View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Calhoun, Institutional Archive of the Naval Postgraduate School

A FEASIBILITY STUDY OF A HYBRID SECURE VOICE CODING PROCESSOR

John Gary Oehlenschlager

Library
Naval Postgraduate School
Monterey, California 93940

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A Feasibility Study of a
Hybrid Secure Voice Coding Processor

by

John Gary Oehlenschlager

Thesis Advisor: R. W. Adler

December 1972

T155127

Approved for public release; distribution unlimited.

A Feasibility Study of a
Hybrid Secure Voice Coding Processor

by

John Gary Oehlenschlager
Lieutenant, United States Navy
B.S.E.E., Purdue University, 1964

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 1972

Library
Naval Postgraduate School
Monterey, California 93940

ABSTRACT

An investigation of a proposed hybrid voice coding system proved the feasibility of such a system to provide a privacy voice channel with an acceptable degree of intelligibility. The proposed system is basically a voice inversion system employing a randomly generated carrier frequency for inversion. The random carrier frequency generator is controlled by a programmable, digital character generator. The hybrid system is readily adaptable to present military and civilian VHF/UHF voice communications systems at a relatively low cost and with a very minimum of equipment modification.

TABLE OF CONTENTS

LIST OF DRAWINGS

I. INTRODUCTION TO VOICE CODING SYSTEMS

Voice security systems can be divided into two general types--digital systems and analog systems. The digital systems are usually characterized by analog to digital and digital to analog converters with coding/decoding applied to the digital data stream. Analog systems are characterized by balanced mixers, oscillators and filters.

A. DIGITAL VOICE CODING SYSTEMS

Typically a digital system is wide band. Wide band is defined as being several times the unencoded base band signal width in contrast to narrow band being approximately the same bandwidth. The wide band characteristic virtually eliminates any retrofit capability without extensive rework of existing communications equipments. It does lend itself well to new system designs employing psuedo-noise transmission techniques. A digital system can be made highly secure by using complex pseudo-random encoding data streams. Figures 1 and 2 show typical digital coders/decoders.

