UNCLASSIFIED

AD NUMBER

ADA800127

CLASSIFICATION CHANGES

TO:

unclassified

FROM:

confidential

LIMITATION CHANGES

TO:

Approved for public release; distribution is unlimited.

FROM:

Distribution authorized to DoD only; Administrative/Operational Use; 31 JAN 1942. Other requests shall be referred to Office of Scientific Research and Development, Washington, DC. Pre-dates formal DoD distribution statements. Treat as DoD only.

AUTHORITY

SOD memo dtd 2 Aug 1960; SOD memo dtd 2 Aug 1960

THIS PAGE IS UNCLASSIFIED







Speech Privacy Decoding - Final Report, January 31, 1942 - Parts I - II63157Heising, R. A.
Bell Telephone Labs. Inc., New York, N. Y.
OSRD, NDRC, Div. C, Washington, D. C.(None)OSRD-386

Jan⁴2 Confd⁴1 U.S. English 28 photos, diagrs, graphs

The object of this project was to discover and develop a means whereby speech-scrambling methods used in telephone privacy systems could be recognized and decoded. It was found that no specialized knowledge of different languages was necessary. Considerable emphasis was placed on discovering and developing methods for speeding up the dedoding process. Fart II concerns a speech-pattern machine equipped to monitor voice frequency currents submitted to it and to record a sample 1.8 sec long at any time. The speech pattern portrays frequency along the vertical axis, time along the horizontal axis, and intensity of energy by the density or blackness of the pattern. This machine, although compact and rugged, does not conform to the requirements for Army or Navy use.

Copies of this report obtainable from CADO. Electronics (3) Communications (1) Decoders (288

and the second second

recoders (28877) Telephony, Code modulated (92690)



BELL TELEPHONE LABORATORIES

January 31, 1942

3520-0BJ-EJF

DR. C. B. JOLLIFFE, Chairman Communications Section National Defense Research Committee 1530 P Street, NW Washington, D.C.

Final Report on Project C-32, Speech Privacy Decoding (Symbol No. 582)

Dear Dr. Jolliffe:

Attached are 27 copies of the final report covering the work done in accordance with the terms of a contract now under negotiation between the Office of Scientific Research and Development and the Western Electric Company on Speech Privacy Decoding.

Yours truly,

R. A. HEISING

Att. 27 copies of Final Report C-32.

}

This Document contains information affecting the National Defense of the United States within the Meaning of the Espionage Act, 0.S.C. 50; 31 and 32. Its transmission or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

NATIONAL DEFENSE RESEARCH COLLITTEE Division C, Section 1, Communications

-

Project C-32 SPEECH PRIVACY DECODING Final Report January 31, 1942

Contract No: Under Negotiation (Symbol No. 582) Western Electric Company, Inc. Bell Telephone Laboratories, Inc. Contractor: Research by:

.

.

.

NATIONAL DEFENSE RESEARCH COMMITTEE

Final Report on Project C-32

SPEECH PRIVACY DECODING

Symbol No. 582

TABLE OF CONTENTS

Page

PART I, METHOD AND RESULTS

1.	General	l
2.	Speech Patterns	2
3.	Scrambled Speech Patterns	3
4.	Special Methods for TDS	6
	4.1 Wave Form Traces 4.2 Partial Matching	6 7
5.	Further Possibilities	7
	5.1 Instantaneous Speech Patterns 5.2 Large Variable Area Patterns 5.3 Decoding by Automatic Trial 5.4 Decoding Equipment	8 8 8 9
6.	Recommendations for Increasing Privacy	9
	6.1 General 6.2 For TDS 6.3 Compounding	9 10 10
7.	Other Speech Pattern Lethods	10
8.	Records of Scrambled Speech	11
9.	Laboratory Notebooks	13
LO.	Photographs	13

Continued on Next Page

TABLE OF CONTENTS (Cont'd.)

同語

PAI	RT II - THE SPHECH PATTERN MACHINE	Page
1.	General	
2.	Description of Dress to T	1
-	Deserver of Recorder Unit	2
э.	Description of Method of Making Speech Patterns	3
	 3.1 Capturing the Speech Sample 3.2 Placement of the Teledeltos Paper 3.3 Playing Back the Magnetic Tape Recording 3.4 Frequency Analysis 3.5 Recording the Speech Pattern 	3 3 4 4 5
4.	Physical Description of Units	5
5.	Photographs	0
6.	Drawings	6
	· · · · · · · · · · · · · · · · · · ·	6

للمسعد

-1

,

-

NATIONAL DEFENSE RESEARCH COLMITTEE

Final Report on Project C-32

SPEECH PRIVACY DECODING

Symbol No. 582

PART I - METHODS AND RESULTS

1. General

The object of this project was to discover and develop general means whereby speech scrambling methods used in telephone privacy systems could be recognized and the requirements for decoding determined. Originally, it was thought that a comparison of the characteristics of different languages before and after scrambling might be required in order to recognize scrambling methods. As the work progressed, however, it appeared that no specialized knowledge of different languages is needed. Considerable emphasis, therefore, was placed on discovering and developing methods for speeding up the decoding process.

