PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO Y SIMULACIÓN DE UN SCRAMBLER DIGITAL DE VOZ

Tesis para optar el Título de Ingeniero Electrónico, que presenta el Bachiller:

ROBERTO ISAAC MONTOYA LIMÓN

ASESOR: PAUL ANTONIO RODRIGUEZ VALDERRAMA

Lima – Septiembre del 2012

RESUMEN

Un primer acercamiento a la definición de comunicación puede realizarse desde su etimología. La palabra deriva del latín *communicare*, que significa "*compartir algo, poner en común*". Por lo tanto, la comunicación es el proceso mediante el cual el emisor y el receptor establecen una conexión en un momento y espacio determinados para compartir ideas, transmitir e intercambiar información o significados que son comprensibles para ambos.

Desde un punto de vista técnico se entiende por comunicación al hecho que un determinado mensaje originado por el emisor llegue a un receptor, distante en el espacio o en el tiempo. La comunicación implica transmitir y recepcionar una determinada información que en la actualidad se encuentra muy vulnerable e insegura debido a las interceptaciones, la existencia de intereses personales, empresariales o de terceros. Este problema ha motivado la presente tesis a diseñar una alternativa de solución mediante el cual se mejora la confidencialidad de las comunicaciones que en su mayoría de casos se requiere.

En tal sentido, la presente tesis tiene como objetivo presentar un Diseño y Simulación de un Scrambler Digital de Voz, el cual permitirá codificar la señal de voz a fin de transmitirla por el canal.

La transmisión permitirá la comunicación exclusiva entre el emisor y receptor. Sólo el receptor podrá decodificar el mensaje y a su vez recibirá del emisor una contraseña que será establecida aleatoriamente en cada transmisión. Para la recepción, se decodificará la señal de voz con la contraseña recibida aleatoriamente garantizando de esta manera una comunicación segura.

ÍNDICE GENERAL

CAPÍTULO I

PROBLEMÁTICA DE LA SEGURIDAD EN LAS COMUNICACIONES

1.1 Aspectos Generales

Las telecomunicaciones surgieron a partir de una serie de experimentos en telegrafía por Samuel Morse en 1837 usando la *inducción electromagnética* logrando transmitir información en forma de puntos, guiones y espacios por medio de un cable metálico. Después en el año 1876, Alexander Graham Bell y Thomas A. Watson transmitieron exitosamente una comunicación humana a través de un sistema telefónico funcional usando cables metálicos como medio de transmisión [1].

A raíz de tales experimentos se concibió la idea de lo importante que es la comunicación con el transcurrir del tiempo y el avance de la tecnología, se creó lo que hoy en día se llama teléfono, el cual fue mejorándose y modificándose para satisfacer las necesidades de la comunicación humana con un aparato mucho más simple y compacto, convirtiéndose en un elemento tan común de nuestras vidas y que lo aceptamos como algo muy natural.

La invención del teléfono y otros equipos de telecomunicaciones permitieron la comunicación a grandes distancias, lo cual amplió el concepto de comunicación, definiéndose como el proceso por el cual la información se transfiere de un punto llamado fuente, en espacio y tiempo, a otro punto que es el destino o usuario, permitiendo la interacción y desarrollo de las personas en uno o entre varios grupos sociales.

1.2 Alcance y Objetivos

El objetivo principal de la presente tesis es diseñar y simular un Scrambler digital de voz para lograr una comunicación segura en la que sólo el receptor pueda decodificar el mensaje recibido a través del hilo telefónico.

La presente tesis no tiene por objetivo implementar un sistema en tiempo real, sino comprobar lo factible que es la seguridad en la comunicación para la presente tesis. Además se tiene como objetivos específicos: Disminuir en cierta forma la vulnerabilidad que tienen los actuales sistemas de comunicación de voz, analizarlos y observarlos a fin de superar sus deficiencias.

La aplicación del sistema a diseñar se realizará en una simulación usando la plataforma MATLAB. Para lo cual se desarrollará las técnicas de codificación y decodificación a fin de obtener un mejor análisis de su comportamiento ante diferentes circunstancias y sobre todo evitar cualquier tipo de interceptación.

1.3 Problemática

Con el avance de la tecnología en las comunicaciones la transmisión de información se ha tornado insegura y vulnerable, por lo que ha surgido la necesidad de incrementar la seguridad y velar por su integridad. Con este propósito se emplean técnicas que permiten que la voz llegue a su destino sin ninguna distorsión tal como fue emitida. Estas técnicas consisten en codificar y decodificar la voz para su transmisión y recepción a través de un canal sobre el cual no se tiene control alguno.

Debido a las características no seguras del canal de transmisión, es de alto riesgo realizar una comunicación de emisor a receptor sin ninguna clase de codificación. Si se realizarán las comunicaciones hoy en día sin codificación alguna, cualquier persona podría manipular y tener acceso a la comunicación demostrando con ello que es un sistema vulnerable.

Teniendo en cuenta la baja seguridad del canal de comunicación se han diseñado métodos de seguridad para codificar las comunicaciones de voz. Sin embargo codificar las comunicaciones no es una solución completa al problema, pero si ayuda a mantener su integridad durante la transmisión.

Además de garantizar la integridad de la comunicación, existen otros problemas como: la atenuación y la distorsión de la señal a través del canal. Estos problemas se producen debido a la existencia del ruido y pérdida de potencia de la señal. Estos problemas son importantes a tomar en cuenta al realizar cualquier diseño de un sistema de seguridad de voz.

A raíz de la existencia de los problemas de seguridad, atenuación y distorsión existentes en todo canal, es necesario que todo sistema de seguridad de voz sea robusto. Pero la solución de estos factores, que afectan directamente a la comunicación, no resuelve el problema de las comunicaciones de voz.

Además indirectamente existen otros factores que afectan a los sistemas de comunicación de voz como: los altos costos de los equipos, el avance de la tecnología, el uso ilegal de este medio de comunicación, el requerimiento de una elevada seguridad para las autoridades y su prohibida comercialización en el mercado negro.

El problema principal que se presenta en cualquier comunicación, es la presencia de terceros que quieren interceptar la comunicación para manipularla y usarla en beneficio propio o de su organización. Llámese a estas personas: espías, infiltrados políticos, infiltrados organizacionales, delincuentes, terroristas, narcotraficantes, etc. (ver Anexo 1)

Dada la necesidad de manejar confidencialmente la información es necesario contar con equipos de última generación para contrarrestar la inseguridad que se genera con el avance de la tecnología. Por ejemplo, de no tomar en cuenta este factor en una organización, su seguridad puede ser fácilmente vulnerada por equipos actuales más sofisticados en hardware,

procesamiento y en encriptación que los que se fabricaron años atrás convirtiéndolos en equipos en obsoletos.

Otro factor existente son los altos costos de estos equipos *[ver Anexo 2]*. Debido a la necesidad de tener y mantener la seguridad de las comunicaciones por voz solo pueden ser adquiridas por personas de altos recursos económicos ó grandes organizaciones que consideran la seguridad un problema muy importante.

Como resultado del análisis de los problemas de la comunicación por voz, se aprecia lo vulnerable que es este tipo de comunicaciones, lo que ha motivado que sean amparadas por leyes peruanas, de manera que solo con una orden judicial se puede interceptar las comunicaciones.

Finalmente, tener un alto grado seguridad con equipos de última generación que hacen uso de un *Scrambler Digital* resulta muy beneficioso a las personas u organizaciones que desean un cierto grado de seguridad en sus comunicaciones de voz. Este tipo de seguridad no es extremadamente segura debido a su vulnerabilidad producida por el avance de la tecnología y al no uso de complejos algoritmos de encriptación.

La necesidad de tener un cierto grado de seguridad en las comunicaciones se debe a la existencia de personas u organizaciones que se aprovechan del avance de la tecnología y vulnerabilidad de estos equipos para obtener un beneficio propio o con fines delictivos.

CAPÍTULO II

TÉCNICAS EMPLEADAS EN LA COMUNICACIÓN DE VOZ

2.1 Estado del Arte

Con el avance de la tecnología y la invención de equipos cada vez más sofisticados surge la necesidad de asegurar su integridad, autenticidad de los usuarios y confidencialidad para lograr una comunicación segura por un canal de voz.

Diseñar un sistema de comunicación motiva a tomar en consecuencia varios criterios teóricos para llevarlos a la práctica a una determinada aplicación. En tal sentido las tecnologías empleadas para la codificación de voz hacen uso de los siguientes conceptos que se explican a continuación con más detalle.

2.1.1 Transformada de Fourier y Transformada Inversa de Fourier.
2.1.2 *Scrambler.*
2.1.3 Elección de la clave.
2.1.4 Técnicas de codificación empleadas por Scrambler.

El teorema de Nyquist es más conocido como el *Teorema de Muestreo* por ser un criterio muy inherente en la teoría de la comunicación y se define de la siguiente manera. [2]

El teorema establece que una señal de banda limitada a *B* Hz definida en un intervalo mostrado en la expresión 2-1 se puede reconstruirse a partir de sus muestras tomadas uniformemente a una razón no menor de *2B* muestras por segundo.

$$f_o - B/2 < |f| < f_o + B/2 \qquad (2\text{-}1)$$

Cuando existe la necesidad de reconstrucción de una señal automáticamente se le asocia a la idea del valor de Nyquist. Este concepto permite encontrar el valor de muestreo que nos dará una reconstrucción perfecta de la señal. Si se muestrea con un valor por debajo del valor de Nyquist surgirán problemas para hacer la reconstrucción. A este problema se le conoce como ***Aliasing*** (algunos autores lo llaman solapamiento). El efecto Aliasing ocurre cuando hay un traslapo en el desplazamiento, copias periódicas de la señal en frecuencia.

En el dominio de la frecuencia, se observa que parte de la señal se trasladara con la señal siguiente a él. En este solapamiento los valores de la frecuencia serán sumados juntos y la forma del espectro de la señal será indeseablemente alterada como se puede apreciar en la figura 2.1.

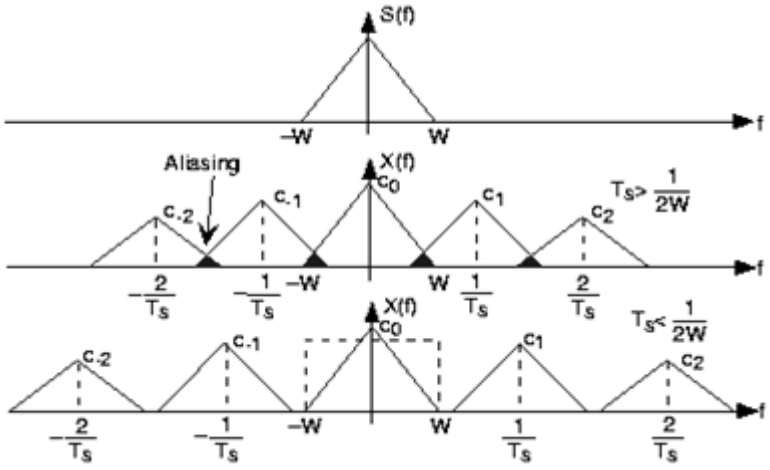

Figura 2.1 Efecto Aliasing [3]

La figura 2.1 se divide en tres gráficas una debajo de la otra. La primera gráfica muestra una señal limitada en banda a (*W* Hz). En la segunda gráfica se ilustra un muestreo en la cual ocurre una superposición de la señal llamada *Aliasing*. En la tercera gráfica se muestrea la señal cumpliendo con el teorema de Nyquist evitando el Aliasing.

Nótese que si la señal no fuera limitada en banda, el componente del espectro siempre sería traslapado.

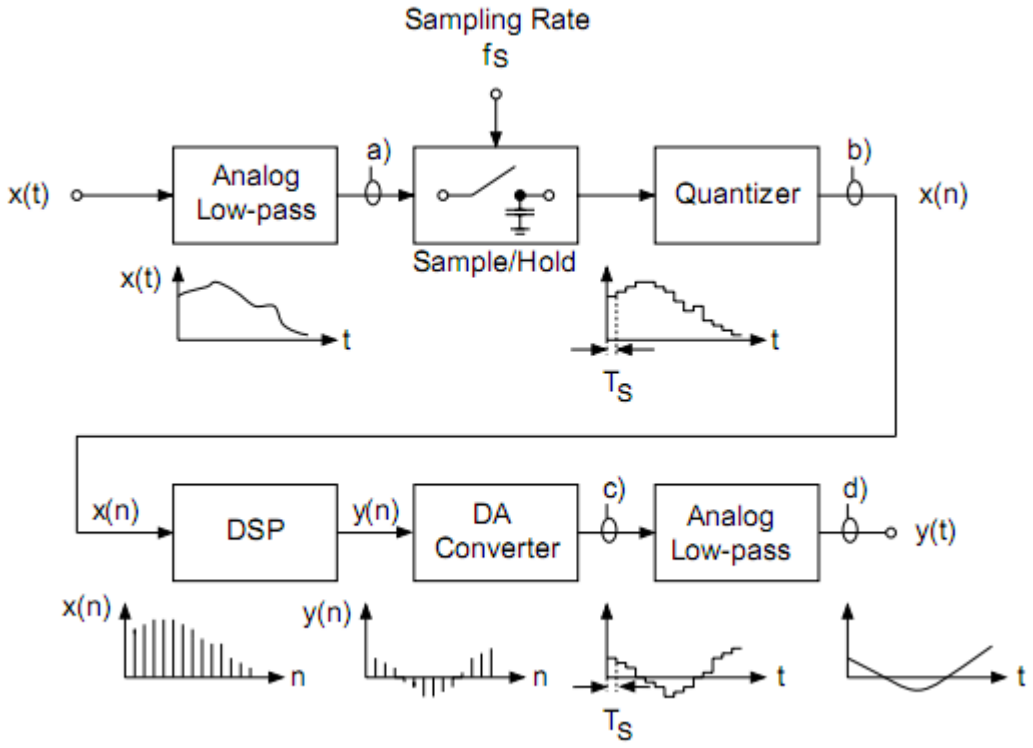

Figura 2.2 Diagrama Esquemático del muestreo Nyquist [4]

En la figura 2.2 se muestra como se realiza el muestreo de Nyquist aplicada a la señal de voz tanto para digitalizarla y volverla a recuperar. Siendo estas secuencias muy importantes para codificar la voz.