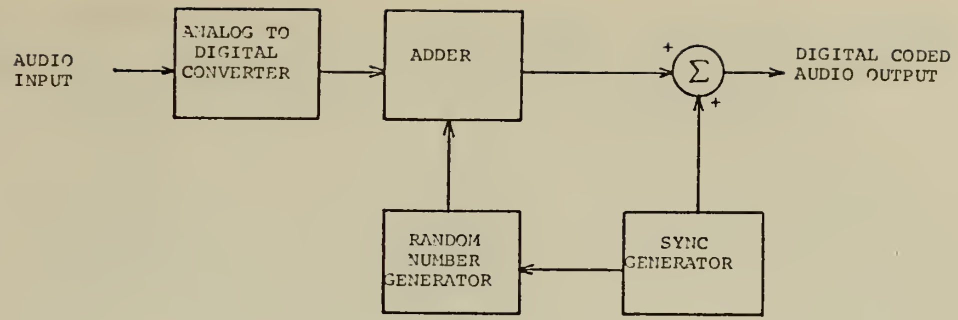

Figure 1. DIGITAL ENCODER

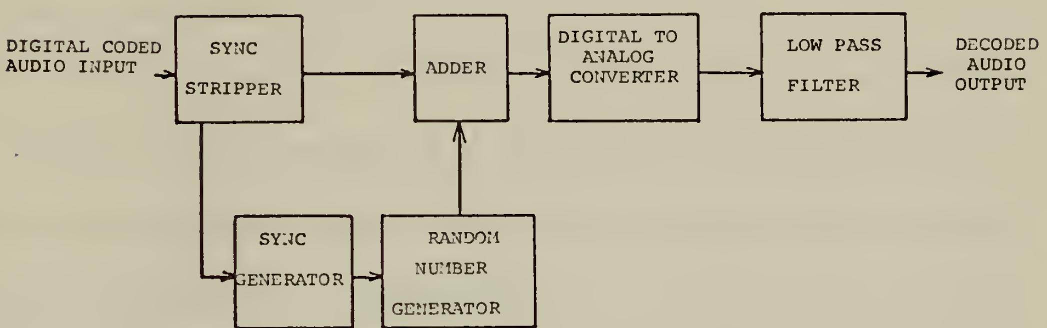

Figure 2. DIGITAL DECODER

B. ANALOG VOICE CODING

Analog systems using inversion techniques have been in use for many years dating from about 1930. Simplest of all is the straight voice inversion. Figure 3 shows a typical scheme for generating inverted voice coding.

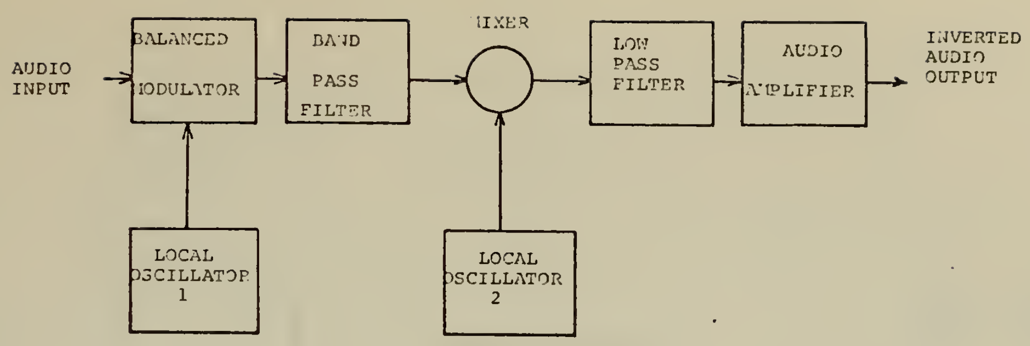

Figure 3. VOICE INVERSION SYSTEM

The relative security of this system is low. It is effective only on wire lines and against only a very casual listener on radio telephone systems. If in fact, such an encoded signal is applied to an AM transmitter, the only device necessary to effectively decode the signal is a communications receiver with a BFO! Simple inversion is somewhat more secure if applied to an FM system.

A more complex encoding system employs band splitting, inversion and band juxtaposition. In this type of system, the 300-3000 HZ voice signal is applied to a network of band pass filters. Each sub-band is then processed in a manner similar to the simple inverter, except that each sub-band is not necessarily returned to its original position, nor need it be inverted. A simple three band system is shown in Figure 4.

This system provides an extra degree of security in that the total system variables include (1) number of sub-bands, (2) inversion or non-inversion of each sub-band (3) the translation scheme utilized and (4) the programming scheme used. This system can be considered to be