The speed of decoding will vary with different privacy systems. Some systems depend for their effectiveness only on the inability of an unauthorized listener to recognize what had been done to the speech. If he is able to recognize the scrambling method, and can build unscrambling equipment, he can thereafter decode the intercepted message directly. In such cases the only delay will be in getting started. On the opposite extreme are privacy systems which do not depend on secrecy of method. In these cases the best that can be expected is that the message, recorded in scrambled form, can be decoded piece by piece. Such methods will usually have a very large number of codes available, so that even though the method is known, the code must be redetermined every time it is changed. If the code is changed often enough, there will be not only the initial delay, but also a ratio of decoding time to message time which may reach prohibitive proportions. That is, if a one-minute message takes one hour to decode, a ten-minute message would take ten hours, unless a multiplicity of decoding teams operate simultaneously.

Between these extremes are systems in which a relatively small number of codes are available. Assuming the method is known, these cases probably can be decoded directly, either by a multiplicity of listening devices set for different codes, or by rapidly trying all the codes in succession.

It should be noted that the present project does not include study or development of systems for intercepting or recording signals. Nor does it include the development of means for reassembling scrambled speech. It is concerned only with developing means for recognizing the scrambling method, and for determining the code.

The general method developed here is based on analyses of the energy distribution in the scrambled speech as a function of both time and frequency, displayed in a particular graphic form developed at the Bell Telephone Laboratories some time ago. These analyses are hereafter referred to as "speech patterns," and it is expected that with their help any distortion in frequency or in time can be recognized both qualitatively and quantitatively. Naturally, however, this can be tried out and demonstrated only on existing privacy systems.

In addition to the speech patterns, special methods have been developed for use against an existing privacy system of the multiple-code type.

2. Speech Patterns

and the second second

Even in a steady flow of speech, the distribution of energy over the frequency range is constantly changing. Voiced sounds have a definite structure, consisting of a series of harmonics of the fundamental voice pitch, the harmonics being stronger in some frequency regions than in others. Unvoiced sounds have no such definite structure, but show a "smear" of energy which may or may not be concentrated in definite frequency regions. Words and sounds are recognized by their energy pattern in.both time and frequency. Different speakers uttering the same sentence will produce patterns which show a distinct general resemblance, but also marked differences. The speech pattern also may be considerably distorted by artificial means before the ear fails to recognize the speech, provided the distortion is not too discontinuous in frequency or time. Since privacy systems depend for their effectiveness on distorting the speech pattern beyond the possibility of recognition by the ear, it seems reasonable that this distortion would also be

visible to the eye if the scrambled speech pattern could be reduced to suitable graphic form. This is the basis of the general method developed under the present project.

The machine for producing the speech patterns is described in Part II of this report. Examples of the patterns are shown in the attached photographs. Figure 1 shows some normal speech, undistorted except that a sloping net-work was introduced in the electrical circuit to bring out the high frequency structure, since this is always weaker in normal speech than the low frequency regions. In these pat-terns, the horizontal scale is time (about 1.8 seconds is represented in each example) the vertical scale is frequency (the upper limit is 3000 cycles) and the density or blackness represents the intensity of the energy in a given region. should be noted that the resolution of the process is sufficient to separate each harmonic in the voiced sounds. This is important, as will be seen later, because normally the voice fundamental is constantly changing, that is, the voice is inflected, and since the harmonics are multiples of the fundamental, the higher harmonics show progressively more change than the fundamental. For instance, if the fundamental goes from 100 to 200 cycles the tenth harmonic goes from 1000 to 2000 cycles, a difference of 1000 cycles as compared to 100 cycles for the fundamental. The traces of harmonics in the visual speech patterns will, therefore, have greater slopes at the high end of the pattern than at the low end. This may be seen quite clearly in the examples of Fig. 1.

Figure 2 shows patterns of some vowel sounds. In making these patterns, an attempt was made to enunciate clearly, and also to keep the pitch constant (monotone), so as to show the difference in energy distribution for these sounds. These are of interest because of the possibility that the visual patterns thenselves might give clues as to the words they contain. Figure 2 also shows the effect on the frequency resolution of widening the band pass scanning filter. The wide filter gives much better resolution in time, however, as will appear subsequently. Figure 3 shows some diphthong patterns, showing transitions from one vowel to another. These pairs were chosen because their time characteristics are direct opposites.

3. Scrambled Speech Patterns

a a second and a second s

an in the second se

Figure 4 shows the output of an existing privacy system which depends on simple inversion. These patterns, incidentally, were made with a commercial telephone set including a carbon transmitter. It will be noted that in the inverted speech, the slopes of the harmonic traces become greater towards - 4

the bottom of the pattern, which is the direct opposite of normal speech as pointed out in the previous section, and is therefore a definite sign of inversion. The pattern also thins out at the bottom, but this could be altered by a suitable distorting network. No network, however, can change the slopes of the harmonic traces. Incidentally, the carrier leak chows up in the pattern, giving a direct indication of the frequency about which the inversion was performed. If the carrier is completely suppressed, however, its location may be determined by trial.

A more complicated privacy system is the split band system, used in transatlantic radiotelephony. In this system the frequency range is divided by filters into several bands, which are then arranged in a different order, and some are invertea. Figure 5 shows patterns of the output of such a syster with two different codes. Both of these samples contain portions in which the voice was quite markedly inflected. The apparatus has been so constructed that it is fairly easy to capture such samples. The fact that the frequency range has been divided into five bands is quite apparent from discontinuities in the energy distribution, and also from discontinuities in the harmonic traces. It is also quite apparent that some of the bands have been inverted because the voice cannot be inflected both up and down at once. Looking at the inflected portions, it is quite easy to find one which is either definitely inverted or definitely erect. Obviously, the other bands can then be immediately labeled inverted or erect depending on whether they have the same direction of curvature as the band previously identified. Now, since the frequency scale is linear*, the relative slopes of the harmonic traces in the different bands indicate their original position in the frequency scale; the band showing the least slope (or curvature) must originally have been the lowest band, and the band with the greatest slope (or curvature) must have been the top band.