En resumen, de las definiciones anteriores cabe resaltar que una señal podrá ser muestreada sin pérdida alguna de información, siempre y cuando su frecuencia de muestreo F_s no supere la cantidad $2F_b$, es decir: $F_s >= 2F_b$. Si no se cumple este criterio aparecerá el fenómeno llamado ***Aliasing.***

2.1.1 Transformada de Fourier y Transformada Inversa de Fourier

La transformada discreta de Fourier (DFT) es uno de dos grandes procedimientos encontrados en el campo del tratamiento digital de señales. El otro procedimiento es el filtrado digital. El DFT nos permite analizar, manipular y sintetizar señales no posibles con procesamiento de señales continuas ó analógicas.

La DFT es un procedimiento matemático para determinar las armónicas ó frecuencias contenidas en una secuencia de señal discreta. Para propósitos

de la presente tesis, una secuencia de señal discreta es un conjunto de valores obtenidos mediante el muestreo periódico de una señal continua en el dominio del tiempo. [5]

La DFT tiene su origen de la transformada continua de Fourier y se define:

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi f t}\, dt \qquad \textbf{(2-2)}$$

Donde x(t) es alguna señal continua en el dominio del tiempo. En el campo del procesamiento de señales continuas la ecuación 2-2 se usa para transformar una expresión de una función continua en el dominio del tiempo a X(f) una función continua en el dominio de la frecuencia. La función X(f) permite conocer el contenido de frecuencias de cualquier señal de interés. [17]

Con la llegada de las computadoras y los esfuerzos anticipados de los primeros procesamientos digitales se motivó a una mayor difusión de la DFT definida como la secuencia discreta en el dominio de la frecuencia donde X(m) es la ecuación DFT de forma exponencial. Ver ecuación 2-3.

$$X(m) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi nm/N} \qquad \textbf{(2-3)}$$

En la ecuación 2-3, x(n) es una secuencia discreta en el domino del tiempo que muestra el valor de la variable continua x(t). El “e” es la base de logaritmo natural y $j = \sqrt{-1}$.

La IDFT es un tema muy importante por su aplicación hoy en día y es conocida como la transformada inversa discreta de Fourier. Inmediatamente se piensa como la transformación de datos en el dominio de la frecuencia a

una representación en el dominio del tiempo. Las expresiones que definen la IDFT son:

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} X(m)e^{j^{2\pi mn}/N} \quad \textbf{(2-4)}$$

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} X(m)[\cos(2\pi mn/N) + j\sin(2\pi mn/N)] \quad \textbf{(2-5)}$$

2.1.2 Scrambler

La voz es una habilidad humana que permite iniciar una comunicación entre dos o más personas cercanas o distantes a través de dos ó varios equipos electrónicos. Pero debido a la existencia de intereses personales o de terceras personas de conocer o manipular esta información que en su mayoría es confidencial se producen las interceptaciones telefónicas.

Debido al interés de terceras personas, se ve la necesidad de codificar la información haciendo uso de sistemas de seguridad, como por ejemplo un Scrambler de voz. Los Scramblers se han usado por varios años y hasta nuestros días se continua mejorándolos y desarrollándolos haciéndolos mucho más sofisticados que antes [6].

En la actualidad existen dos tipos de *Scramblers* agrupados en dos grandes clases. *Scramblers Digitales* y *Scramblers Analógicos.* La diferencia básica entre estos dos tipos de *Scramblers* es la forma de transmitir la comunicación por el canal.[18] Mientras los *Scramblers Analógicos* transmiten la señal codificada por el canal de forma analógica, los Scramblers Digitales lo hacen de forma digital, logrando así una mejor comunicación, más segura e inmune al ruido.[19] Debido a que primero se diseñaron los *Scramblers Analógicos* esta codificación emplea técnicas más antiguas y no muy seguras comparadas con los Scramblers digitales. [20]

2.1.2.1 Scrambler Digital

El Scrambler Digital es un tipo de codificación el cual tiene como salida una señal digital transformada en comparación con la señal original. Esta transformación toma lugar en el dominio del tiempo y/ó frecuencia.

La codificación digital tiene como potencial ser más segura que la codificación analógica, y más aún, con el avance de la tecnología se demuestra que cada vez es más imprescindible para los sistemas de comunicación de voz por la ventaja de operar en entornos ruidosos con bastante inmunidad. Por lo que requiere poseer una codificación robusta en constante mejora, actualizada detección de errores y nuevos métodos de evaluación de la calidad de voz para escucharla lo más clara posible.[18]

La figura 2.3, muestra el diagrama de bloques básicos de un Scrambler Digital de voz. Su funcionamiento se explica de la siguiente manera. En una codificación digital, la señal de voz es primero codificada por un conversor análogo-digital para obtener un adecuado formato digital. Ese formato binario consta de 8 bits y se usa para representar la amplitud de la forma de onda de la señal de voz en repetitivos intervalos de muestreo llamados segmentos de voz. A estos segmentos se les asocia a una contraseña y se les permuta en frecuencias.

Estos segmentos de voz ya digitalizados son sometidos a una codificación digital en donde existen varias técnicas de encriptación ó solamente son codificadas pudiendo ser utilizadas para obtener virtualmente un alto grado de seguridad durante la transmisión en el dominio del tiempo a través del canal de la comunicación. [19]

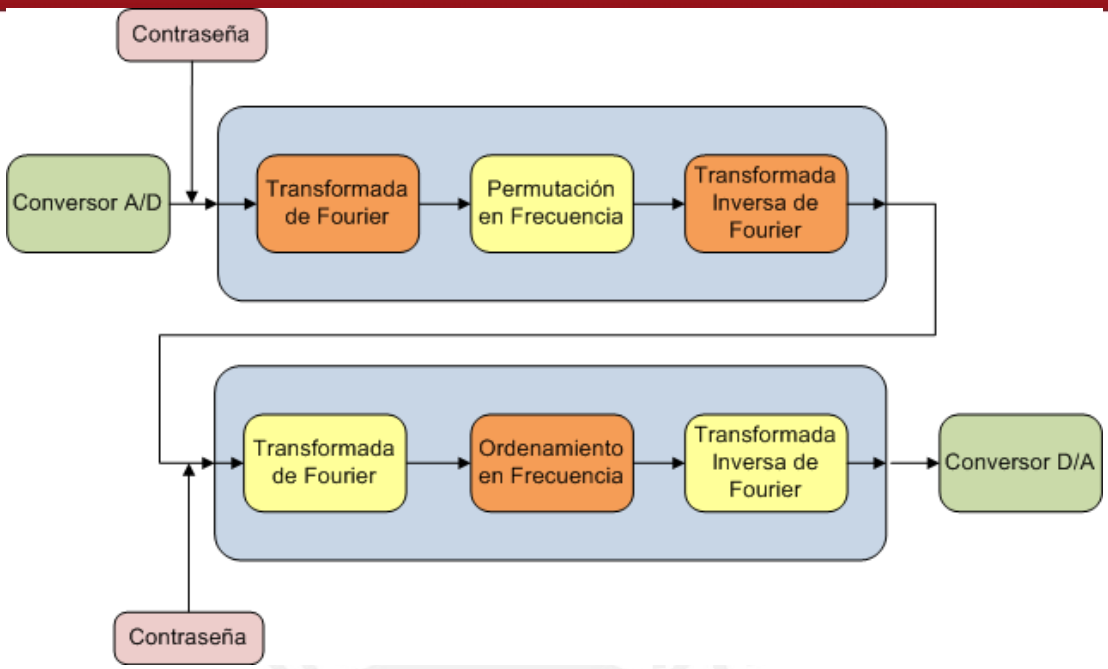

Figura 2.3 Scrambler Digital

En la etapa de recepción se realiza el proceso inverso con el objetivo de recuperar la señal inicialmente procesada y poder comprender el mensaje enviado.

Dado que la codificación digital es más segura y confiable frente a la codificación analógica, la codificación digital no es la ideal por cuanto también posee desventajas. La más importante se percibe en el uso de sistemas de transmisión telefónica donde existe un sustancialmente incremento de ancho de banda. Por ejemplo una transmisión por un canal telefónico que requiere un ancho de banda de 3.5Khz, una tasa de muestreo de 8000 Hz y con 8 bits por muestra supone una tasa de transmisión de 64Kbps.

En la actualidad existen tecnologías de telefonía móvil que permiten reducir la tasa de transmisión como la 3G (Tercera Generación) y dentro de unos años cuando esté totalmente implementada por los operadores de telefonía celular la 4G (Cuarta Generación) será la tecnología más actual y segura en redes móviles. [7]

Si bien se puede conseguir velocidades de transmisión de bits reducidas, esta también puede ser causa de una calidad de voz inferior y de un mayor procesamiento. Sin embargo se tolera esta relación entre calidad de voz y ahorro de ancho de banda puesto que los sistemas de compresión ofrecen una optimización considerable del ancho del banda a la par que ahorra costes. [7]

2.1.2.2 Scrambler Analógico

La codificación analógica fue el primer tipo de codificación que se creó. Luego de pocos años de investigación se creó lo que hoy se llama la codificación digital.

La codificación analógica divide en uno ó más sub-bandas la señal de voz. Estas sub-bandas pueden ser invertidas, reordenadas ó por otro modo pueden ser codificadas con el fin de convertirlas en señales ininteligibles.

En la figura 2.5 se observa una banda limitada de voz de 300Hhz-3000Hhz que filtra todas las componentes en frecuencia que no pertenecen a este rango. Por este motivo al escuchar a una persona hablar por teléfono su voz cambia debido a que sus componentes en frecuencia fueron filtradas. En ese sentido el canal telefónico se comporta como un filtro pasa banda.

El Scrambler analógico en el dominio del tiempo visto en la figura 2.4 es una forma de codificación no segura debido a que cualquier persona ajena a la comunicación puede realizar de forma rápida y sencilla la decodificación de la señal codificada con equipos de última generación probando y analizando todas las combinaciones posibles para demodular cada sub-banda con las cinco frecuencias utilizadas (W1, W2, W3, W4 y w5) en este Scrambler Analógico. Por cada sub-banda codificada se realizaría cinco combinaciones posibles y en total se tendría factorial de cinco (5! = 120) combinaciones para tener éxito en recuperar la señal original.

Los Scramblers trabajan con filtros, dividiendo la señal de voz en bloques de frecuencia ó tiempo para alterar la secuencia inicial de la señal.

La codificación se realiza dividiendo convenientemente la señal de voz en pocas bandas de frecuencia e intercambiando las bandas como se muestra en la figuras 2.6. De esta manera estos segmentos ó sub-bandas de voz se ordenan de acuerdo a una clave definida que es enviada a través de otro canal seguro por el emisor con el objetivo que el receptor reciba esta señal y la reordene para poder escuchar el mensaje como se muestra en la figura 2.7.