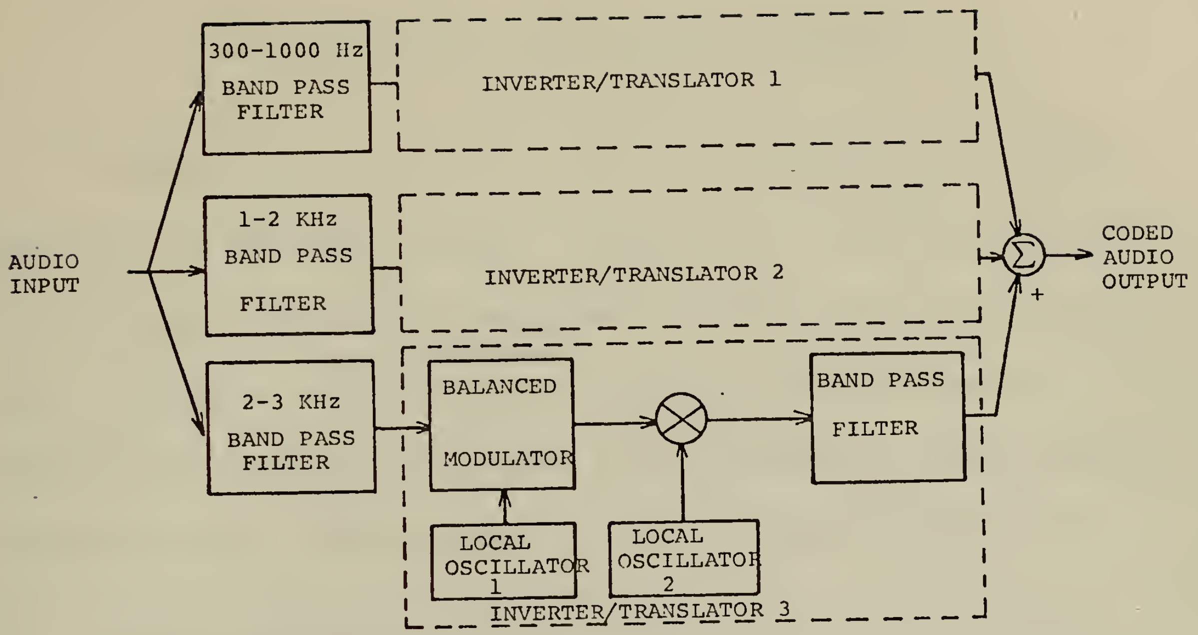

Figure 4. MULTI BAND ENCODER

of medium security if the information being transmitted is of a highly volatile nature. For non-volatile information, this system provides only nuisance value. With the use of spectrum analyzers, tuneable filters and a methodic reconstruction plan, the original signal can be reconstructed. In any case transmission security is increased only by system programming flexibility and use of a secure method of preprogramming the system such as changing the program on an hourly, daily or weekly basis.

The primary objection to this system is the necessity for the many bulky bandpass filters. Digital filtering techniques might be considered as a replacement for lumped constant filters.

II. PROPOSED VOICE CODING SYSTEM

The design of a new voice encoder/decoder system was undertaken with the following criteria. First the system must be compatible with existing radio telephone equipment. Second, the system must provide a reasonable amount of privacy against not only the "snooper" on the RF channel but also against loss of the equipment or compromise of equipment design. Third, the system must be reasonable in cost.

A. SYSTEM DESIGN REQUIREMENTS

The requirement to be compatible with present radio telephone restricts the voice communications channel to 300 to 3000 HZ with an additional data signalling channel in the 60 to 300 HZ region. This constraint rules out any high data rate digital coding system. Since the system must provide a reasonable degree of privacy, it should be at least equivalent to a four or five band splitting/inversion system. To keep system cost to a minimum, it is necessary to avoid using the many filters associated with the band splitting system.

B. BASIS SYSTEM FOR HYBRID VOICE CODING SYSTEM

It was believed that perhaps a combination of hybrid systems using concepts from both the analog and digital voice coding systems could be used to advantage to meet the desired design criteria. The proposed system is based upon a remotely synchronized voice coder shown in Figure 5.