The scrambling methods thus far illustrated alter the frequency characteristics of the speech patterns. A recently developed privacy system, known as Time Division Scrambling (TDS), operates on the time characteristics of speech. In this system successive sections of speech, each m seconds long, are divided into n short time elements, and these n elements are sent in a scrambled time sequence. The elements are much shorter than a syllable, so that each word is cut up and received as short bursts of energy in the wrong

* In the present illustrations this not true. The scale depends on the shape of the plates of an air condenser, and new plates have since been made.

ALL PROVIDENCES

order. The number of scrambled orders available increases very rapidly with n. Systems have recently been developed in which m is as short as .6 second, and n is 20, making each element 30 milliseconds. A pulse of tone is sent every m seconds to keep the transmitter and receiver in synchronism. In one such system over 60,000 codes are available, and they may be changed quite readily.

Obviously, if it is desired to decode such a privacy system, it is necessary first to evaluate m and n. Presumably a machine could then be built to unscramble the speech if the code were known. Means must then be found for determining the code, and this decoding process must be repeated every time the code is changed. If the code is changed often enough, the decoding will lag far behind the message. It is essential, therefore, that every artifice be employed to increase the speed of decoding.

Figure 6 shows some speech patterns scrambled by a TDS system. It is quite apparent that the speech has been chopped up on the time scale rather than on the frequency scale. It is quite easy to determine n by the length of the elements, and since the synchronizing pulse shows in the pattern, the most natural assumption is that m is given by the distance between these pulses or some multiple of it. In the illustration of Fig. 6, duplicate patterns were made, each element was numbered, and one of the scrambled patterns was then cut up and reassembled, giving the code. It should be noted that in the scrambled patterns a few elements within each code cycle immediately stand out as probably belonging together, particularly when voice inflection occurs. Usually the other elements in a section cannot be positively matched, It is of tremendous help, therefore, that the scrambling order is repeated over and over, A doubtful match can be checked in another section, and matches which are impossible to spot in one section can be readily spotted in another.

and the second se

Rather than cut the pattern up as in the illustration, an optical system has been built for viewing two duplicate patterns simultaneously. This is shown in Fig. 8. The two identical patterns are mounted on moveable slides, and viewed through a system of mirrors which superposes the two, but all of the upper pattern to the right of a definite line is blocked out, and all of the lower pattern to the left of this line is blocked out, so that effectively any two elements may be jurtaposed to see whether they look as though they were originally consecutive. If a match is discovered in one section, the viewer may be shifted without moving the slides, for an immediate check in other sections. Instead of dividing the scrambled pattern with lines and numbering them as in Fig. 6, suitable scales and numbers for a particular TDS system can be incorporated in the slides.

Figure 7 shows TDS patterns for a system using elements only 30 milliseconds long. Here it is distinctly noticeable that the dark areas in the patterns carry over from one element into the next to a degree which somewhat interferes with visual matching. This is caused by the exceedingly narrow scanning filter. The lower part of the picture shows the same section of speech scanned with a filter twice as wide. Here it is apparent that the time resolution is much sharper, but some of the frequency resolution is lost. It is not known at present which filter will prove the more useful for the analysis of patterns from TDS systems. Both are available in the present machine.

Speech patterns have now been shown to be useful in decoding all systems of speech privacy known to be in use. This method, however, which is quite general, may not necessarily be the speediest in all cases. and the second se

4. Special Methods for TDS

The TDS system appears to be the most difficult to decode of all the speech privacy systems known to have been reduced to practice, particularly if a large number of codes are available and if they are changed often. A great deal of emphasis naturally has been placed on TDS in this investigation. The following sections discuss methods particularly applicable to TDS, investigated in parallel with the speech pattern development,

4.1 Wave Form Traces

ander in der Sternen der Besternen der Stationen und sinder einen der Stationen der Stationen der Stationen und Andere Besternen der Stationen der Stationen und seinen der Stationen der Stationen der Stationen besternen und

Speech patterns of the type thus far discussed are particularly designed to display the frequency composition of speech, so that distortion of the frequency scale could be recognized visually. Where only the time characteristics have been scrambled, the wave form itself provides evidence which can be visually interpreted. Various methods have been tried, the first being the ordinary oscillograph. Figure 9 shows traces of TDS speech, divided into three frequency regions. It is quite apparent that there are discontinuities in time more sudden and frequent than occur in normal speech. It is possible to cut up such traces and piece them together, as has been done in Figure 10.

It was thought that a variable area sound track would provide more distinctive patterns than oscillographic traces, and would have the additional virtue that they could be played back, and could, therefore, serve perhaps as the primary record of the intercepted message. This appears to be true, as is illustrated in Fig. 11 and 12, showing variable area patterns of TDS speech, scrambled and reassenbled. The silhouettes have more distinctive character than the oscillographic traces, and similarities can be more easily spotted and checked. In these illustrations, two frequency bands are represented, the upper band having been modulated down to the same region as the lower band, to be more easily visible.