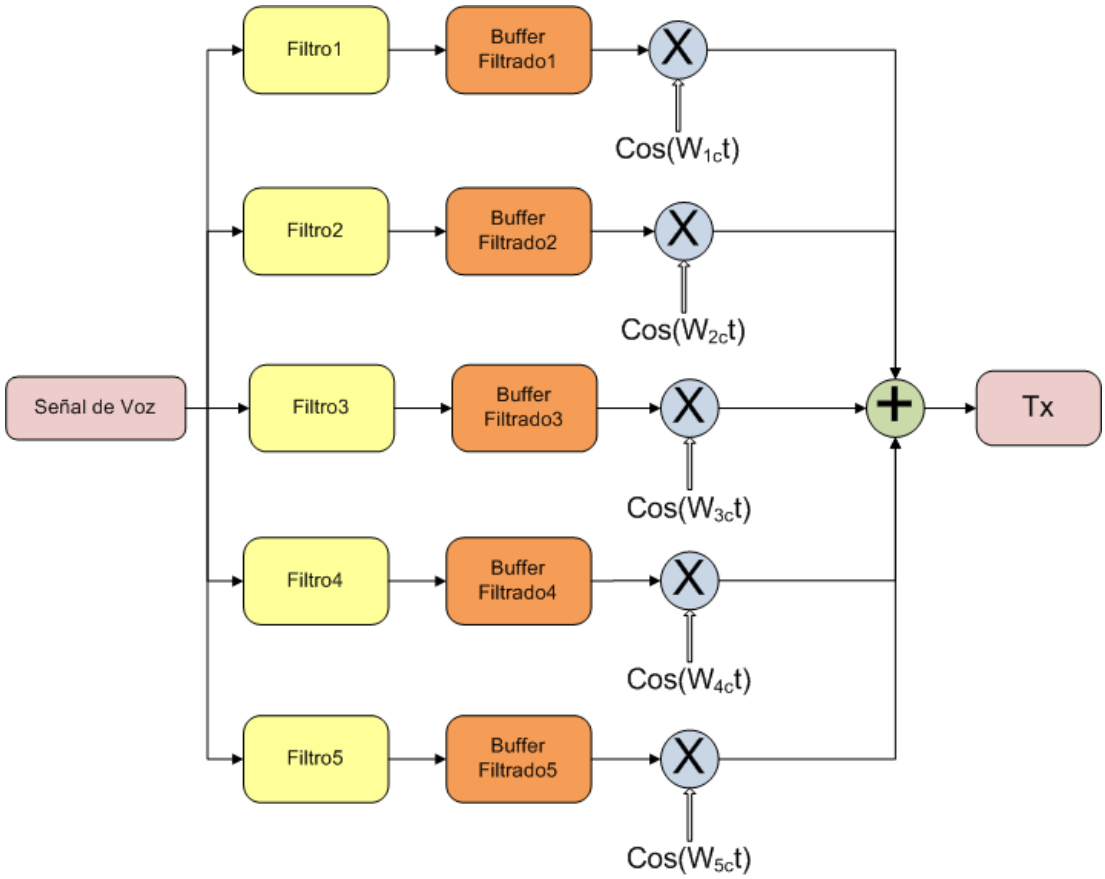

Figura 2.4 Scrambler Analógico

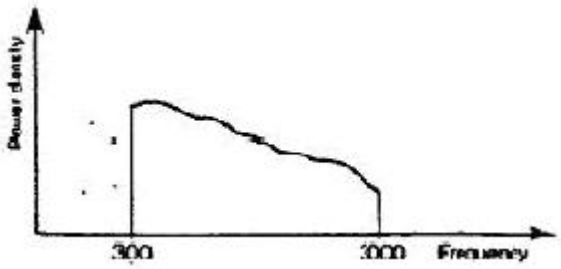

Figura 2.5 Banda limitada de señal de voz 300-3000 Hz [8]

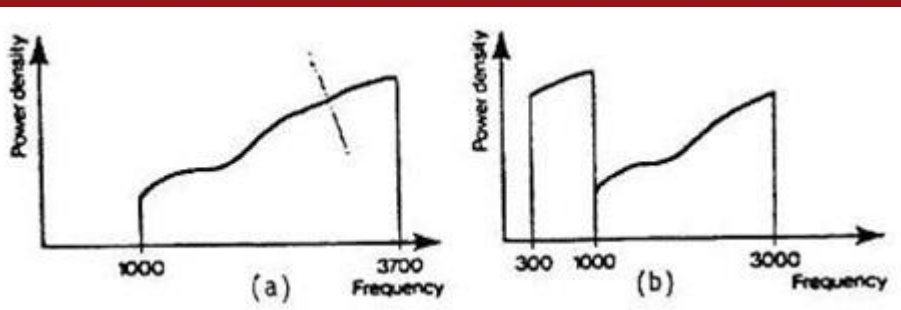

Figura 2.6 Principio de inversión de cambio de banda [8]

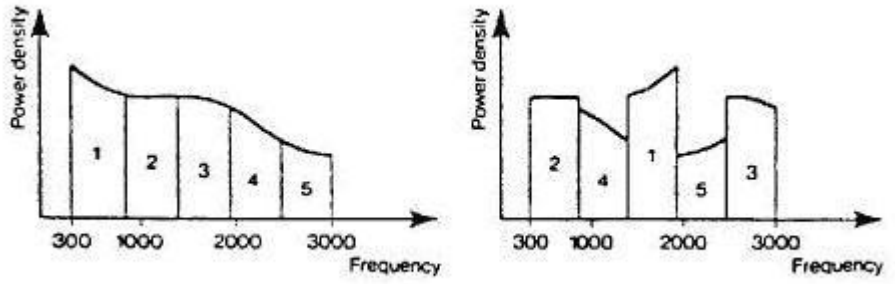

Figura 2.7 Técnica de codificación de banda [8]

La principal desventaja que presenta un Scrambler analógico durante su transmisión es su relativa facilidad de poder *"romper"* su seguridad analizando todas las combinaciones posibles utilizando el método de ensayo y error hasta encontrar la combinación correcta.

Debido a este gran problema, una forma de compensar la transmisión de un *Scrambler Analógico* es requerir mayor complejidad y precisión empleando circuitos altamente sofisticados que hacen uso de algún tipo de encriptación. Además de mencionar el problema principal existen otros a tomar en cuenta como el tiempo de respuesta, la sincronización y la mejor manera de seleccionar el reordenamiento de los pequeños segmentos de voz.

El tiempo de respuesta es una inevitable consecuencia del algoritmo empleado por el Scrambler porque se necesita tiempo para segmentar la voz y ordenarla para su transmisión. Y a su vez también se necesita tiempo para realizar la operación inversa para recuperar la señal de voz lo cual aumenta el retardo. El tiempo de respuesta y la mejor selección de ordenamiento no son los únicos problemas, también existe el problema de sincronización que

depende mucho del tiempo de respuesta, la forma de realizar la transmisión sea full dúplex ó half-dúplex y finalmente la velocidad a la que se transmite la señal.

El no darle la debida importancia a dichos problemas, en el proceso de decodificación se recuperaría cualquier cosa menos el mensaje transmitido. En consecuencia frente a estos problemas, es necesario el uso de Scramblers digitales por ser más robustos y poseer una mejor codificación para el mensaje de voz. En la figura 2.8 se muestra su instalación y uso.

En años anteriores cuando solo existían Scramblers analógicos era muy común el uso de la codificación por inversión de voz la cual proveía una privacidad básica de codificación analógica de voz. En la actualidad este tipo de codificación es fácilmente descifrable por interceptores debido al avance de la tecnología.

Para realizar una comunicación entre dos equipos de codificación analógica se debe tener idéntica combinación de códigos entre ellos de lo contrario no será entendible la comunicación entre el emisor y receptor, dando como resultado la pérdida del mensaje. Esta combinación de códigos lo maneja internamente un Scrambler con la ayuda de una clave.

Para establecer una combinación de códigos los sistemas de codificación telefónica incluyen un selector de combinaciones de códigos que se define antes de empezar la comunicación.

Figura 2.8 Comunicación mediante Scrambler [9]

Esta característica de seguridad impide que un tercero no autorizado compre un equipo codificador telefónico y lo conecte a la línea telefónica ó sintonice una determinada frecuencia y escuche ó manipule conversaciones ajenas y confidenciales como se muestra en la figura 2.9.

Figura 2.9 Comunicación no segura con intermediarios [9]

Para evitar las interceptaciones telefónicas de terceros, los equipos de telefonía que codifican la señal de voz utilizan algoritmos de encriptación para proteger el canal de comunicación y ofrecer una máxima seguridad en la transmisión del mensaje. Entre los algoritmos de encriptación que se hace mención son de tres procesos matemáticos diferentes: Los Algoritmos HASH, Los Simétricos (DES, Triple DES, AES, RC5, IDEA, etc.) y Los Asimétricos (Diffie-Hellman, RSA, DSA, ElGamal). [9]

Para codificar la voz en estos equipos se requiere instalar un equipo de codificación telefónica en cada extremo de la comunicación para codificar y decodificar las señales de voz como se muestra en la figura 2.10.
Con este dispositivo, es posible establecer una comunicación totalmente segura, incluso cuando la línea está intervenida.

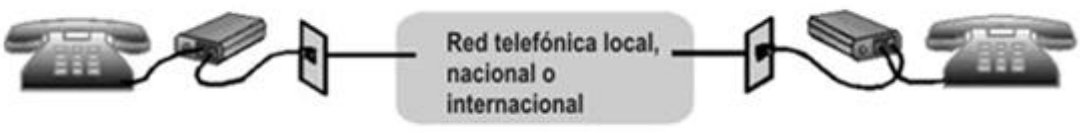

Figura 2.10 Comunicación segura codificada [9]

2.1.3 Elección de la Clave

Para proteger la información a transmitir se suele recurrir a técnicas de codificación que consisten básicamente en convertir el mensaje enviado en otro de forma tal que el mensaje original solo pueda ser recuperado por el otro extremo de la comunicación que solo sabe como decodificar el mensaje haciendo uso de una clave aleatoriamente definida. [10]

La necesidad de usar una clave se debe a que aumenta la seguridad en las comunicaciones previniendo, impidiendo y corrigiendo vulnerabilidades durante la transmisión de la señal de voz.

Para lograr estos objetivos se deben considerar algunos aspectos que se presentan a la hora de elegir una clave. Entre las consideraciones a tomar en cuenta para elegir una clave se tiene: espacio de clave reducido, elección de una clave pobre, claves aleatorias, frases de paso, distribución de claves, almacenamiento de claves, tiempo de vida de la clave y destrucción de claves.

El espacio de clave reducido, se define cuando existen restricciones en el número de bits de la clave, o bien en la clase de bytes permitidos (ya sea caracteres ASCII, caracteres alfanuméricos, imprimibles, etc.). Esta vulnerabilidad permite atacar con hardware especializado o proceso en paralelo todas las combinaciones posibles logrando así desbaratar en un tiempo razonable estos sistemas.

La elección de una clave pobre, se define cuando los usuarios eligen sus claves y esa elección suele ser muy fácil de obtener en general (por ejemplo, su propio nombre o el de alguna otra persona), convirtiéndose en claves muy débiles para un análisis de todas las combinaciones posibles que primero prueba las claves más obvias como el ataque de diccionario.

Las claves aleatorias, son las más seguras porque son cadenas de bits generadas por medio de algún proceso automático como una fuente aleatoria fiable o un generador pseudo-aleatorio seguro.

De tal forma que si la clave consta de 64 bits, las 2^{64} combinaciones o las 18446744073709551616 claves posibles serían igualmente probables.

Las frases de paso, son una solución al problema de la generación de contraseñas seguras y fáciles de recordar por parte del usuario. Las frases de paso son generadas por una frase suficientemente larga que posteriormente será convertida en una clave aleatoria por medio de un algoritmo.

La distribución de claves, hace referencia a los problemas de gestión de claves que constituyen los procedimientos de distribución de éstas mismas ya que esta distribución debe efectuarse previamente a la comunicación. [10]

La seguridad de esta distribución dependerán de para qué y cómo van a ser utilizadas las claves. De esta manera se garantiza la identidad de su origen, su integridad y su confidencialidad.

Las consideraciones más importantes en un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger pero la distribución es automática y la transferencia suele iniciarse con la petición de clave por parte de una entidad a un Centro de Distribución de Claves (intercambio centralizado) o a la otra entidad involucrada en la comunicación (intercambio directo). Otra posible alternativa es una distribución manual (mediante el empleo de correos seguros, por ejemplo), independiente del canal de comunicación. [10]

Esta última alternativa implica un alto costo económico y un tiempo relativamente largo para llevarse a cabo, lo que la hace descartable en la mayoría de las situaciones.

En caso de realizar una distribución de claves sobre un canal inseguro se requiere de protección criptográfica y por tanto, la presencia de otras claves, conformando una jerarquía de claves. En cierto punto se requerirá protección no criptográfica de algunas claves para intercambiar con los

usuarios de forma segura las claves que usarán en sus futuras comunicaciones. [10]

El almacenamiento de claves, en sistemas con un solo usuario es la solución más sencilla que pasa por ser su retención en la memoria del usuario. Pero una solución más sofisticada y que desde luego funcionará mejor para claves largas, consiste en almacenarlas en una tarjeta de banda magnética, en una llave de plástico con un chip ROM (ROM key) o en una tarjeta inteligente, de manera que el usuario solo tenga más que insertar el dispositivo empleado en alguna ranura a tal efecto para introducir su clave. [10]

El tiempo de vida de la clave, refiere a que una clave nunca debería usarse por tiempo indefinido, debe tener una fecha de caducidad, por las siguientes razones:

- Cuanto más tiempo se usa una clave aumenta la probabilidad de que sea usada por otras personas.
- Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, ya que toda la información protegida con esa clave queda al descubierto.
- Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar desbaratarla.
- En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

La destrucción de claves, refiere a la caducidad de las claves que deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de un adversario, puesto que con ellas podrían ser usadas como patrón para decodificar futuras comunicaciones.

En el caso de haber sido escritas en papel, grabadas en una EEPROM, PROM o tarjeta de banda magnética, se deberá buscar la forma de volverlas irrecuperables.

2.1.4 Técnicas de codificación empleadas por un Scrambler

Con el transcurso de los años el conjunto de conocimientos técnicos ordenados científicamente permitieron primero diseñar y luego crear diferentes maneras de transmitir la señal de voz de forma segura mejorando estos conocimientos cada día hasta la actualidad.

Debido a la necesidad de proteger las comunicaciones se inventaron varias técnicas que con el tiempo poco a poco fueron quedando obsoletas por lo vulnerable e inseguras que se convirtieron, lo que incentivó a la creación de nuevas técnicas más sofisticadas, robustas y menos vulnerables.

Las actuales técnicas de codificación pueden desarrollarse tanto en el dominio del tiempo como en el dominio de la frecuencia dependiendo del tipo de codificación a emplear.

