PERFORMANCE BOUNDS FOR ANALOG SIGNAL ENCRYPTION

Allen Gersho
Dept. of Electrical & Computer Engineering
University of California,
Santa Barbara, CA 93106

ABSTRACT

It is sometimes desirable to perform analog scrambling on an analog signal rather than digitizing the signal and performing digital encryption and transmission. Analog signal encryption is usually assumed to offer only a very limited degree of security. However, it is in fact possible to achieve perfect secrecy (just as is obtained with the one-time pad, for example) in encrypting an analog signal. The price paid for perfect secrecy is an inevitable degradation in the quality of the recovered analog signal. Under the constraint of perfect secrecy, the minimum possible degradation can be specified, at least in principle. This minimal degradation is a decreasing function of the key size for a fixed length message or key rate for an ongoing message. This bound on performance is determined by the rate distortion bounds for optimal digitization of the analog message.

INTRODUCTION

Many schemes have been developed for scrambling of analog signals to achieve varying degrees of privacy. Nevertheless, there has been very little if any theory to indicate the fundamental limits on what can be achieved. On the other hand, the encryption of digital signals is quite well developed. Theoretical results exist and high security techniques are readily available.

One approach to analog encryption is to first digitize the analog message, then encrypt digitally. The receiver decrypts and then reconstructs an approximation to the original analog message. But it is not known if this is indeed the most effective approach. Since the encrypted digital must be converted into an analog waveform for transmission over an analog channel, this approach is actually connverting an analog message into another analog waveform using digits as an intermediary. Hence, digital encryption is simply a special way of doing the needed analog to analog transformation.

In the field of speech encryption, it is widely recognized that there is a trade-off between the degree of security and the quality of the recovered speech. However, the fundamental

nature of this trade-off is not well understood. In speech scrambling schemes where digitization is not used as an intermediary, key size is closely linked to cost or complexity of the scheme; consequently, the key size in effect controls the trade-off between degree of security and degradation of the recovered speech. In encryption schemes that first digitize the speech, high security is obtained by using a key size that is in effect one bit of key for each bit of digitized speech. In this case, high security is available, but the quality of the recovered speech is limited directly by the bit rate and hence, indirectly by the key size.

The key size is the number of distinct keys producing distinct scrambling transformations. Generally, we assume that a key is chosen at random from the ensemble of possible keys. For a given degree of security, the key size should always geared to the total length of the message or messages to be encrypted before changing the key. For an ongoing message it is more appropriate to consider the key rate which is the ratio of key size to message length or the number of key bits per, unit time of message transmission. There is clearly a need for a better understanding of the fundamental trade-offs involved in analog signal encryption.

Recently, a general model for analog encryption was formulated [8] under the assumption of perfect secrecy and a constraint on key size. Here we clarify these results and their implications. The conclusion is that analog encryption is not fundamentally better than encryption via digitization. On the other hand, there is no reason to believe that analog encryption is fundamentally inferior to digital encryption.

PRIOR WORK

Existing scrambling devices, based largely on ad hoc designs, generally used rolling code bandsplitting or time segment permutation or a combination of these techniques. Most of these devices offer workable but “Model T Ford” solutions to the need for privacy and are grossly inadequate for this modern age of sophisticated signal processing methodology and large scale integration technology. The systems usually suffer from one or more of the following deficiencies:

a) residual intelligibility in the scrambled signal, allowing partial detection of contents by eavesdroppers,
b) greatly degraded quality of the recovered signal after descrambling,
c) excessive processing time delay for applications such as two-wire voice telephony,
d) need for an expanded bandwidth transmission channel
e) easily descrambled by an eavesdropper with modest technical resources,
f) excessively complexity and cost.