In Figs. 9 to 12, the TDS elements were numbered in their scrambled order, so that the reassembled order gives the code. In both these illustrations, the elements were 30 milliseconds long, twenty elements to the code cycle. (The pictures show only half the code cycle for space reasons.) They were numbered, 1, 1', 2, 2' --- 11, 11', 12, 12', etc. Since the code cycle is constantly repeated, any match found in one cycle must also occur in the other cycles. The cut up traces therefore were mounted on vertical strips of Scotch Tape before matching, 1, 11, 21, 51, 41, on one strip, 2, 12, 22, 32, 42, on another, and so on. This facilitated checking matches in 5 sections at once. Notice, for instance, that 31 and 32' appear to match in Fig. 12 and this is immediately corroborated by 41 and 42', the other sections being inconclusive.

4.2 Partial Matching

يە كەرۋە ۋە تەرىپىدىكە بىرىغانىيە بىلىغانىيە بىلىغانىيە بىلىغان بىلىغان قىلىغانىيە بىلىغان بىلىغان بىلىغان بىلى ئىلىدىكالاتىكى مەت بەلىكاكە ئەت بىلىغانىيە بىلىغان بىلغان بىلغان بىلىغان ئىلىغان بىلىغان بىلىغان بىلىغان بىلىغان

¢

The above systems would not serve if the TDS code were changed very often, in the extreme case if it were changed every cycle. One branch of the investigation has, therefore, attacked TDS from a statistical angle. In a system with a sufficient number of elements the total number of available codes is very large. If, however, in a given code cycle a few elements can be visually matched, the others being inconclusive, it appears possible to tabulate in advance all the codes which will satisfy the observed matches, perhaps on IBM punched cards, thereby enormously reducing the number of codes remaining pos-sible. The most complex TDS system under consideration has twenty elements per code cycle with over 60,000 good codes available. This may be reduced to only 8 possible codes by matching two groups of three elements. These eight codes might conceivably be tested successively by automatic means, the correct one being recognized by ear. Presumably, the message could thus be decoded cycle by cycle. A cycle containing insufficient material for visual matching may possibly contain no indispensable portion of the message either.

5. Further Possibilities

Assuming that the methods outlined in this report apply to all privacy systems which it is desired to crack, further work would be directed toward speeding up the processes. Improvements in speed can, it appears, be made in all of the processes outlined previously. These improvements may be summarized as follows.

5.1 Instantaneous Speech Patterns

As described in Part II of this report, the selected sample of speech already is scanned at more than twice its normal speed, the filters, etc. being designed for this purpose, It appears quite feasible, by pushing this process up into television frequencies, to obtain speech patterns of the same type on the face of a cathode ray tube, for instance, representing either a "still" or a "moving" picture of say 1 second of speech. In the latter case the picture would be running off one edge of the screen and onto the other continucusly. Desirable sections could be stopped at any time. This appears, however, to require considerable equipment as well as considerable development, and would be undertaken only if it appeared quite certain that speech patterns afforded the best means of keeping up with a rapidly changing code,

5.2 Large Variable Area Patterns

The variable area patterns discussed in Section 4 were produced by a process not requiring photographic film, but they had to be photographically enlarged for easy inspection and handling, which is a slow process at best. It does not appear impractical, particularly if it is not necessary to play the record back, and if the high frequencies are going to be modulated down, to develop a simple recording system to produce patterns of the variable area type big enough to see and handle without enlargement, thus providing instantaneous patterns. For cases where the code is repeated, means may be provided by a synchronously revolving once per code cylinder, with a corresponding lateral movement, to obtain a spiral record on which the similarly located elements of each code cycle would be vertically disposed in a manner similar . to that described in Section 4.1, whereby several matches may be seen simultaneously.

The state of the s

5.3 Decoding by Automatic Trial

group and survey and a start a start structure of a start start and and a start and a start and a start again a Maintai air Maintai Aanaadhaa anaadhaa aa daaradhaa aa daaraadha daha aha aha aha aha ahaadhaadha ala ar dhaadha

It appears quite feasible to combine a modified TDS receiving machine with a crossbar switch system, actuated by punched cards, perhaps, so as to try successive codes until one unscrambles the speech. This is particularly applicable to cases where the code is changed often, but where the number of possibilities can be greatly reduced by visual means. It is also, of course, applicable to cases where the total number of available codes is small.

5.4 Decoding Equipment

Equipment might be assembled for actually decoding scrambled speech. For instance, a system of adjustable filters and carriers might be built to take care of all split band systems. This includes shifting and inverting frequency bands, introducing different delay into various bands, removing bands of noise, wobbling the carrier, and whatever other frequency distortion may be included. A TDS decoding system with adjustable elements and codes also deserves consideration.

It appears desirable that all the proposals for privacy methods which appear in the literature should be reviewed, and that any which look feasible should be examined as if for actual development, thus perhaps suggesting new decoding problems and new techniques to meet them.

6. Recommendations for Increasing Privacy

The new information obtained during the present investigation concerning speech characteristics which prove helpful in decoding existing privacy systems naturally has suggested methods of making decoding more difficult. The following methods, for instance, are based on principles expounded in this report, and they do not depend on secrecy for their effectiveness.

6.1 General

an and the second s

a. Use a low-pitched voice. This makes it difficult to get good speech patterns. A filter narrow enough to resolve the harmonics is too narrow to give good results in time. and the second of the second o

- b. Don't inflect the voice. An absolute monotone would avoid the changing slopes referred to in earlier sections. Unfortunately it is difficult to achieve, as can be seen by referring back to Fig. 2 and 3 which were intended to be uninflected.
- c. Add noise after scrambling the speech. The object here is to cause the maximum disturbance to the <u>visual</u> speech patterns. The ear can concentrate on speech and disregard noise. The eye has not learned to do that. Noise of the right kind might make TDS patterns look more continuous in their scrambled order than in the order which unscrambles the speech but scrambles the noise.

