp. 91-98, April 1995.

[17] X. Wang, Y. Wu and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Trans. Broadcasting*, vol. 50, no. 3, pp. 244-252, Sep. 2004.

[18] V. Milosevic, V. Delic and V. Senk, "Hadamard transform application in speech scrambling," *Proc. IEEE*, vol. 1, pp. 361-364, July 1997.

[19] Tai-Kuo Woo, "Orthogonal variable spreading codes for wideband CDMA," *IEEE Trans. Vehicular Tech.*, vol. 51, no. 4, pp. 700-709, July 2002.

[20] B. Wysocki and T. A. Wysocki, "Modified Walsh Hadamard sequences for DS-CDMA wireless systems," *School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Australia.* [Online] Available: www.elec.uow.edu.au/staff/wysocki/publications/J1.pdf.

[21] A. Mitra, "On Pseudo-Random and Orthogonal Binary Spreading Sequences", to appear in *Int. J. Info. Tech.*, 2007.

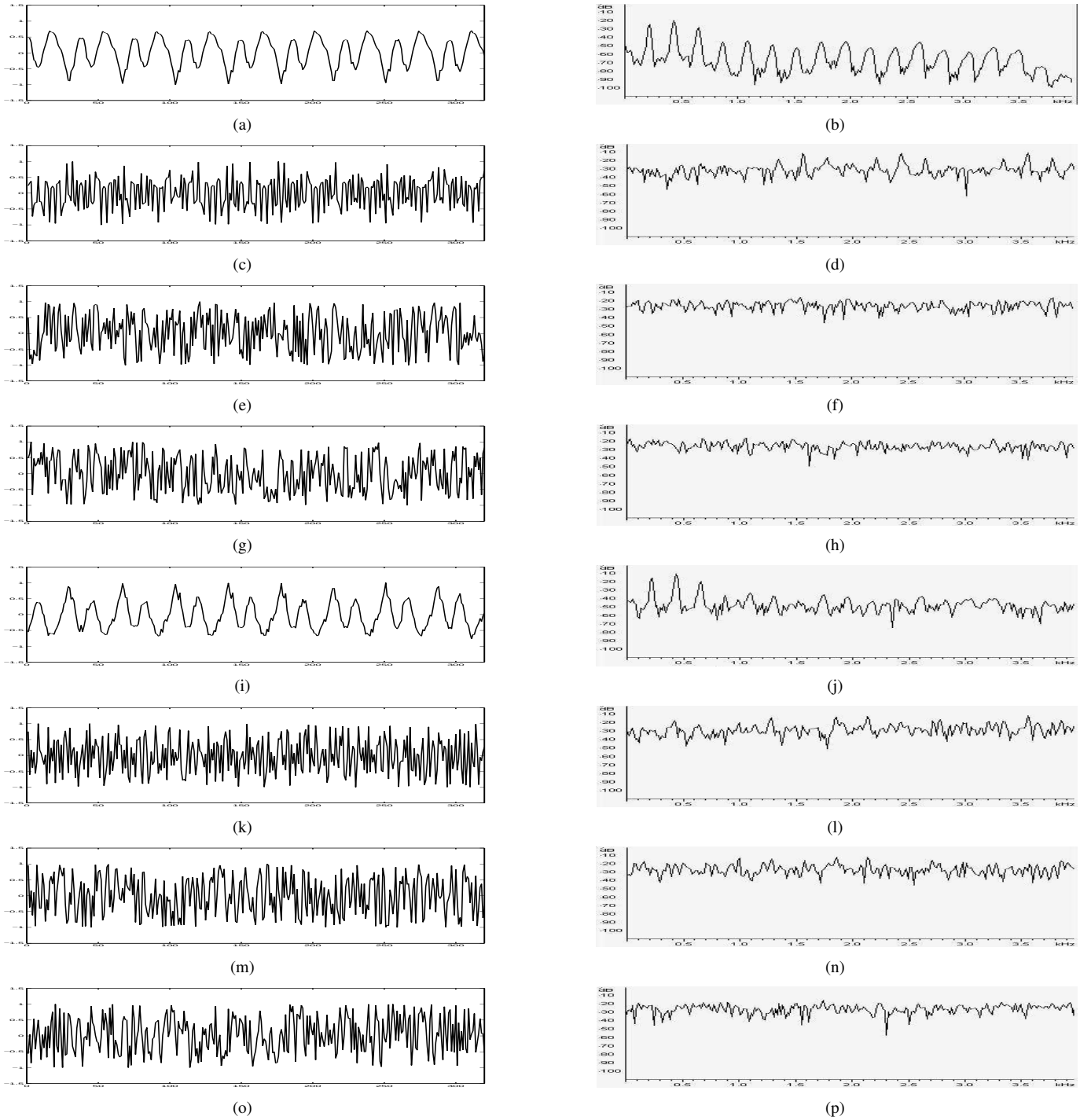

Fig. 2. Time domain and its spectrogram representation for 30 ms speech segment of the utterance */vande mataram/* are shown in (a)-(b). The encrypted time domain speech segment and its spectrogram are shown using: (c)-(d) m-sequences, (e)-(f) Gold sequences, (g)-(h) Gold-like sequences, (i)-(j) Barker sequences, (k)-(l) Barker-like sequences, (m)-(n) small set of Kasami sequences, and (o)-(p) large set of Kasami sequences.