Prior appraoches to speech scrambling center largely on what might be called a “jig-saw puzzle” approach. The waveform or its spectrum is divided into segments and the

segments are permuted to form a scrambled signal with much reduced intelligibility. If the scrambled signal is transmitted over a sufficiently benign channel, the receiver can isolate these segments and rearrange them back into order. Inverting and/or permuting frequency bands with a time varying permutation is a common procedure, but a high residual intelligibility results. Permutation of time segments within a block of speech requires relatively long segments to avoid bandwidth expansion and the result is a large processing time delay as well as some residual intelligibility. Combining both frequency and time domain operations offers low residual intelligibility but also a notably degraded quality of the recovered speech signal (after descrambling). The key idea of a jig-saw approach is that sufficiently large signal “pieces” are being transmitted intact so that the signal integrity is preserved in the face of most channel degradations that would not bother the unscrambled signal. A problem with this approach (as with any jig-saw puzzle with large identifiable pieces) is that it is relatively easy to reconstruct the original without knowing how the pieces were mixed up.

A third approach is modulo masking where the analog smaples of the speech are altered by Modulo addition with pseudorandom amplitudes. This method expands the bandwidth to the half sampling rate and requires sophisticated channel equalization.

Several studies of transform domain scramblers have been proposed but never implemented. In this approach a group of speech samples are transformed by a linear matrix operation, the transformed values are then permuted, and the inverse transform is then forged and the resulting samples transmitted.

One interesting technique introduced by French [5,6] was the permutation of time segments using a sliding block method. Previously the signal was partitioned into fixed blocks and segments within each block were rearranged. With this approach, the artificial boundary between blocks disappears and the scrambled segments can be separated much farther apart for a given segment length and processing time delay. An important problem for which fully effective solutions are not known is the design of suitable permutation sequences for such a scheme. The approach still suffers from long processing delays. French’s work led to workable scramblers but is limited in security due to the nonuniform distribution of time delays with his permutation rule and due to the basic segment length needed to avoid bandwidth expansion.

An interesting approach studied briefly at Jet Propulsion Labs but never implemented or published is the use of a sliding block approach on individual samples of the signal rather than on segments.[10,18] The JPL scheme requires effective permutation rules to avoid bandwidth expansion.

PERFECT SECRECY

Perfect secrecy is the condition where the enciphered signal is statistically independent of the original message. If this condition is satisfied, observation of the ciphertext is totally useless to the cryptanalyst. It is in fact achievable for digital signal encryption as in the well known one-time pad which requires one bit of randomly generated key for each message bit.

DEGRADATION OF RECOVERED ANALOG SIGNAL

In analog encryption we must always expect and tolerate a certain amount of degradation of the recovered analog message. Random noise on the channel of course introduces degradation even if nothing else does. Assume we have some suitable measure of degradation for comparing the original and recovered signals. We then can define an "optimal" encryption system as one for which the degradation is the least possible subject to the constraints of perfect secrecy and a fixed key size.

Any digitization system will of course introduce some degradation due to quantization of the analog amplitudes.

PERFORMANCE LOWER BOUND

Suppose we could design the very best digital encoding system possible for a given bit rate. Then we could achieve perfect secrecy encryption by modulo 2 addition of one key bit with each message bit, the resulting signal could be applied to a modem producing an analog waveform, transmitted, and at the receiver, the demodulated bit stream can be decrypted and the decoder finally will produce a recovered analog signal. If we neglect channel errors, this scheme introduces a degradation only due to the quantization or source coding process and it does achieve perfect secrecy. This scheme achieves a performance in degradation versus key rate that is exactly equal to the performance of the optimal source coding scheme in degradation versus encoded bit rate. This gives a lower bound on the best achievable performance of any analog encryption system. In other words, the best possible analog encryption system (for a given degradation and key rate) should do at least as well as the above scheme which uses digital encryption as an intermediary.