نې تې<u>يت</u>

6.2 For TDS

- a. Change the code often; repetition is the most favorable single factor for determining the code.
- b. Make the elements, or the code cycle, or both, vary in length. This makes it difficult to get a multiplicity of comparable elements favorably disposed for matching.

6.3 Compounding

Indiscriminate piling of one privacy method on another is not recommended. It is notable, however, that split band systems are decoded by their time characteristics such as discontinuities or slopes in the harmonic traces. TDS systems are decoded by means of the frequency distribution of energy, particularly by visually matching the harmonic traces in frequency. If TDS speech, for instance, were subjected to some kind of frequency multiplication (not differing greatly from unity) which changed from one element to the next in some not too regular manner, visual matching would be very seriously impaired. Other combinations may suggest themselves whereby both the frequency and time patterns were operated on in such a way that neither operation provided clues for the other.

7. Other Speech Pattern Methods

and the straight of the straight os

Some methods of producing speech patterns were tried or considered, which appear to be of less aid in privacy cracking than the methods outlined in this report. Some of these speech pattern methods, however, may find other applications.

First there is a scheme using a multiplicity of frequency channels, each continuously registering its energy content, either on paper or on a cathode ray tube. This system has the advantage of being instantaneous but there appears to be great difficulty in having a sufficient number of channels recorded close enough together to give good resolution in the frequency scale. A sufficient number of channels suitably recorded might make it useful for TDS, but hardly for any system whose frequency distribution has been distorted.

In another system which was tried, the band-pass scanning filter was moved (effectively) back and forth across the frequency range at a rate (10 to 30 times per second) intended to blend into a continuous visual pattern. This also gave instantaneous patterns, and could be registered either on paper or on a tube. The resulting patterns, however, showed too much discontinuity in the time scale for the present purposes.

3. Records of Scrambled Speech

يەركىم ئەركىمىڭ ئەركى ئەلكىمىكە ئەكەركىمىڭ ئەركىمىڭ ئ

La the second second

Early in this project it was felt that decoding might depend on recognizing certain physical characteristics of speech (other than the harmonic traces which have proved so useful) such as the length of syllables, the general distribution of energy density, and the like, all of which would naturally be expected to differ for different languages. Records were, therefore, made of speech before and after being scrambled by the systems using inversion, band splitting, and TDS. Four foreign languages were included: German, Italian, Japanese, French, and English. Six different codes are represented in the TDS and in the split band privacy systems. The speech samples represented in these records were obtained from commercial phonograph records (Linguaphone) designed to teach the different languages. Table I lists the Linguaphone Records, and Table II lists the records designed to illustrate scrambled speech.

TABLE I

LINGUAPHONE RECORDS

	Record				Playir	ig Time
Language	No.	Topic	<u>Voices</u>	Band	Mins.	Secs.
Japanese " * "	2E 1E 1E	Paying a visit Syllables Dialogue	Male "	Entire Outside Inside	3 1 1	10 45 45
*French " "	7 7 8 8	Dialogue " " "	Male " Male & Female	Outside Inside Outside Inside	1 1 1 1	55 5 50 45
Italian * " "	17 17 18 18	Dialogue " "	Male " "	Outside Inside Outside Inside	1 1 1 1	45 55 40 40
*German " "	11 11 12 12	Dialogue " "	Male " Male & Female	Outside Inside Outside Inside	2 1 2 1	10 0 20

La desta state and a state of the

* Selections chosen to be recorded through various privacy systems.

TABLE II

B.T.L. RECORDS TO ILLUSTRATE SCRAMBLED SPEECH

Band Splitting Privacy System

B.T.L. Record Number	Language
5602	Japanese
5603	French
5604	Italian
5605	German

These records are made up of several sections with different codes and a section in which the code is changed every 20 seconds.

T.D.S. Privacy System

E.T.L. Record Number	Language
6015	Japanese
6016	French
6017	Italian
6018	German

These records are made up of several sections with different codes, some with 60 millisecond elements and some with 30 millisecond elements, also one section with the speech decoded.

Inversion Privacy System

B.T.L. Record Number	**Section Number	Language
5606	2	Japanese .
5606	3	French
5606	4	Italian
5606	5	German

Normal Speech

B.T.L. Record Number	**Section Number	Language
5606	1	Japanese
5607	1	German
5607	2	Italian
5607	3	French

** Counting from outside to inside.

*

12

the week and the second of the second s

9. Laboratory Notebooks

Engin	eer	Notebook Nos.				
A. D.	Fowler	T-3757				
L. Y.	Lacy	T-4690 and T-4815				

10. Photographs

· 1

and the second se

a that a start and the set of the

5

A STATISTICS STATISTICS

Numbers 97410 to 97421 inclusive, constituting Figures 1 to 12, respectively.

1

The state of the state of the

and a start which a start to the start

NATIONAL DEFENSE RESEARCH COMMITTEE

Final Report on Project C 32

SPEECH PRIVACY DECODING

Symbol No. 582

PART II - THE SPEECH PATTERN MACHINE

1. <u>Ceneral</u>

and the second s

The speech pattern machine is equipped to monitor voice frequency currents submitted to it, and to record a sample 1.8 seconds long at any time. It then makes a frequency analysis of this sample, and records the result on dry facsimile paper. The result, known as a speech pattern, portrays frequency along the vertical axis, time along the horizontal axis, and intensity of energy by the density, or blackness, of the pattern.