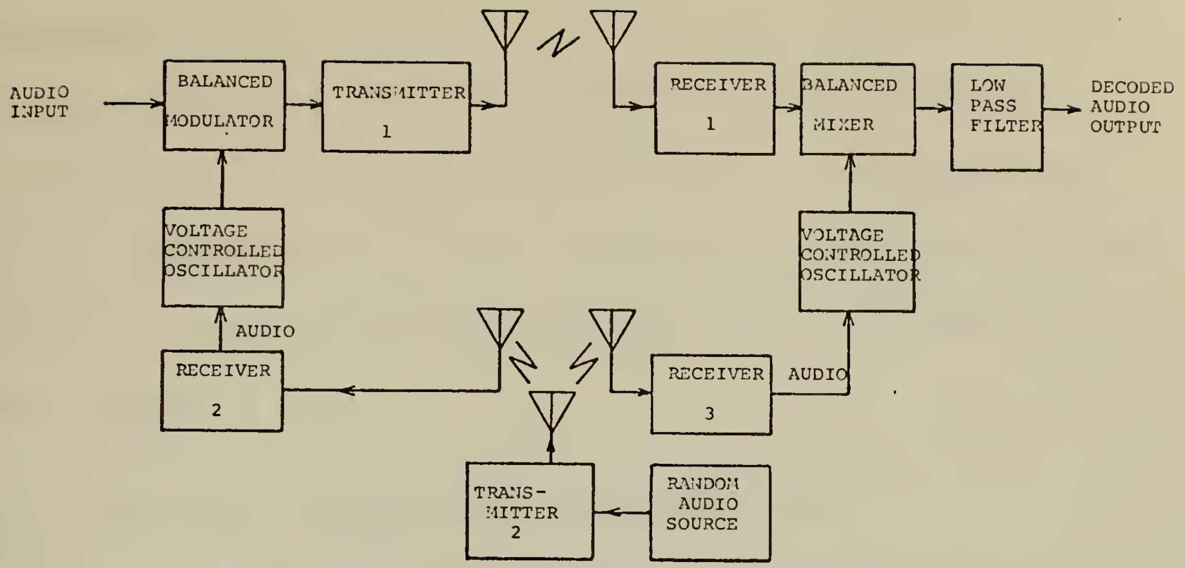

Figure 5. REMOTELY SYNCHRONIZED VOCODER SYSTEM

This is an inversion system using a signal source which can be received by both the transmitting and receiving sites. For correct operation it is required that the transmission path from the coding source transmitter 2 to receiver 2 and from transmitter 2 to receiver 3 must introduce neither additional modulation nor different distortion and that the propagation delay from transmitter 2 via receiver 2 and transmitter 1 to receiver 1 be equal to the delay from transmitter 1 to receiver 3. If both of these requirements are not met, the decoded output will not be equal to the original input signal. System privacy is dependent upon knowing what transmitter is used as the coding information source. A simple system such as this can provide a relatively private means of coding with a minimum of cost. The major problem with the system is synchronism error. In theory, there exists only

one hyperbolic line of position on which the coding information source transmitter may be located which will give the phase differential necessary for correct decoding. The LOP is actually a hyperbolic band of approximately $\pm$ 18.5 micro-seconds or $\pm$ three nautical miles. This represents a path phase differential of 10° at the highest modulation frequency (3 KHZ).

C. PROPOSED HYBRID VOICE CODING SYSTEM

The concept employed in the above system appeared to provide a reasonable approach to a new system. The proposed hybrid voice coder system is shown in block diagram in Figures 6 and 7.

The operation of the proposed system is similar to the one shown in Figure 5 with the exceptions of the integral synchronization and the use of a programmable pseudorandom frequency input to the balanced modulator.

Referring to Figure 6, the audio input signal is processed by amplification and filtering and appears as a 300 to 3000 HZ band limited signal at the input to the balanced modulator. The synchronization generator generates two outputs, one of which will apply a low frequency uncoded audio tone to the transmitter. The second output triggers the number generator according to some preset coding scheme. The output of the number generator is then converted to an analog signal which is then used to control the local oscillator frequency. The balanced modulator output is then lowpass filtered and appears as a 300 to 3000 HZ signal at the input to the transmitter.