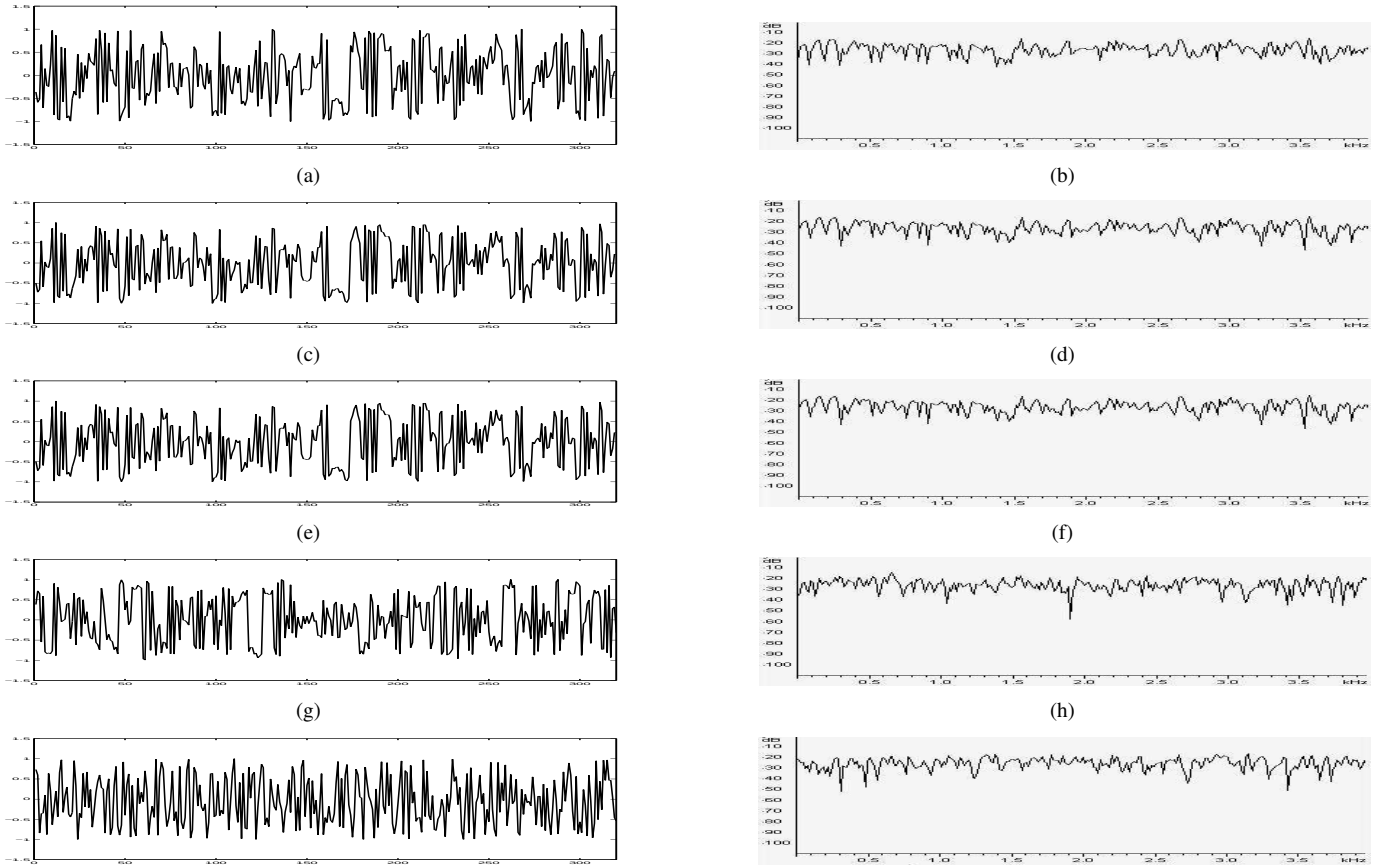

Fig. 3. Time domain and its spectrogram representation for the same 30 ms speech segment when encrypted with: (a)-(b) orthogonal codes, (c)-(d) Walsh Hadamard codes, (e)-(f) modified Walsh Hadamard codes, (g)-(h) OVSF codes, and (i)-(j) orthogonal Gold codes.