Apart from mounting the facsimile paper, making certain initial adjustments of the controls and selecting the desired sample of speech, the action of the machine is entirely automatic and requires 2-1/4 minutes for the completion of a pattern.

The present embodiment of the speech pattern machine is a laboratory model based on experimental work carried out at the Bell Telephone Laboratories before the present project was initiated. Although it has been made compact and rugged it does not conform to any special standards for portability or to requirements which might be imposed for Army or Navy use.

The machine comprises three main units:

(1) The recorder unit, shown in the attached photograph (Fig. 13), which serves as a magnetic tape recorder as well as the speech pattern recorder.

- (2) The amplifier-analyzer unit, which is the upper panel in Figs. 14, 15, and 16.
- (3) The power supply unit, which is the lower panel in the above three photographs. A block schematic of the complete system is shown on drawing ES-J96253.

2. Description of Recorder Unit

and a start and

and a strain a

In the main, the recorder unit consists of a modified 12-inch disc recording machine, type 2C S.P., manufactured by the Presto Recording Corporation. In addition to the usual cutting head carriage and lead screw drive, there is a brass cylinder about 2-1/2 inches in diameter, mounted of a shaft parallel to the lead screw and driven through a pair of 1:1 spiral gears from the main vertical shaft. A sheet of Teledeltos facsimile paper is secured to the cylinder by means of a pair of rolling springs encircling the cylinder. The recording stylus, consisting of a stainless steel wire about 10 mils in diameter, is mounted on an insulating block affixed to the cutting head carriage. The latter can be raised or lowered by hand, and in the lowered position the pressure of the stylus on the facsimile paper is about 40 grams.

by means of a synchronous motor and rim drive mechanism, providing both 33-1/3 and 78 rpm speeds, the turntable, cylinder and lead screw all rotate, and the stylus moves laterally across the paper surface of the cylinder at the rate of 96 lines per inch. The marking or recording on the Teledeltos paper is effected by varying the electric current flow from the stylus through the facsimile paper into the cylinder, the stronger the current the darker the mark made on the paper. In addition to the above, the recorder has a magnetic tape mounted on the rim of the turntable. On this tape may be recorded a 1.8 second sample of the signal to be analyzed. Exact synchronism between the cylinder and magnetic tape is secured by means of the spiral gear drive mentioned above.

Three electro-magnets, forming part of the magnetic tape recording system, provide for (a) erasing previously recorded material, (b) biasing and recording new material, (c) playing back whatever is recorded. Continuous erasing and recording are obtained as the speech currents are monitored, and by opening the circuits to the recording and erasing coils, which is done by releasing a key, the last 1.8-second interval of material is captured and played back over and over, once for each revolution of the turntable.

3. Description of Method of Making Speech Patterns

The purpose of the following is to trace the action of the speech pattern machine from the point where the speech currents to be analyzed enter the input of the machine to the final recording of the speech pattern itself. The description will be given with reference to the block schematic diagram, drawing 2S-396253, and also to the circuit schematic, drawing 2S-396254, both attached.

3.1 Capturing the Speech Sample

The source of speech currents should be connected to the input jack of the machine. A non-locking key (which operates all the switches shown in the block schematic) should be thrown to position 1. In addition to connecting the recording and reproducing amplifier to the recording coil of the magnetic tape recorder, this switch also turns on the 20 kc erasing and biasing oscillator. Under this condition, the incoming speech currents are being continuously recorded and subsequently (1.8 seconds later) erased. A loud speaker mounted on the front of the amplifier-analyzer panel, permits monitoring the input, and the level is adjusted to approximately zero on the V.U. meter.

The recording and reproducing amplifier incorporates sloping networks on switches so that the higher frequencies of the speech currents recorded on the magnetic tape may be emphasized if desired.

Upon hearing a suitable sample of speech, the nonlocking key is released. This returns it to position 2, thereby turning off the biasing and erasing oscillator and connecting the input of the amplifier to the play-back coil. By the release of the nonlocking key, the 1.8-second interval of speech just previously heard is captured as a recording on the magnetic tape. When making the recording the speed of the recorder unit is set at 33-1/3 rpm.

3.2 Placement of the Teledeltos Paper

The release of the nonlocking key, as discussed above, also provides for the proper setting of an index, or pointer, associated with the brass cylinder on the recorder unit. This index enables the operator to place the Teledeltos paper on the drum in such a way that the beginning of the captured speech sample and the beginning of the paper will be concurrent. The Teledeltos paper may now be secured to the drum by means of the springs. Where the ends of the paper come together around the drum, there should be provided a slight and trailing overlap to prevent the stylus from tearing the paper.

3.3 Playing Back the Magnetic Tape Recording

The knob controlling the oscillator frequency should be turned to the right against an internal stop, and held there, The turntable speed should be set for 78 rpm, and the level of the reproduced signal should be set to a few db below zero in the VU meter, depending on how dark a pattern is desired. The stylus should be lowered onto the paper, at the same time releasing the frequency control. The stops at both ends of the frequency control are contacts which short circuit the marking current, so that the patterns are automatically fixed in width.

The original band of voice frequencies ranging from about 200 cps to 3000 cps is changed due to the increased speed by a factor of 2.34 to about 470 cps to 7000 cps. This band of frequencies is then amplified by the recording and reproducing amplifier to a suitable level and transmitted into the analyzer circuit. The frequency response of the magnetic tape plus the recording and reproducing amplifiers is shown in the lower portion of ES-396258.