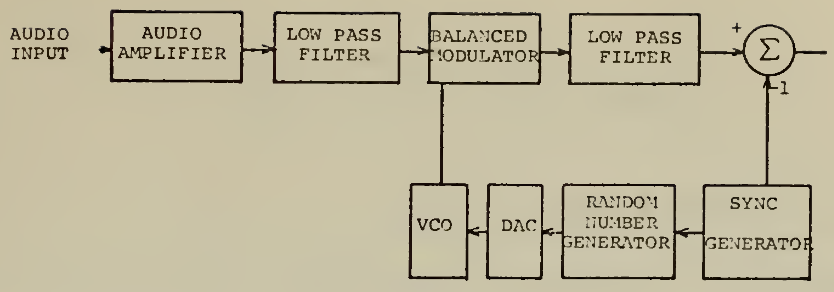

Figure 6. PROPOSED HYBRID ENCODER

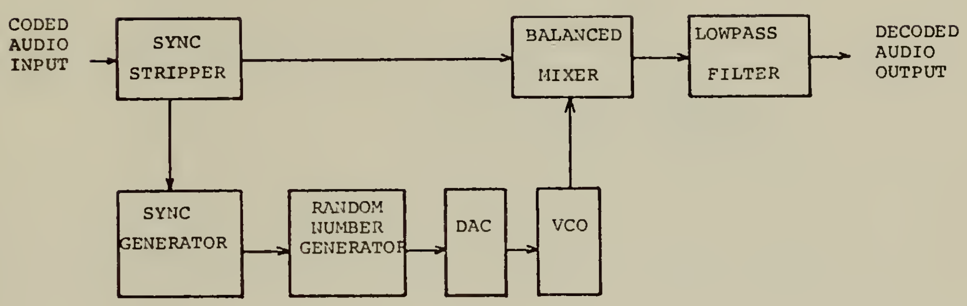

Figure 7. PROPOSED HYBRID DECODER

Decoding, shown in Figure 7, is simply an inverse operation. Synchronization information is stripped from the coded audio input and used to generate local oscillator signal which is identical to the encoder local oscillator. The coded audio and local oscillator are mixed in the balanced modulator and applied to a low pass filter. The resultant output is the original signal.

III. FEASIBILITY TEST MODEL

In order to evaluate the proposed system, a simplified test design was constructed to examine the feasibility of the system. Figure 8 is the simplified system block diagram of the test design.

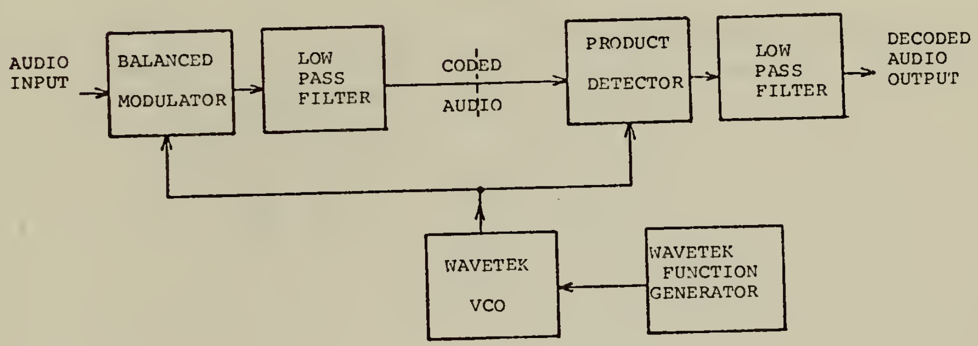

Figure 8. SIMPLIFIED TEST SYSTEM

The operation of the test circuit is quite similar to the proposed system with the sync circuits eliminated and the local oscillators replaced by a single voltage controlled oscillator driven by an audio function generator.

The audio function generator and the voltage controlled oscillator are used to generate a frequency modulated local oscillator signal for insertion into the balanced modulator and the product detector. This interconnection simulates the proper operation of the sync circuitry, random number generators and ADC/DAC circuits.

A. BALANCED MODULATOR AND PRODUCT DETECTOR

The balanced modulator and the product detector were constructed utilizing Motorola MC 1496 balanced modulator integrated circuits. The modulator and product detector are identical in design and operation. The schematic of the modulator/product detector is shown in Figure 9.