Entre las técnicas más importantes se tiene:

- "Salto de codificación por ventanas".
- "Codificación sin cuadro deslizante por ventana".
- "Sistema de codificación analógica empleando una secuencia de coeficientes esferoidales discretos".
- "Codificación por inversión de banda".
- "Sistema de Codificación en el dominio del tiempo ó de frecuencia sin ventana de sincronización".

Salto de codificación por ventanas

Esta técnica se desarrolla en el domino del tiempo y consiste en dividir la señal en iguales periodos de tiempo llamados *frames* (ventanas). Cada ventana es subdividida en un número fijo ***n*** datos de menor tiempo de duración igual a los periodos llamados segmentos, cuya duración de estos segmentos suele ser típicamente en el orden de los 30-50 ms.

Con los segmentos ya definidos, la codificación se realiza permutando dichos segmentos dentro de cada ventana para luego ser transmitidos en el nuevo orden permutado. Para cada ventana, el receptor conoce la permutación realizada en la etapa de codificación siendo capaz de recuperar la señal aplicando una permutación inversa.

Una desventaja importante de esta técnica es el retardo inherente que produce. Este retardo se calcula numéricamente de la siguiente manera. Si la duración del segmento es en **T** segundos, entonces el tiempo total de retardo para el sistema es ***2*n*T***. Por ejemplo si *n*=8 y T=50ms, el retardo del sistema será 0.8 segundos lo cual es un tiempo suficiente para ser perceptible.

A pesar de la existencia de un retardo inherente esta técnica tiene como gran ventaja de ser fácilmente implementada. Esta técnica es más utilizada cuando el requerimiento de la comunicación no es importante realizarla en tiempo real. [11]

Codificación sin cuadro deslizante por ventana

Esta técnica se desarrolla en el domino del tiempo y a diferencia de la técnica anterior el tiempo de retardo puede ser reducido. De hecho esta técnica también posee un inherente retardo en su implementación y se define como *(k+1)*T* segundos, donde la duración del segmento es **T** segundos.

La técnica consiste en escoger uno de los ***k*** elementos almacenados mediante un generador numérico pseudo-aleatorio al inicio de cada segmento. La cantidad de *k* elementos determinará el retardo del sistema. En el otro extremo de la comunicación el receptor almacena los recientes segmentos recibidos.

La ventaja de esta técnica es que provee un alto grado de seguridad y una gran posibilidad de reordenamiento de los patrones reduciendo así considerablemente el nivel de inteligibilidad.

La desventaja que presenta esta técnica se debe a la sincronización al momento de realizar la implementación dado que es necesaria una continua sincronización donde una actualización sincronizada puede estar disponible una vez cada pocos segundos. [12]

Sistema de codificación analógica empleando una secuencia de coeficientes esferoidales discretos

A fin de proporcionar seguridad a los sistemas de comunicaciones, esta técnica convierte la comunicación por voz en una señal analógica inteligible codificándola de forma preestablecida. Su codificación la realiza dentro de la banda de codificación de una manera segura.

Esta técnica primero realiza un muestreo digital de la señal analógica, para luego transformar esas muestras digitales en una forma intermedia digital que pueda ser codificada de una manera ventajosa. Esta forma intermedia digital consiste es una serie de números digitales conocida como "la secuencia discreta de coeficientes esferoidales" ó brevemente "Prolate Coefficients" (PC).

Para obtener la secuencia de coeficientes esferoidales “PC” en el codificador, las muestras digitales son convertidas por multiplicación con una matriz Q. Mientras que en el decodificador se multiplica con una matriz $(Q)^t$ (transpuesta de Q) para convertir las muestras digitales codificadas a la forma de codificación "PC".

La "PC" de la señal original es codificada por un proceso digital particular que resulta en "PC" de la nueva señal analógica codificada con un ancho de banda sustancialmente igual a la señal original. Este proceso digital se realiza multiplicándola con una matriz H y su decodificación se realiza multiplicándola con una matriz $(H)^t$ (su transpuesta). Las matrices H y $(H)^t$ pueden ser cualquier clase de matriz cuya transpuesta sea proporcional a la inversa. Estas matrices son llamadas *Hadamard.*

Las muestras digitales de la señal analógica codificada son semejantes a la forma de las muestras digitales de la señal analógica. Las muestras digitales codificadas son obtenidas directamente de la codificación "PC" y son transmitidas usando una modulación por amplitud de pulsos (PAM).

En la decodificación en el extremo receptor, los dígitos binarios de la señal digital codificada son convertidos a una forma codificada "PC". La codificación "PC" es convertida a una decodificación "PC", esta decodificación es transformada a una forma de muestreo digital para que finalmente estas muestras digitales sean cambiadas a una forma analógica. [13]

Codificación por inversión de banda

Esta técnica se desarrolla en el domino de la frecuencia con una codificación analógica. Esta técnica es relativamente elemental al proporcionar una codificación de voz por inversión de bandas de frecuencia de audio.

En operación significa que en la codificación, la señal se mezcla para ser transmitida con una frecuencia de referencia fija y utilizando un mezclador que a su salida da como resultado la frecuencia de la señal referida menos la frecuencia de la señal original con el fin de obtener una señal inteligible para su transmisión por un canal no seguro.

En el otro extremo de la comunicación, el receptor realiza el proceso inverso para recuperar la señal original. Lo realiza mezclando la señal codificada con la señal correspondiente utilizada durante el proceso de la codificación. A la salida del mezclador da como resultado la señal de frecuencia fija menos la señal codificada obteniendo la señal idéntica a la que se le aplicó la codificación en el emisor.

La mayor desventaja de los sistemas de codificación analógica de voz es que son muy fácilmente interceptables y decodificables por personas ajenas a la comunicación. Esta técnica no es complicada de realizar pero tiene como particular desventaja de requerir un amplio ancho de banda para la

transmisión de la señal codificada que sustancialmente se ve incrementada en la decodificación de la señal de voz debido a la forma inherente del proceso. [14]

Sistema de Codificación en el dominio del tiempo ó de frecuencia sin ventana de sincronización

La siguiente técnica se desarrolla tanto en el dominio del tiempo como en frecuencia evitando así el problema de sincronización de ventanas.

Esta técnica podría ser utilizada directamente para transmitir una comunicación cifrada dado que la expansión del ancho de banda es completamente controlable. Además la llave utilizada para realizar el cifrado es muy grande y permite lograr un alto grado de seguridad.

Esta técnica permite el uso de una señal digital codificada por el emisor para transmitir dígitos al receptor quien es capaz de decodificar la señal digital transformándola en una señal analógica.

La codificación de esta técnica comienza con la transformación de la forma de onda de la señal de voz mediante un conversor A/D para luego segmentarla en una cantidad fija de N muestras digitales. La codificación continúa con la aplicación de algún procedimiento predeterminado para formar el vector V con los varios segmentos obtenidos en la etapa anterior. Seguidamente se le aplica la transformada rápida de Fourier al vector V dando como resultado el vector W. A este vector se le multiplica con una matriz criptográfica M de N x N para luego realizar una combinación lineal de múltiples permutaciones uniformes resultando el vector T.

Finalmente mediante un conversor D/A la señal codificada y permutada se convierte a una señal analógica para poder ser transmitida al receptor a través del canal de comunicación. Una vez recibida la señal analógica codificada por el receptor se realiza el proceso inverso para reconstruir la señal tal cual como la fue originalmente.

Dada la seguridad que brinda, esta técnica no es perfecta y posee desventajas como: el requerimiento de una sincronización entre emisor y el receptor, ser costosa y estar sujeta a la interrupción de la transmisión debido a la pobre condición del canal de comunicación. Además siendo el canal inseguro y vulnerable se ve la necesidad de crear instalaciones de transmisión digital.

La invención de esta técnica proporciona mejoras a las desventajas anteriormente mencionadas. Sin embargo el medio de la señal de comunicación adoptada en esta técnica sigue siendo una transmisión de modo convencional lineal. [15]

CAPÍTULO III

PLANEAMIENTO DEL DISEÑO DE UN SISTEMA DE SEGURIDAD DE VOZ DIGITAL

3.1 Descripción

La presente Tesis tiene como objetivo principal mostrar lo factible que es utilizar un Scrambler Digital para lograr un canal de comunicación segura. Se manejará entradas y salidas de audio logrando de esta manera realizar modificaciones en la señal de voz para un mejor análisis y convertirla en menos vulnerable. Se presentarán simulaciones bajo la plataforma MATLAB porque muestra muchos beneficios en el análisis de pruebas experimentales.

La presente tesis propone tomar la señal de voz digitalizada proveniente de una tarjeta de sonido a una frecuencia de muestreo de 8000Hz. La figura 3.1 muestra la secuencia a seguir.

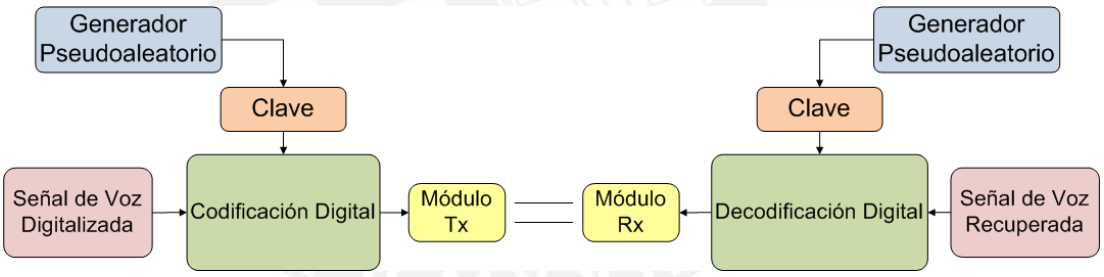

Figura 3.1 Proceso de Codificación y Decodificación en el Scrambler propuesto

Como se aprecia en la figura 3.1 a la voz digitalizada se codifica empleando una clave de cinco números la cual es obtenida de un generador pseudoaleatorio en ambos extremos de la comunicación. Luego de ser codificada la señal es modulada para su transmisión a través del canal. Los módulos de Tx y Rx no se desarrollarán para el diseño de la presente tesis.

El generador pseudoaleatorio introduce un método de generación de números aleatorios mediante el cual un término de la serie se obtiene como

función del término inmediatamente anterior ($x_n=f(x_{n-1})$). La función aplicada es la siguiente:

$$x_{n+1} = (ax_n + c) \bmod m, \quad siendo\ 0 \le x_n < m\ \forall n \qquad \textbf{(3.1)}$$

En el generador se distingue cuatro elementos:

- x_0, es el valor inicial o **semilla**.
- a, **multiplicador**, siendo $0 \le a < m$.
- c, **incremento**, siendo $0 \le a < m$.
- m, **módulo.**

Los valores a, x_0 y c tienen que ser mayores que cero. Y la variable m tiene que ser mayor que las tres anteriores. Veamos como genera los valores arbitrarios. Suponiendo que a = 5, c = 7, X_0 = 7 y m = 8. Entonces los resultados se observan en la siguiente tabla 3.2

n	X_n	X_{n+1}
0	7	2
1	2	1
2	1	4
3	4	3
4	3	6
5	6	5
6	5	0
7	0	7

Tabla 3.2 Secuencia de números aleatorios

Nótese que después de 8 pasadas el valor inicial de X_n se repite. Decimos entonces que el **periodo del generador** es 8 igualito al valor del módulo siempre y cuando el valor del periodo sea mayor que m.[21]

Con la señal codificada en el otro extremo de la comunicación, se recibe la señal para decodificarla empleando la misma clave que usó en proceso de

codificación. Los módulos de Codificación y Decodificación se explicarán detalladamente a continuación.

3.1.1 Codificación

El proceso de codificación se inicia con la necesidad de codificar la señal de voz para acotarla en un intervalo de tiempo con la finalidad de poder hacer un mejor análisis. De esta manera se segmenta la señal de voz en ventanas de datos que pudieran contener o no información alguna dependiendo del tamaño de ventana. La figura 3.3 ilustra con más detalle el proceso de codificación.

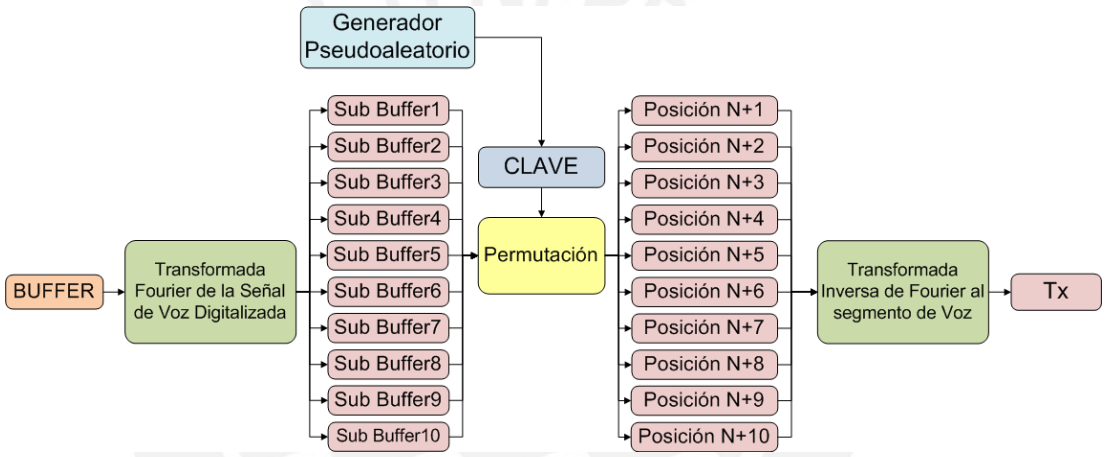

Figura 3.3 Proceso de Codificación del Scrambler propuesto

En la figura 3.3 se observa el proceso secuencial de la codificación que comienza con la aplicación de la transformada de Fourier a un segmento de la señal de voz contenida en un buffer.