3.4 Frequency Analysis

The analyzer circuit comprises, in the main, a double balanced modulator, a carrier oscillator whose frequency is continuously varied by means of a synchronous motor drive on the frequency control condenser, and a fixed narrow band-pass filter.

The double balanced modulator provides that neither the carrier nor the original input signal are present in the modulator output, only the upper and lower sidebands being present. These sidebands, which have an energy-frequency distribution (with respect to the carrier frequency) identical with the input signal to the modulator, occupy a position in the frequency scale depending on the carrier frequency. A change in the carrier frequency, say, lowering it 200 cycles, will cause the two sidebands to shift to a position in the frequency scale 200 cycles lower.

The narrow band-pass filter has a mid-band frequency such that when the carrier has one extreme value, only the lowest frequency components of the lower sideband fall within the pass band of the filter; when the carrier has its other extreme value, only the highest frequency components of the same sideband are passed. When the carrier frequency is slowly changed from one extreme to the other, the filter will select the high frequencies, say, and progressively select lower frequencies until the whole sideband has been scanned. The output of the filter will be substantially constant in frequency but will vary in amplitude with the amount of speech energy falling lane

in the selected band of frequencies passed by the filter. A switch makes it possible to change the effective band width of the filter from 45 cps to 90 cps.

The circuit and response of the filter is shown on the attached E3-396257. The band width is changed by means of a two-circuit, three-position switch which serves to select the proper values of mutual inductance to give the desired characteristics. A balanced 600-ohm input winding is provided on the core of one of the filter inductance elements for connection to the copper oxide modulator. A center tap on this winding provides a path for the carrier frequency introduction, thus eliminating the necessity for a balanced center tapped repeating coil between the filter and modulator. There is an impedance transformation in the filter so that the output works into the grid of the following amplifier directly.

3.5 Recording the Speech Pattern

The output of the band-pass filter is transmitted to a compressor and marking amplifier. The level variations of the output of the filter, of the order of 35 db, are compressed to about 12 db. The input-output characteristic of the compressor is shown at the top of ES-396258. This degree of compression is necessary because of the limited range afforded by the Teledeltos paper. The marking amplifier which follows the compressor provides for sufficient output power to cause very dense, or black, marking for the maximum levels.

The output of the marking amplifier is connected directly to the stylus and the brass cylinder, the latter connection being made through a slip ring and brush.

It will be noted that the power transmitted to the stylus and drum is substantially S kc in frequency. This has been found to work satisfactorily, since the action of marking the paper is purely thermal, depending on the current flow from the stylus through the paper to the drum to generate heat localized at the point of contact of the stylus with the paper. The impedance of the paper varies over wide limits depending on the current flow, another factor necessarily taken into consideration when designing the compressor and marking amplifier.

4. Physical Description of Units

a a stand a sta A stand a stand

and a state of the second s

The recorder unit is approximately 18" x 18" x 19" high and weighs approximately 30 pounds. It is equipped with an attachment plug and cord for connections to 105-125-volt, 60-cycle power mains. The power consumption of the synchronous motor is 60 watts or 250 volt-amperes. The type of paper used for the word patterns is known as "Teledeltos Grade H" facsimile paper developed by the Western Union Telegraph Company. A sheet 4-3/4" x 8-1/4" is required for each record.

٦

The emplifier-analyzer unit has an input impedance of 600 ohms and requires a level of voice frequency currents in the range from -40 vu to 0 vu. The usable range of frequencies of the voice currents lies between 200 cycles and 5000 cycles. The electrical circuit is shown in ES-396254. The unit is mounted on a standard 19" pench 14" high and 10" deep. It weighs approximately 40 pounds.

The rower supply unit furnishes a regulated supply of voltage for the plates and screens of the amplifieranalyzer tubes It also furnishes the necessary power for the heaters of those tubes. The electrical circuit is shown in ES-391255. An attachment plug and cord is furnished for connections to 105-125-volt, 60-cycle mains. The power consumption is 170 watts or 215 volt-amperes. The unit is mounted on a standard 19" panel 7" high, 10" deep and weighs approximately 40 pounds.

The parts required for the amplifier-analyzer unit and the power supply unit are listed on drawing ES-396256.

5. Photographs

No.	97422	(Fig.	13)
No.	97423	(Fig.	14)
No.	97424	(Fig.	15)
No.	97425	(Fig.	16)

6. Drawings

ES-396253 to ES-396258 inclusive.

- 6 -

UNDISTORTED SPEECH PATTERNS.

FIG-1



÷.





, m,

· • • •

ŝ

•

¢



ł

9.2411

FIG 2

i F



OI aur te

: ...

. .

1

YAW The aw-

97412

FIG 3

÷

OUTPUT OF C. FRIVACY SYSTEM



INVERTED

. UNINVERTED

, š.



OUTPUT OF SPLIT BAND PRIVACY SYSTEM.



NUMBERS INDICATE ORIGINAL ORDER. L INDICATES INVERTED BAND.

š.

97414

FIG 5



1,3 - Scrambled. 2,4- Rearranged in original order. 1 Marks synchronizing pulse.

......

1

÷

97415

į



PATTERNS OF T.D.S. SPEECH.

1

.

.ia _____

1.11

1

97416

1G 7

'. i

:

.