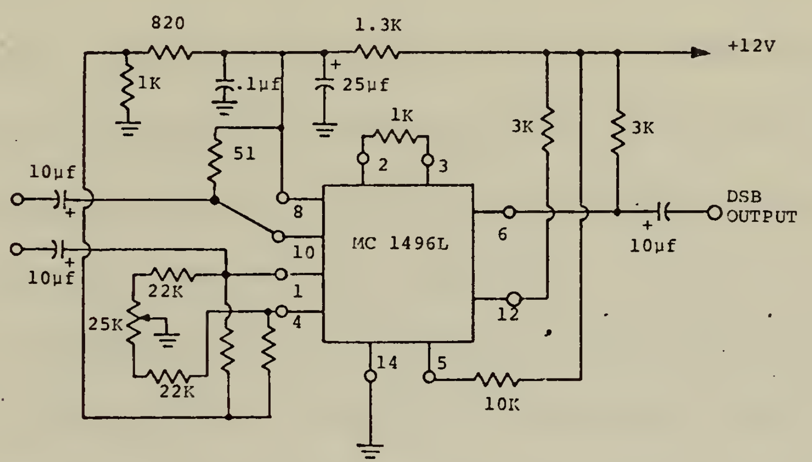

Figure 9. BALANCED MODULATOR/PRODUCT DETECTOR

B. LOW PASS FILTERS

Lumped constant low pass filters with 3 KHZ cutoff frequencies were used in the test design. Since the filters were low impedance, an IC operational amplifier with zero db gain was used between the modulator/detector and the low pass filter to avoid loading.

C. LOCAL OSCILLATOR

The local oscillator signal was simulated using a Wavetek model 130 function generator driving a Wavetek model 142 voltage controlled oscillator. The function generator and VCO both have selectable sine,

triangular and square wave outputs permitting good flexibility for observation of local oscillator waveform effects upon the vocoder intelligibility and privacy.

IV. TEST RESULTS

A. OPERATION

The voltage controlled oscillator was set for a center frequency of 3500 HZ (sine wave) and the function generator set to 45 HZ (sine wave). The function generator (warble) output amplitude was then increased to produce a decoded voice signal with a reasonable amount of distortion. Qualitative observations of the decoded signal, the coded signal and the signal as decoded by a conventional fixed frequency inversion system were made by several different observers who were all experienced in voice communications over noisy channels.

B. OBSERVATIONS

It was observed that different "warble" frequencies and waveforms produced varying effects on both intelligibility and privacy of the voice signal. In general, it was quite easy to produce a decoded voice signal with only a small amount of distortion which could not be decoded using a conventional inversion system by setting the "warble frequency within the 10 to 60 HZ range, setting the carrier deviation to a sufficient level, and by varying the "warble" and VCO wave shapes. Individual observer's reactions to a particular choice of variables were not always in agreement as to small amount of distortion

intelligibility and privacy. It was noted that the periodic nature of the "warble" did enable some observers to make a reasonably accurate "calculated" guess at some words.

V. CONCLUSION AND RECOMMENDATIONS

The qualitative testing of the test circuit proved the feasibility of a voice inversion system utilizing periodic FM modulation of the balanced modulator local oscillator. The privacy of the system was found to be much higher than the normal inversion technique with some reduction of intelligibility. The circuits employed for the encoder/decoder are well adapted to inclusion in a single medium scale integration (MSI) device.

As a continuation to the investigation of this voice coding system the following topics should be considered.

1. Use of active filters to replace lumped constant filters.

2. Use of the programmable random voltage source to replace the "warble" oscillator.

3. Testing of privacy and intelligibility using standard wordlists.

4. Designing and testing of a synchronization system suitable for inclusion with the vocoder.

5. Design of a medium scale integrated circuit containing all analog portions of the voice coder. The MSI would have the following inputs and outputs.

a. Inputs

(1) Microphone

(2) Coded audio from transceiver

(3) Control voltage to VCO

(4) Switching circuitry

b. Outputs

(1) Coded audio to transceiver

(2) Speaker

A functional block diagram for the MSI is shown in Figure 10.