Cada buffer a codificar es permutado en frecuencia y a su vez es subdividido en diez sub-buffers con la finalidad de realizar internamente las permutaciones en frecuencia de estos sub-buffers dentro de cada buffer. Las permutaciones son definidas por la clave de cinco números. Finalmente, el buffer codificado es transmitido en el dominio del tiempo

Antes de empezar la codificación es bueno tener en cuenta que el contenido de cada buffer no asegura abarcar todos los datos segmentados de la señal

de voz y más aún puede darse el caso de incluir algunos datos parciales ó quizás tener información irrelevante. Esto ocurre cuando los buffers no tienen la misma cantidad de datos. Siendo la cantidad de datos un parámetro de entrada en la simulación.

En la simulación se codifica una señal con 8000 muestras por segundo en un intervalo de 2 segundos. La codificación secuencial se inicia con la aplicación de la transformada de Fourier al segmento de la señal de voz digitalizada contenida en buffers de 512 datos.

Luego cada buffer es segmentado en 10 sub buffers para ser permutarlos internamente con la clave proporcionada por el generador pseudo aleatorio. Al permutarlos se salva el dato1, el dato256 y el dato 512. Luego los demás datos son agrupados en pequeñas ventanas de 51 datos para formar los sub buffers que con la ayuda de la clave son permutados en grupo. Como se explicará más adelante gráficamente el sub buffer1 se permutara al mismo tiempo que el sub buffer10 en cualquiera de las 5 posiciones posibles. De igual forma se realizará con el sub buffer2 con el sub buffer9 y así sucesivamente hasta llegar el sub buffers 5 con el sub buffer6.

Cuando se mencionó que los buffers no tienen la misma cantidad de datos se debe a que las pequeñas ventanas tienen un valor mayor o menor a 51datos. Cuando se tiene más de 51 datos, los buffers no tienen toda la información a permutar convirtiéndose en buffers con información irrelevante de valor cero por lo cual son descartados para la codificación. Si la pequeña ventana tiene menos de 51 datos los buffers almacenan poca información y no completan una correcta codificación de los 512 datos. Esto se aprecia al escuchar la señal voz cortada respecto de la señal original.

Una vez permutados los sub buffers se continua con la permutación de los buffers. Estos son permutados de igual forma que los sub buffers en grupo. El buffer1 se permuta al mismo tiempo que el buffer10 y así sucesivamente.
La permutación de los diez sub buffers y los buffers se realiza con la señal de voz segmentada en frecuencia y la clave de cinco números.

La clave proveniente de un generador pseudoaleatorio indica las posiciones a permutar en frecuencia los diez sub-buffers contenidos en el buffer de análisis para cada transmisión secuencial con la finalidad de aumentar la seguridad durante la transmisión.

La clave define las posiciones a permutar de la siguiente manera. Cada posición del uno al cinco tiene su recíproco en posiciones que comienza de la posición seis a la diez lo cual asocia por ejemplo la posición uno con la posición diez, la posición dos con la posición nueve, la posición tres con la posición ocho y así sucesivamente hasta completar las cinco posiciones posibles. Hablar de asociar se refiere a mover a otra posición en conjunto estos buffers en caso de un cambio de contraseña.

El orden que establece la clave consiste en permutar simétricamente con respecto al origen los sub-buffers en cinco posiciones diferentes de tal forma que el sub-buffer1 y el sub-buffer10 se permuten juntos. De igual forma ocurre con el sub-buffer2 y el sub-buffer9 y así sucesivamente hasta llegar con los sub-buffer5 y el sub-buffer6 en conjunto. La figura 3.4 ilustra una mejor explicación.

Las posiciones establecidas ordenadamente por la clave se pueden definir imaginariamente si se imagina en una recta numérica acotada que va desde -5 a 5 descartando el cero. Entonces a modo de ejemplo, las posiciones del sub-buffer1 y sub-buffer10 corresponderían a los números -5 y 5 respectivamente. De igual forma para el sub-buffer2 y sub-buffer9 les correspondería los números -4 y 4 respectivamente y así sucesivamente hasta llegar a los sub-buffer5 y sub-buffer6 que les corresponderían los números -1 y 1. Comprendida las posiciones que define la clave, se realiza las permutaciones en frecuencia de dos sub-buffers en conjunto como se explicó anteriormente.

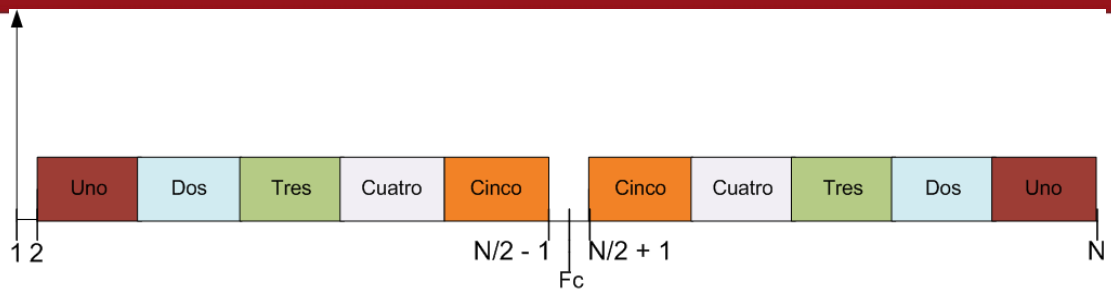

Figura 3.4 La Clave Ordenada

Con los sub-buffers ya permutados en frecuencia de acuerdo a la clave se procede a permutar el buffer completo con sus diez sub-buffers en una posición definida por la clave. A diferencia de la permutación de los sub-buffers donde la clave tiene cinco números, ahora la clave es internamente convertida en una nueva clave de diez números para definir todas las posibles posiciones de los probablemente diez buffers validados como máximo en caso todos los buffers contengan información.

A modo de ejemplo, si en un momento dado el generador pseudoaleatorio diera la siguiente secuencia: 4, 2, 1, 3 y 5 entonces la permutación gráficamente se realizaría como se muestra en la figura 3.5.

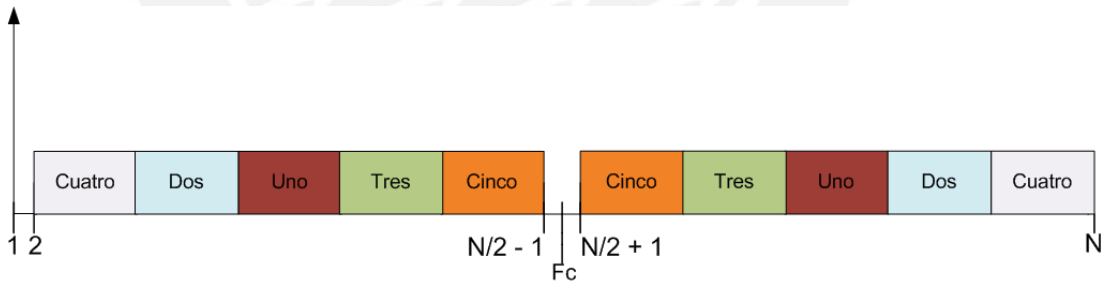

Figura 3.5 La Clave en un momento dado

Luego de permutar cada buffer se transmite secuencialmente en tiempo para que posteriormente sea decodificada del otro lado de la comunicación en el orden que fuese recibido. Pero dado que el buffer esta en frecuencia, no es posible transmitirlo de esta manera por lo cual se le aplica la transformada inversa de Fourier y se toma solo la parte real para transmitirlo. El proceso de codificación continúa secuencialmente con el siguiente buffer hasta completar toda la señal de voz originalmente digitalizada.

Para efectos de análisis, el código desarrollado fue almacenando buffer a buffer hasta completar los diez en un solo arreglo y poder observar mediante una gráfica como se transmite la señal buffer secuencialmente.

3.1.2 Decodificación

La decodificación realizada en el otro extremo de la comunicación no es más que hacer los mismos procedimientos explicados anteriormente pero en orden inverso a como fue realizada en la codificación.

Para la decodificación, lo primero que se hace es obtener los datos que se usaron en la codificación como: la clave empleada en la permutación y el tamaño de ventana de los buffers y sub-buffers. Con estos datos obtenidos se recupera la señal de forma secuencial tal como se recibió. La figura 3.6 ilustra mejor el proceso de decodificación.

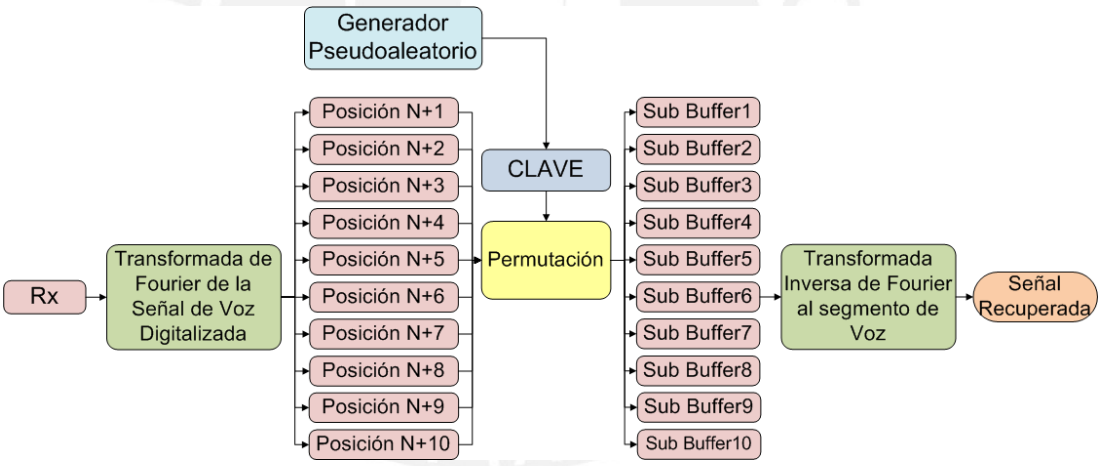

Figura 3.6 Proceso de Decodificación del Scrambler propuesto

La figura 3.5 muestra como se recupera la señal de voz proveniente de la codificación en buffers que son recibidos y decodificados secuencialmente para su posterior recuperación. De esta forma se procede hasta completar la señal de voz digitalizada. El proceso de decodificación ilustrado se inicia secuencialmente con la aplicación de La Transformada Inversa de Fourier al buffer recibido para desplazarlo en el dominio de la frecuencia debido a que son recibidos en el dominio del tiempo.

Los buffers con su respectiva ventana de datos son permutados nuevamente a la posición en la cual fueron segmentados antes de ser codificados. De esta manera se recupera las posiciones originales la señal de voz recién digitalizada. Por ejemplo el buffer5 que permutada en otra posición definida por la clave es reubicada en la posición cinco tal como lo estuvo antes de ser codificada. De igual forma se hace con los demás buffers que contengan información de la señal de voz digitalizada.

Una vez lograda la reubicación del buffer en análisis se realiza las permutaciones en frecuencia de los sub-buffers de acuerdo a la clave para ubicarlos en las posiciones iniciales antes de ser codificados.

Si se diera el caso de encontrarse algún sub-buffer con sus datos iguales a cero no será tomado en cuenta en la decodificación debido a dos circunstancias que puede haber sucedido: la primera, la ventana de datos del sub-buffer es mayor que la ventana de datos del buffer en análisis produciéndose una incoherencia ó la segunda posibilidad, si se decidió tener grandes ventanas estas abarcarán la mayor cantidad de datos lo que producirá que las restantes ventanas sean cero porque el tamaño de la voz a analizar es limitado y no se puede obtener un tamaño mayor a este.

Ordenados los sub-buffer se continúa con la unión de estos en uno solo con la finalidad de obtener el mismo buffer con la misma ventana de datos ordenados como lo estuvo originalmente.

Finalmente, con el buffer recuperado en el dominio de la frecuencia se le aplica La Transformada Inversa de Fourier con la finalidad de obtener la señal de voz en el dominio del tiempo lo cual devuelve una señal de voz muy parecida a la que fue digitalizada inicialmente pudiéndose ser escuchada en altavoces.

CAPÍTULO IV
RESULTADOS EXPERIMENTALES

Con el objetivo de diseñar y simular un Scrambler Digital de Voz y logar una comunicación segura que solo el receptor pueda decodificar el mensaje recibido se muestran los siguientes resultados experimentales las cuales permiten que la presente tesis sea viable.

Estos resultados se realizaron bajo la plataforma de Matlab con la finalidad de observar con más detalle el análisis de su espectrograma y saber cuan verídica es una señal original respecto de su señal decodificada ya sea de: voz, un conjunto de tonos y una señal matemáticamente artificial. El análisis se detallará a continuación.