PERFORMANCE UPPER BOUND

It is less trivial to determine whether it is possible for an analog encryption system to do better than the above performance. In the previous study [8] it was shown that in fact we cannot. In other words, no analog encryption system can achieve a better trade-oft between degradation and key rate than a digital encoding system for the same analog

signal can achieve in trade-off between degradation and bit-rate. Although not altogether surprising, the result is not so apparent. After all, how can we prove that no matter what kind of analog processing operation you do for scrambling, by whatever jig-saw puzzle or other methods, you cannot do better than this performance bound? The proof is a bit tricky and will not be given here. The basic idea is to suppose you found some fancy analog scrambling system that gives less degradation than the above bound for a given key rate and achieves perfect secrecy. The basic idea is to show that the key stream available to the receiver contains all the information needed to recover the original analog signal with the given degradation. and that this would imply that we could digitize and recover an analog signal with a degradation lower than theoretically possible for the given bit rate.

EXAMPLE

To illustrate the implications of our main result, consider the case of speech encryption. Suppose the message is a 10 second segment of speech bandlimited to 4 kHz and sampled at a rate of 10 kHz. The message is a discrete-time analog signal that can be viewed as a random vector of dimension 100,000. The possible values it can take on is based on the ensemble of all possible speech segments of 10 seconds duration. Suppose we digitize with the best possible LPC encoding scheme operating at a rate of 4800 bits per second. The digitized message then consists of 48,000 bits. Let D denote the degradation of the reconstructed speech segment, using some suitable performance measure. Finally, suppose we have a key size of 48,000 bits. Then, by the one-time pad approach we may encrypt this speech segment with perfect secrecy via digitization and digital encryption and recover the signal with degradation D.

Now assuming the LPC encoding system is optimal, we can use this scheme to bound the performance of any analog scrambling whatever that operates on a 10 second speech segment using a key size of 48,000 bits. The conclusion is simply that no such system can achieve a degradation of the recovered signal less than D.

Of course the key size discussed here is rather unrealistic. Most speech scrambling schemes use very limited number of distinct scrambling transformationson a 10 second segment of speech. Usually this limitation is a result of the desire to avoid expanding the bandwidth of the scrambled signal. They may achieve a degradation lower than D, but only at the price of having very low security - far from the ideal “perfect secrecy”. Most such systems have some degree of residual intelligibility in the scrambled signal.

CONCLUDING REMARKS

Perfect secrecy is of course a mathematical idealization and is rarely achievable in practice. The key size must be small for practicality while the message size is usually very

large. With suitable nonlinear pseudorandom sequence generators a short key can be used to generate a long pseudorandom sequence which in effect is used as a “pseudokey” or a “keystream”. That keystream may then be used for encryption as if it were a true key. If the key expansion is effectively chosen and the original key size is modestly large (100 bits could be quite adequate), then the security of such a system could be extremely high, although it would not be perfect secrecy. It seems plausible to expect that the results of this paper remain valid if the constraint of perfect secrecy is replaced with a more realistic and suitably defined constraint of “high security”.

BIBLIOGRAPHY

[1] W. Baschlin, “The Integration of Time Division Speech Scrambling into Police Telecommunication Networks,” Proc. 1977 Int’l Conf. on Crime Countermeasures, Science and Engr., pp. 141-144, 1977.

[2] Erling Belland and Nancy Bryg, “Speech Signal Privacy System Based on Time Manipulation,” 1978 Carnahan Conference on Crime Countermeasures, University of Kentucky.

[3] E.R. Brunner, “Efficient Speech Scrambling: An Economic solution to the Secure Voice Communication Problem,” Proc. Int’l Conf. on Commun. Equipment and Systems, Brighton, Great Britain, June 8-11, 1976.

[4] W. Ensslin, “Some Methods of Speech Scrambling on Broadcast Channels,” Elektrotech. Z. pt. B, Vol. 14, No. 12, pp. 324-326, June 11, 1962.

[5] R.C. French, “Speech Scrambling and Synchronization,” Philips Res. Rep. Suppl. , N. 9, p. 115, 1973. Also Eindhoven Univ. Techn. , The Netherlands.