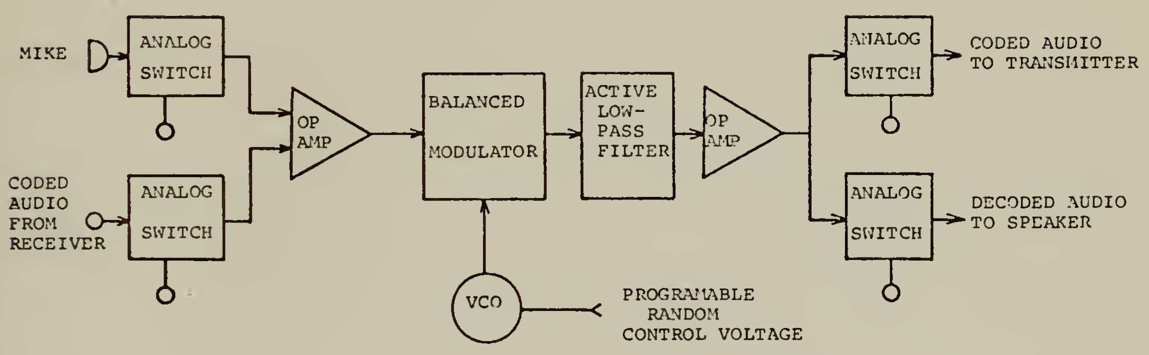

Figure 10. MSI BLOCK DIAGRAM

6. Design and testing of a MSI/LSI programmable voltage source for VCO control.

BIBLIOGRAPHY

Motorola Application Note AN-531, MC 1596 BALANCED MODULATOR, Prepared by R. Hejhall, 1971.

Schroeder, M. R., VOCODERS: ANALYSIS AND SYNTHESIS OF SPEECH: PROCEEDINGS IEEE, Vol. 54, p. 720-734, May 1966.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Asst. Professor R. W. Adler, Code 52ab Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	5
4.	LT John Gary Oehlenschlager, USN R.R. #2 Verndale, Minnesota 56481	1

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

ORIGINATING ACTIVITY (Corporate author)
Naval Postgraduate School
Monterey, California 93940

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

REPORT TITLE
A Feasibility Study of a Hybrid Secure Voice Coding Processor

DESCRIPTIVE NOTES (Type of report and, inclusive dates)
Master's Thesis; (December 1972)

AUTHOR(S) (First name, middle initial, last name)
John Gary Oehlenschlager

REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
December 1972	21	2

CONTRACT OR GRANT NO.

PROJECT NO.

9a. ORIGINATOR'S REPORT NUMBER(S)

9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

DISTRIBUTION STATEMENT

Approved for public release; distribution unlimited.

SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY
Naval Postgraduate School
Monterey, California 93940

ABSTRACT

An investigation of a proposed hybrid voice coding system proved the feasibility of such a system to provide a privacy voice channel with an acceptable degree of intelligibility. The proposed system is basically a voice inversion system employing a randomly generated carrier frequency for inversion. The random carrier frequency generator is controlled by a programmable, digital character generator. The hybrid system is readily adaptable to present military and civilian VHF/UHF voice communications systems at a relatively low cost and with a very minimum of equipment modification.

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Voice Privacy						
Voice Coder						
Hybrid Voice Coder						

141656

Thesis
02456 Oehlenschlager
c.1 A feasibility study
of a hybrid secure voice
coding processor.

OCT 73	21026
OCT 73	21026
3 NOV 73	22737
5 JUN 74	25268
MAR 79	33143
OCT 17 85	

141656

Thesis
02456 Oehlenschlager
c.1 A feasibility study
of a hybrid secure voice
coding processor.

thes02456
A feasibility study of a hybrid secure v
3 2768 000 99925 4
DUDLEY KNOX LIBRARY