4.1 Verificación de la señal de voz

El resultado de esta prueba experimental tiene por objetivo analizar cuanto tiene de similitud la señal de voz inicialmente digitalizada respecto de la señal de voz reconstruida. Esta definición hace mención al uso de la distancia euclidiana de señales en tiempo discreto.

Con la definición brevemente explicada referente a la distancia euclidiana en tiempo discreto, lo que se pretende es conocer la distancia euclidiana entre la señal original y la señal decodificada concluyendo que si la distancia euclidiana (ver ecuación 4.1) entre ambas señales es cero se puede afirmar que es la misma señal. Caso contrario ambas señales no guardan similitud alguna.[16] Este cálculo matemático se obtiene de la siguiente manera:

$$\text{Error} = \| x\_ori - x\_rec \|_2 = \sum (x\_ori(k) - x\_rec(k))^2 \qquad \textbf{(4-1)}$$

4.2 Análisis espectral de la señal de voz

El análisis espectral se va realizar mediante un espectrograma el cual proviene del resultado de calcular el espectro de tramas ventaneadas de una señal de voz. Visualmente representa las variaciones de la frecuencia en eje

vertical y en el eje horizontal muestra la intensidad de la señal de voz mediante colores o grises a lo largo del tiempo.

A modo de ejemplo, el espectrograma de la figura 4.1 corresponde a un ejemplo de una señal segmentada y permutada en frecuencia respecto de la señal original de acuerdo a una clave de cinco dígitos dejándola lista para ser transmitida. Esta descripción realizada en la codificación es lo que hace el Scrambler propuesto para la presente tesis.

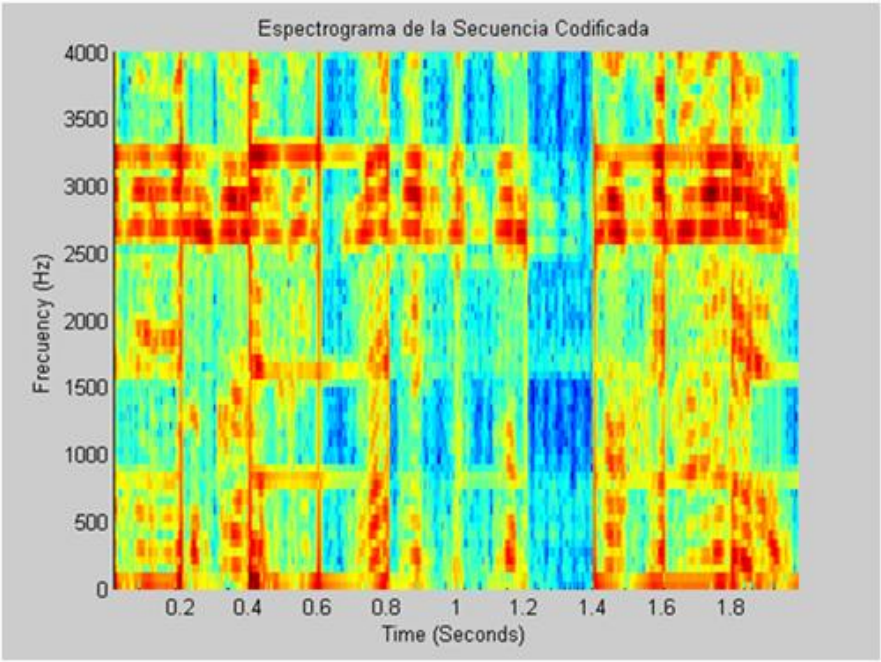

Figura 4.1 Ejemplo de Espectrograma de la Señal de Voz Codificada

4.3 Secuencia de tonos

Esta prueba experimental tiene como objetivo reemplazar la señal de voz a codificar por una secuencia de diez tonos ordenados simétricamente respecto al origen. Además esta simetría se hace más evidente gráficamente al observar la amplitud de cada tono con su par simétrico. Por lo cual los primeros cinco tonos tienen una amplitud diferente y sus tonos simétricos respecto al origen tienen la misma amplitud correspondiente.

Cada tono referido está asociado de acuerdo a la posición en que se encuentra. Por ejemplo, el tono1 está asociado al tono10, el tono2 al tono9,

y así sucesivamente hasta completar el tono5 con el tono6. En la figura 4.2 se puede apreciar lo explicado.

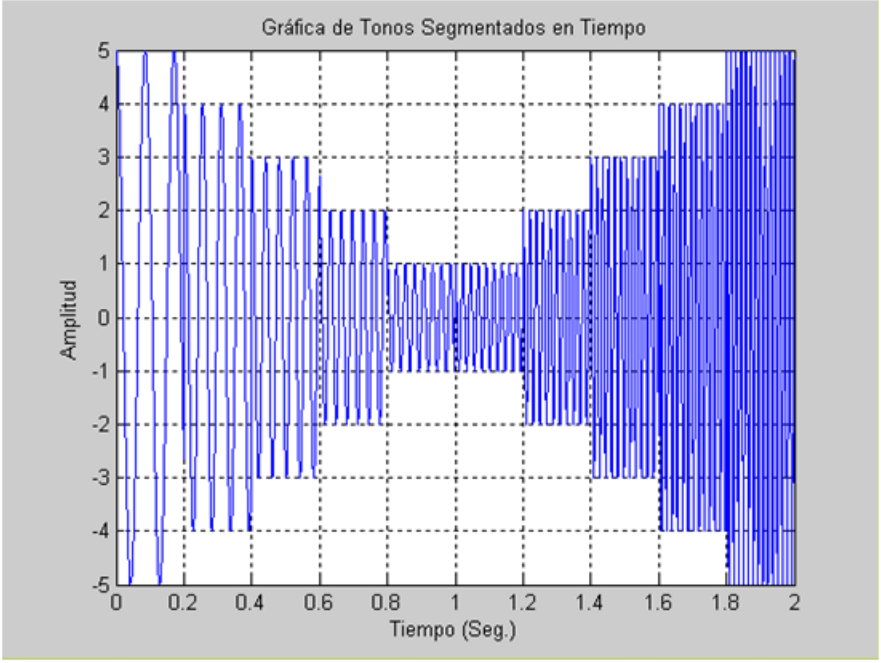

Figura 4.2 Secuencia de Diez Tonos Originales

Para esta prueba experimental, se analizarán los respectivos espectrogramas de los tonos originales, tonos codificados y tonos recuperados para observar las frecuencias permutadas en la codificación y las frecuencias reordenadas en la decodificación. La figura 4.3 ilustra los tonos antes de codificar.

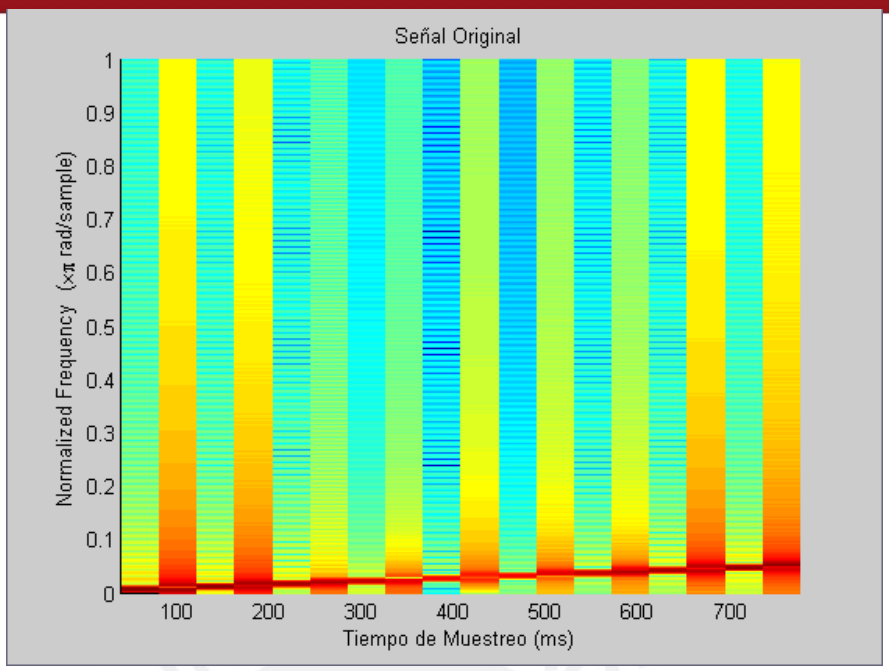

Figura 4.3 Espectrograma de Los Tonos Originales

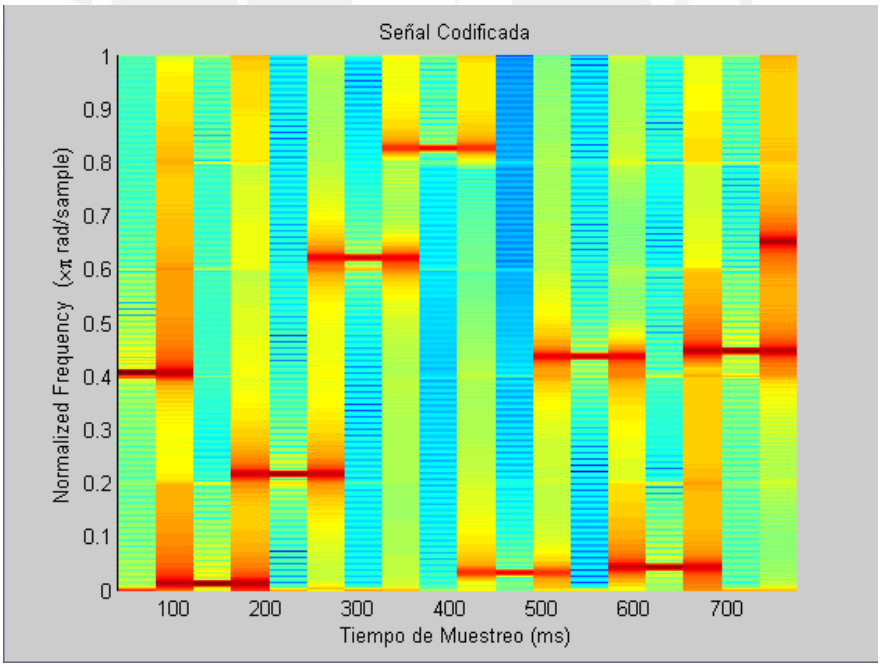

Figura 4.4 Espectrograma de Los Tonos Codificados

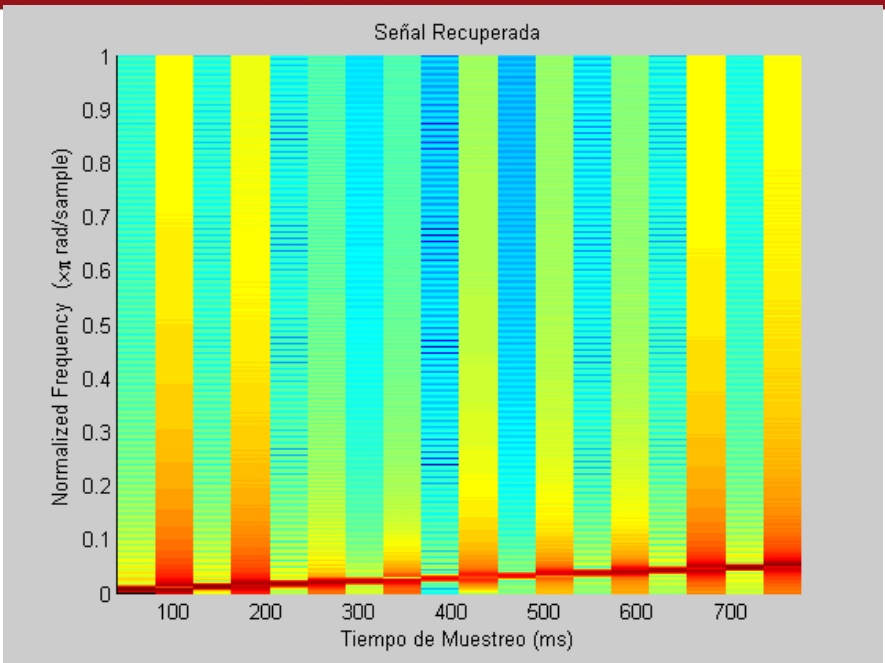

Figura 4.5 Espectrograma de Los Tonos Recuperados

Su similitud referida al cálculo de error explicado anteriormente se obtiene Error=(1.0736)*(10)$^{-27}$, permitiendo concluir que la señal artificial decodificada es muy similares a la señal original. Gráficamente se observa en la figura 4.6.