[6] R.C. French, “Time Division Scrambler,” Conf. on Signal Processing Methods for Radio Telephony,” IEE, pp. 134-138, May 1970.

[7] K.-H. Georgi, “Sprachverschliisselung mit dem Transformationsvocoder,” Nachrichtentech. Zeit., Vol. 30, No. 10, pp. 791-793, 1977.

[8] A. Gersho, “Perfect Secrecy Encryption on Analog Signals,” presented at IEEE Int’l Symp. on Information Theory, June 1979, to be published.

[9] A. Gersho, “Analog Signal Encryption: Scrambling versus Digitization,” Conf. Rec., IEEE National Telecom. Conf., Washington, DC, pp. 43.6.1-43.6.2, 1979.

[10] R.M. Goldstein and E.C. Posner, “Permutation Transformation of Audio,” JPL Space Program Summary 37-61, Vol. 3, Dec. 1, 1969 to Jan. 31, 1970.

[11] G.E. Goode, “New Developments in Data and Voice Security,” Proc. IEEE Electronics Security Systems Symp., 1973.

[12] G. Guanella, “Automatic Speech Scrambling,” Brown Boveri & Co., Ltd., Report No. CH-E7.30038.2E, Switzerland.

[13] H.P. Hartmann, “Analog Scrambling vs. Digital Scrambling in Police Telecommunication Networks,” Proc. 1978 Carnahan Conf. on Crime Countermeasures, pp. 47-51, 1978.

[14] N.S. Jayant, “Speech Encryption by Manipulation of LPC and Waveform-Code Parameters,” Conf. Record, Int’l Conf. on Communication, 1977.

[15] David Kahn, “The Codebreakers,” MacMillan, New York, pp. 549-560, 1967.

[16] Subhash C. Kak, N.S. Jayant, “On Speech Encryption Using Waveform Scrambling,” BSTJ, Vol. 56, No. 5, pp. 781-808, May-June 1976.

[17] K.H. Kirchhofer, “Secure Voice Communication,” Inter. Defense Review, Vol. 9, No. 5, October 1976.

[18] L. Kleinrock, “A Simple Sequence-Permutation Method,” JPL Space Program Summaries, Vol. 3, pp. 37-62, Feb. I - March 31, 1970.

[19] A.M. McCalmont and J.R. Eramo, “Communications Privacy Telecommunications,” Vol. 4, No. 10, p. 34, 36, October 1970.

[20] R.E. Nelson, “A Guide to Voice Scramblers for Law Enforcement Agencies,” National Bureau of Standards, Special Publication 430-8, U.S. Dept. of Commerce, December 1976.

[12] V.J. Phillips, M.H. Lee, and J.E. Thomas, “Speech Scrambling by the Reordering of Amplitude Samples,” Radio and Electronic Engineer, Vol. 41, No. 3, pp. 99-112, March 1971.

[22] V.J. Phillips and J.K. Watkins, “Speech Scrambling by the Matrixing of Amplitude Samples,” Radio and Electronic Engineer (6B), Vol. 43, No. 8, pp. 459-470, August 1973.

[23] S. Udalov, “Microprocessor-Based Techniques for Analog Voice Privacy,” Conf. Rec. Int’l Conf. on Communication, pp. 16.4.1-16.4.5, June 1980.

[24] S.B. Weinstein, “Sampling-Based Techniques for Voice Scrambling,” Conf. Rec. Int’l Conf. on Communication, pp. 16.2.1-16.2.6, June 1980.

[25] L.R. Welch, “A Class of Sequence Permutations,” JPL Space Programs Summary, Vol. 3, 37-61, pp. 78-81, Dec. 1, 1969 - Jan. 31, 1970.

[26] A.D. Wyner, “An Analog Scrambling Scheme Which Does Not Expand Bandwidth,” Part I: Discrete Time, IEEE Trans. on Inf. Theory, Vol. IT-25, No. 3, pp. 261-274, May 1979.