FIG 9

97417

····

SCRAMBLED TDS OSCILLOGRAPHIC PATTERNS TOP TRACE: ENTIRE BAND MIDDLE TRACE: ABOVE 600~ BOTTOM TRACE: BELOW 600~

, b 15. 25, 35 45 35 β THE PARTY OF 13 25 45 545 44 3.4 4 ,41 42 34 24 27 4 4 13' 23, 33' 43' e. 13 23 43 33 ε 12' 25 32' 42' N 42 32 12 22 N 31 . 1 21 41 **HARRENARD MERE** 31 41 1 12

ŝ

đ



! _

ř

in freedown

FIG 10

974 18

		l	i.	ľ						1	<u>.</u> -	
	Э'		13'		23'			33'			43'	-
	/				21			3/			15	
	5'		15'		25						C4	***** **
	E		13		C 2					A a	24	FRNS
			.//		alan 27		37			41		BLED TDS PHIC PATTE
			15	2.5			35			01211211211211211212		UNSCRAME
ł			14'	24,			34'			44,		ö '
2				22			32			42		
, z			12,	22,			32'			42'		
4			-74 1000000000000000000000000000000000000	24			34			44		
	1		1		1	1			1			

1

÷

τ

¢,

S. Tr Jara

FIGII

97419

2 2 2

A CARLEN AND A CARLEN

SCRAMBLED TDS VARIABLE AREA PATTERNS UPPER TRACE : ABOVE 1500 ^w LOWER TRACE : BELOW 1950 ^w

15'		25'		35'	and the second second	45'	
15		25		35	and a subscription of the	43	
.41		24,		34'		44'	
14		24		34		44	
13'	and the second se	23'	an in the second se	e e S		43'	
13		53		33	the second s	43	
12'	and the second second	22'		32.		42'	
12		22		32		42	
		21'		31'		41'	
11		12		: 3/		. +/	

ŝ N 2

Ę

- 1 -

ماغ فرا الماسين المالة المالية المالية

mather a stand and the stand of the set of the stand of the second s

N.

2 · · ·

المتعكة لأشكاء فالخدمات

Ī

FIG 12 97420

UPPER TRACE: ABOVE 1500 ℃ LOWER TRACE: BELOW 1950~ VARIABLE AREA PATTERNS UNSCRAMBLED TDS

N 1 13' 12 15' 14 1 15 Ť 19.61444 4 13

'n,

N

6

ŝ

1

*

TT THE PARTY

134. 201

Level 1 - Le martine

Frank





- į

:

161 - 1

and the second of the second of the

A CONTRACT OF A SHARE A CONTRACT OF A CONTRACT OF

. •



٢

そうちょうちょう 人間をうましいた いって

1 + 1 + 1 × 1

in the second

-1

And the state of the second second

FIG 14

ა

1.1

Line street



1

initiation of

the state of the state of the state of the

The second se



1.1

A Change Bar Carles Later

ĩ ч ч л

*

7

· ·

2.447.5

2

1

ية. 1

> . - i

(--)

FIG-le

1

いいしょうたいしいとうというと

. .

-1

A REPORT AND A STATE AND A STATE AND A

-

. **~**,

141.0

115.12.2.4

111

Ť **5**.

Law D' Law LE MARTIN

-1

1-28-42)- 296250
Issue			ES
PARTS LIST FOR ES-396255	R54 - 15,0000 RC 48 10 ATT R55 - 10,0000 RC 81 1 ATT R57 - 10,0000 RC 81 1 ATT R59 - 500 RC 81 1 ATT R59 - 500 RC 81 1 ATT R50 - 500 RC 81 1 ATT R61 - 500 RC 81 1 ATT R62 - 500 RC 81 1 ATT R63 - 500 RC 81 1 ATT R63 - 500 RC 81 1 ATT R64 - 500 RC 81 1 ATT R65 - 100 MC 81 1 ATT R65 - 100 RC 81 1 ATT R65 - 10000 RC 81 1 ATT	PART - LIST FOR ACAD FATTERN MADHI	A Devision of the second secon
	 K. TYEE D-157873 VARISTCR SPUT GENERUEL TYE E 453 SPST HAND H ARROW TGGGLE SHITCH SPOT GENERALAB TYE 1453 SPOT GENERALAB TYE 1453 HE TYE 1295-A JACK HE TYE 1205-A TLUG HE HEROL TYE 605-D-1 CHASSIS UNIT HERUL TYE 605-D-4 FLUG HERUL TYE 605-D-4 FLUG KPHERUL TYE 605-D-54 FLUG KPHERUL TYE 605-D-54 FLUG KPHERUL TYE 605-D-54 FLUG KPHERUL TYE 605-D-54 FLUG KPHERUL TYE 70 TUSHTAULE TYE 20-SF. 		
	∽∞≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈		
PARTS LIST FOR ES-396254	 M. E. DWERN "TEET" ALTEGRA. TYPE T322-66 M. M. FOREN TIEET ALTEGRA. TYPE T322-66 M. M. TIEET ALTEGRA. THE TABLE CR-000-45 TS. WAY WE TYPE 400-45 THEO VERTILL DUBILIER OTFP-15 S. S. S. NED CORRILL DUBILIER OTFP-25 S. S. S		
	YE TYFE (07-4 WE TYFE (07-4 WE TYFE (07-4 M 33-120 Y0LT LWP ING BT 1 WATT ING BT 2 WATT ING BT 2 WATT ING BT 1 WAT		
	RI RS RS RS RS RS RS RS RS RS RS	•	

-

ŀ

×

14.1

- -----

سعير مر

٩.,

LI MALLAL

T

RINTED IN U. S.

La Martin Di ta Sala

AS I