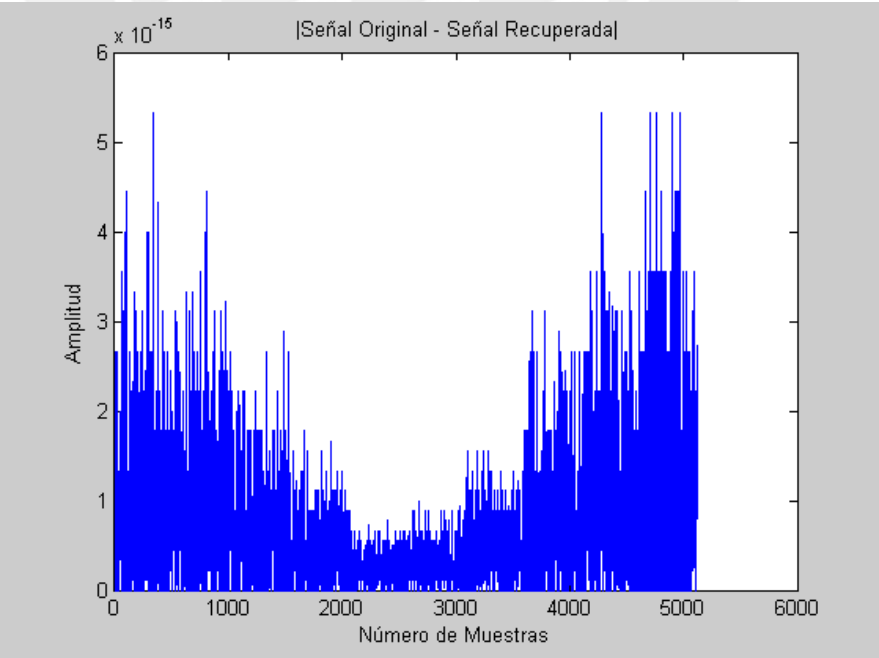

Figura 4.6 Diferencia entre Señal Original y Señal Recuperada

4.4 Representación matemática de una señal artificial

Esta prueba experimental con respecto a la anterior la hace más autentica al codificar y decodificar una señal artificial.

Esta prueba consiste en analizar la señal artificial de forma matemática empleando tonos senoidales y cosenoidales con frecuencias y fases distintas para luego sumarlas y obtener la señal artificial.

Esta suma consta de tres elementos con los valores:

$w_1=2*\pi*700Hz$, $w_2=2*\pi*900Hz$, $w_3=2*\pi*1200Hz$.

$A= \cos(w_1*t)$, $B=\text{sen}(w_2*t)$, $C=\cos(w_3*t + \pi/4)$

Entonces la voz artificial tendría la siguiente forma

Voz Art.= cos(w1*t) + sen(w2*t) + cos(w3*t + π/4)

La voz artificial matemáticamente creada se muestra en la figura 4.7

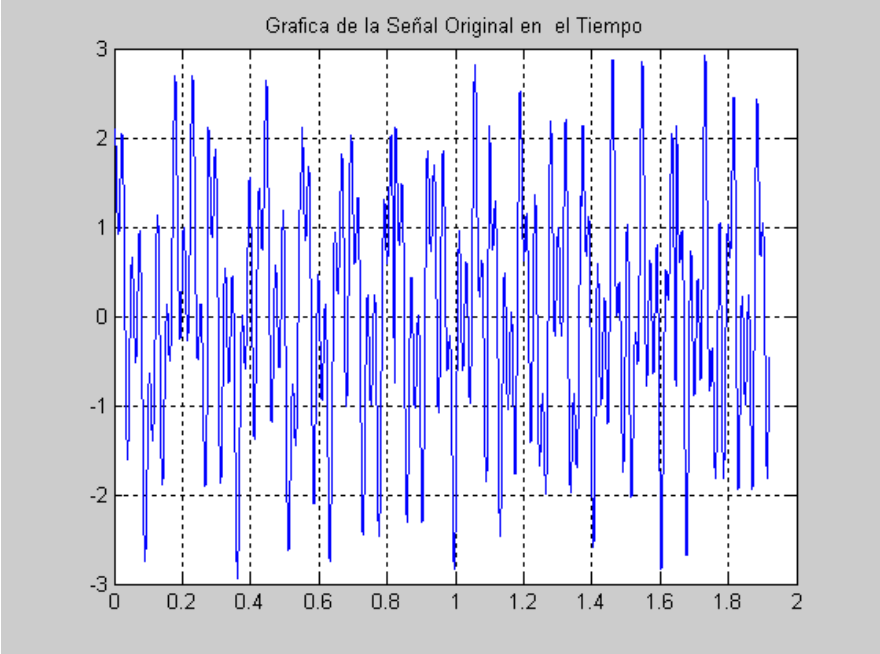

Figura 4.7 La Señal Artificial

Para esta prueba experimental, se analizarán los respectivos espectrogramas de la señal artificial original, la señal artificial codificada y la señal artificial recuperada para observar las frecuencias permutadas al codificarlas y las frecuencias reordenadas al decodificarlas. La figura 4.8 lo ilustra mejor.

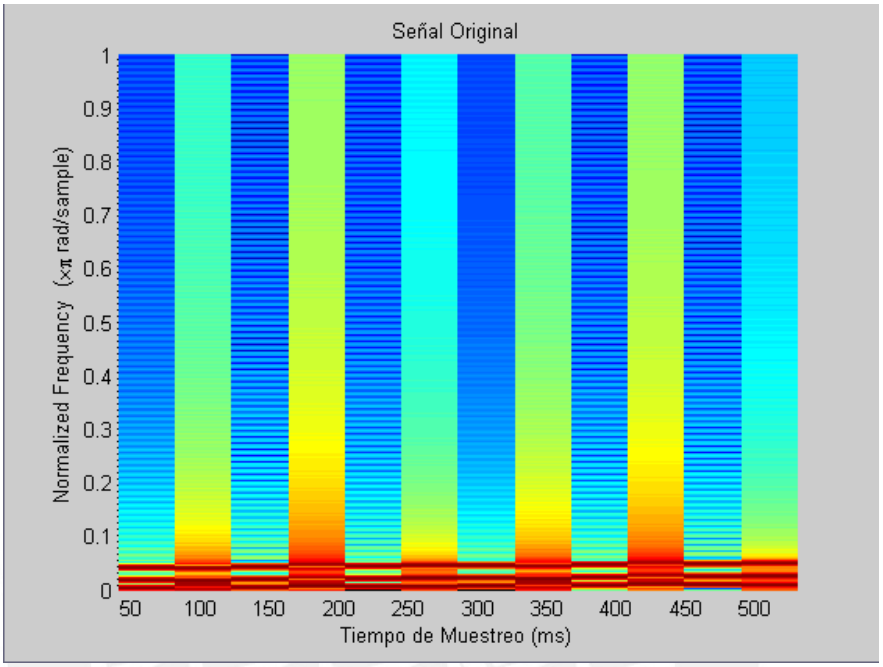

Figura 4.8 Espectrograma de Señal Artificial Original

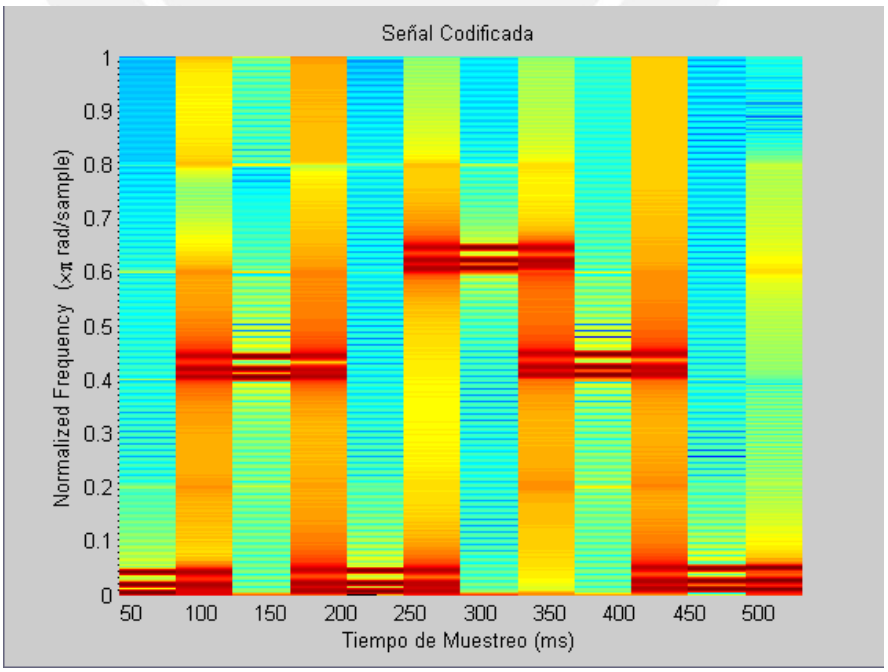

Figura 4.9 Espectrograma de Señal Artificial Original Codificada

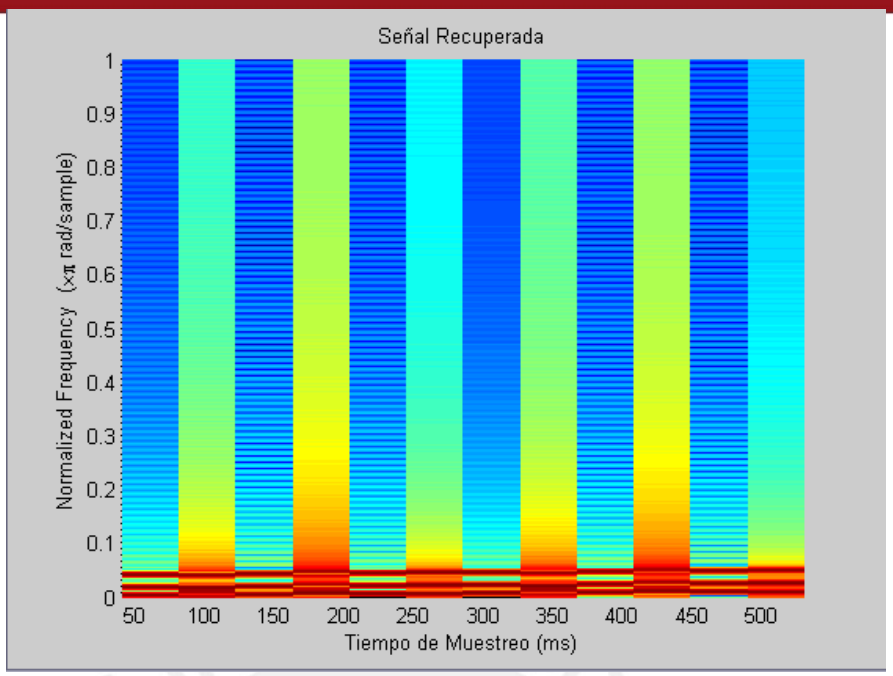

Figura 4.10 Espectrograma de Señal Artificial Original Recuperada

Su similitud referida al cálculo de error explicado anteriormente se obtiene Error=(1.0172)*(10)$^{-28}$, permitiendo concluir que la señal artificial decodificada es muy similares a la señal original. Gráficamente se observa en la figura 4.11.

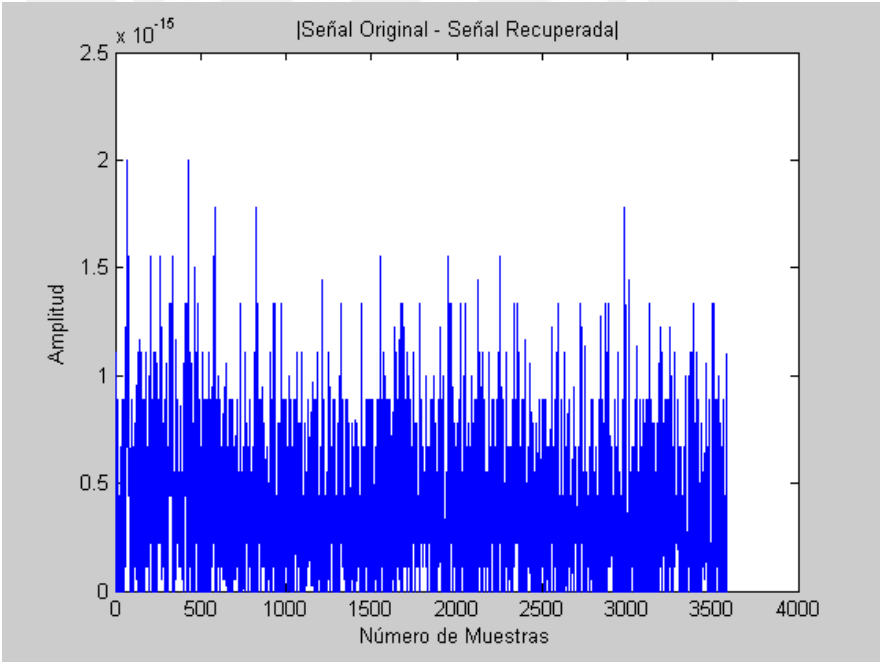

Figura 4.11 Diferencia entre Señal Original y Señal Recuperada

4.5 La Voz Natural

Esta prueba experimental consiste en analizar el espectrograma de la codificación y decodificación para ver como las frecuencias son permutadas al codificarlas y reordenadas al decodificarlas. La figura 4.12 ilustra el espectrograma de la señal antes de codificar.

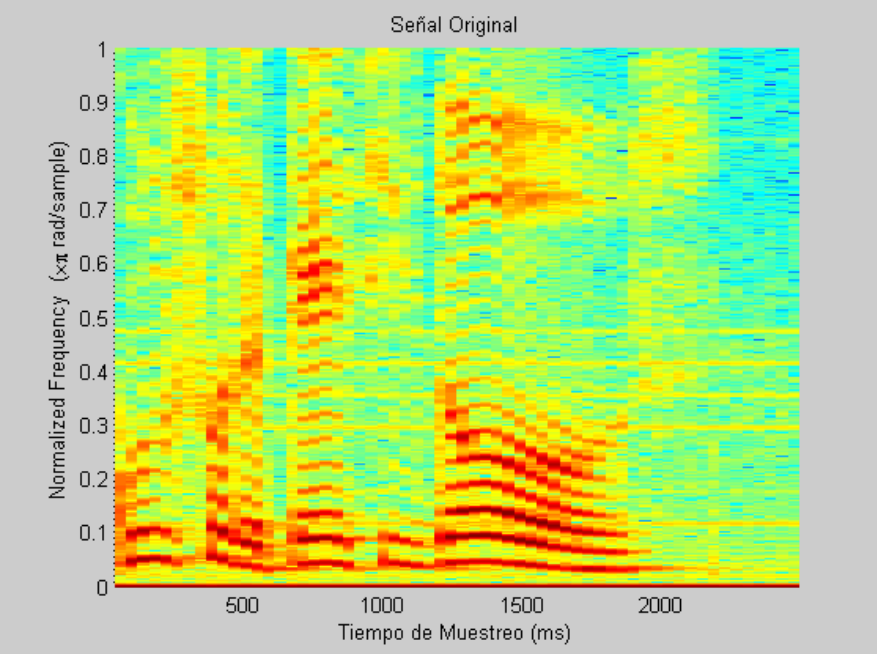

Figura 4.12 Espectrograma de la Voz Natural

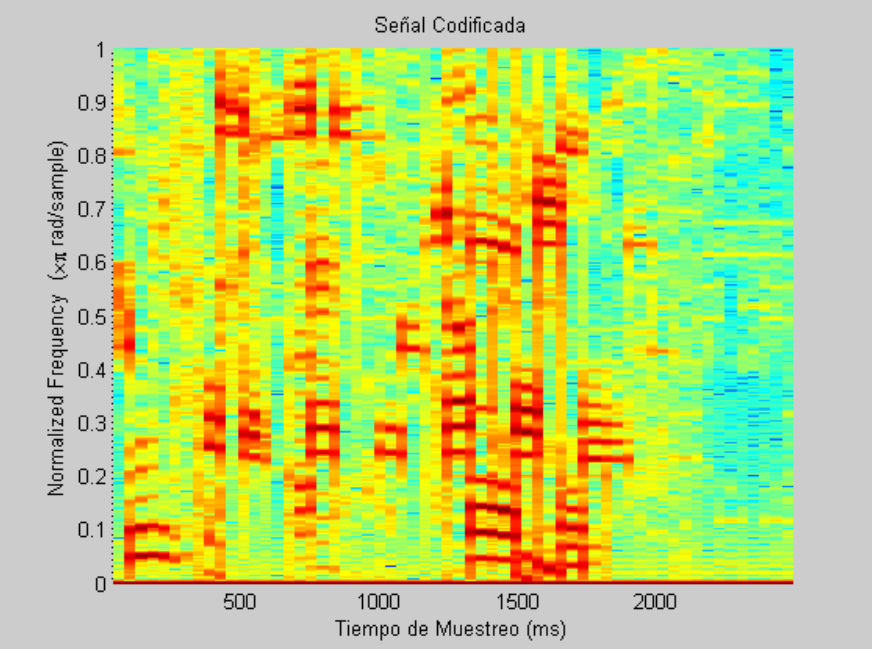

Figura 4.13 Espectrograma de la Voz Natural Codificada

Del otro extremo de la comunicación se decodifica la señal. La figura 4.14 muestra el espectrograma de la señal de voz decodificada.

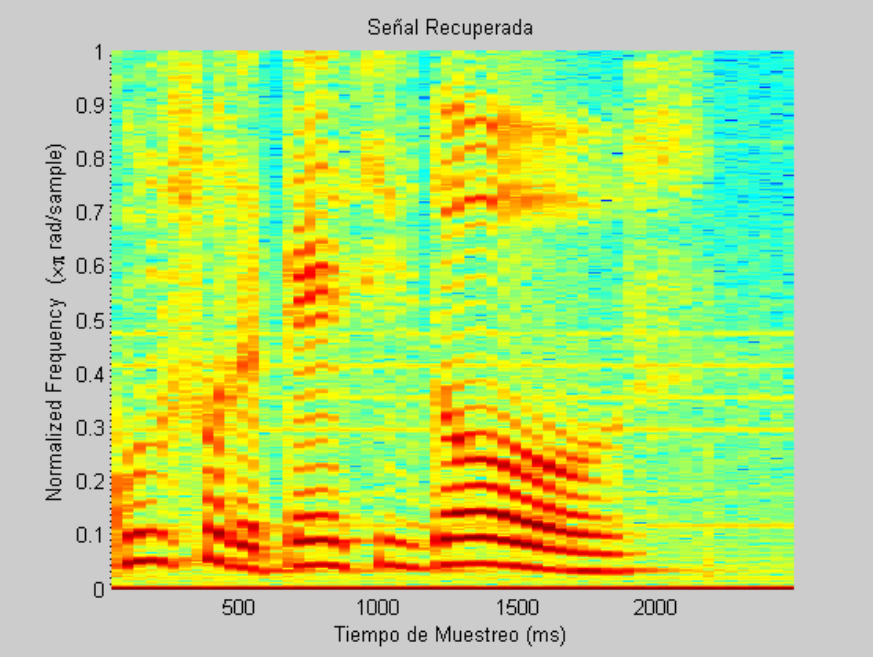

Figura 4.14 Espectrograma La Voz Natural Decodificada

Su similitud referida al cálculo de d_{xy} explicado anteriormente se obtiene $d_{xy}=(2.2461)*(10)^{-32}$, permitiendo concluir que la señal artificial decodificada es muy similar a la señal original. Gráficamente se observa en la figura 4.15.

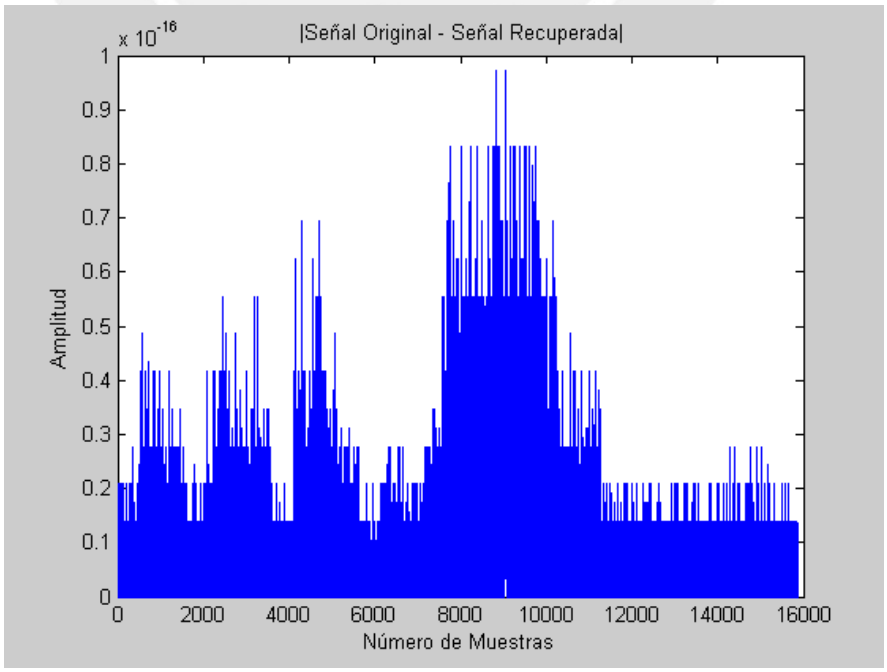

Figura 4.15 Diferencia entre Señal Original y Señal Recuperada

CONCLUSIONES

- El diseño y simulación del Scrambler Digital propuesto asegura la autenticidad e integridad de la señal de voz transmitida a través del canal.

- Los resultados experimentales demuestran que en un intento de interceptación de la comunicación se produciría un sonido ininteligible debido a que el contenido frecuencial está diseminado en todo el ancho de banda destinado.

- Experimentalmente tener una clave aleatoria para cada permutación dificulta cualquier intento de recuperar la señal de voz original.

- Experimentalmente se verificó la veracidad de una señal original respecto de la señal recuperada escuchando ambas señales por separado mediante altavoces resultando ambas señales muy semejantes. Además matemáticamente también se pudo comprobar dicha veracidad mediante el uso de la distancia euclidiana en tiempo discreto.

- De los resultados experimentales se puede concluir que las señales de voz analógica analizadas (Artificial, Ideal y Real) experimentalmente y teóricamente demuestran que el Scrambler digital de voz propuesto cumple con los objetivos de la presente tesis.

RECOMENDACIONES

- La clave es una información confidencial que no se debe transmitir por el canal, por el contrario debe ser transmitida a través de otro canal seguro.

- Usar el presente diseño de Scrambler Digital de voz para comunicaciones de bajo a mediano nivel de seguridad, ya que para una mayor seguridad se recomienda hacer uso de equipos con encriptación.

- Utilizar siempre las recomendaciones internacionales de organismos consolidados como la UIT-T, ANSI, IEEE, ETSI, ya que definen estándares de telecomunicaciones que aseguran un buen funcionamiento de las tecnologías y equipos.

BIBLIOGRAFÍA

[1] W. Tomasi, *Sistemas de Comunicaciones Electrónicas*, Prentice Hall, cuarta edición, México, 2003.

[2] B. P. Lathi, *Introducción a la Teoría y Sistemas de Comunicación*, Limusa, S.A., Decimonovena Edición, México, 2001.

[3] A. V. Oppenheim, A.S. Willsky and S.H. Nawab, *Señales y Sistemas*, Prentice-Hall, Segunda Edición, México, 1998.

[4] R. P. Areny, *El Adquisión y Distribución de Señales*, Marcombo, 1993.

[5] B. P. Lathi, *Sistemas de Comunicación*, McGraw-Hill/Interamericana, México, 1991.

[6] H. J. Beker, C.J. Mitchell *Permutations with restricted displacement*, *Society for Industrial and Applied Mathematics*, Philadelphia, PA, EE.UU. , pag. 338-363, 1987.

[7] A. R. Mishra, *Fundamentals of Cellular Network Planning and Optimization 2G/2.5G/3G...Evolution to 4G,* John Wiley & Son, Ltd, England, 2004.

[8] H. J. Becker, *Analogue Speech Security Systems*, Milford Industrial Estate, EE.UU, 1998.

[9] J. Seberry, J. Pieprzyk, *Cryptography and Introduction to Computer Security*, Pentice Hall, 1989.

[10] G. Álvarez, P. Pérez *Seguridad informática para empresas y particulares*, McGrawHill, España, 2004.

[11] C. J. Mitchell, F. C. Piper, *A Classification of Time Element Speech Scramblers*, Journal of the Institution of Electronic and Radio Engineers, pag. 391-396, 1985.

[12] L. S. Lee, G. S. Chou, C. S. Shang, *Frecuency or time domain speech scrambling technique and system which does not require any frame synchronization*, U.S. Patent 4591673, 1986.

[13] J. B. Tsui, Digital *Techniques for Wideband Receivers*, SciTech Publishing Inc., 2004.

[14] A. D. Wyner, *Analog Signal Scrambling System*, U.S. Patent 4379205, 1983.

[15] S. Lederman, *Speech Signal Scrambler*, U.S. Patent 4156107, 1979.

[16] E. B. Albertí, *Señales y Sistemas de Tiempos Discreto*, UPC, primera edición, 2003.

[17] J. R. Deller, J. H. L. Hansen, J. G. Proakis, *Discrete-Time Processing of Speech Signals*, Macmillan Publishing Co., 2000.

[18] A. Matsunaga, *Speech Scrambler*, U.S. Patent 4747137, 1988.

[19] J. R. Whitten, *Speech Scrambler*, U.S. Patent 4099027, 1978.

[20] H. N. Switsen, *Simple Speech Scrambler*, U.S. Patent 3740477, 1973.

[21] M. S. Ibañez, R. G. Diaz, *Generación y analisis de secuencias pseudoaleatorias*, Ediciones de la universidad Politecnica de Catalunya SL, Epaña, 1999.

[22] L. R. Rabiner, R. W. Schafer, *Digital Processing of Speech Signals*, Prentice-Hall Signal Processing Series, 1978.

[23] U. Zölzer, *Digital Audio Signal Processing*, Jhon Wiley & Son Ltd., 2008.

[24] A. Antoniou, *On the roots of Digital signal processing*, IEEE Circuits and Systems Magazine, pag.8-19, 2007.

[25] J. G. Proakis, D. G. Manolakis, *Digital Signal Processing, Principles, Algorithms and Applications*, Prentice-Hall, International, Inc, 1996.

[26] Ch. S. Lessard, *Signal Processing of Random Physiological Signals*, Morgan & Claypool, 2006.

[27] G. James, *Matemática Avanzada para ingeniería*, Prentice-Hall, Segunda edición, 2010.

[28] R. G. Lyons, *Understanding Digital Signal Processing*, Prentice Hall PTR, 2001.

[29] S. W. Smith, *The Scientist and Engineer's Guide to DIGITAL SIGNAL PROCESSING*, California Techical Publishing, 1999.

[30] S. K. Mitra, *Digital Signal Processing: a Computer-Based Approach*, McGraw-Hill College, 2003.

ANEXO 1

Referido de la *Revista "Seguridad en Informática y Comunicaciones"*

Aplicación de equipos según Clientes

Usuario	Aplicación	Nivel de Seguridad	Protección
Gobierno	Sensitiva y Clasificada	VoSec	Adversarios Sofisticados
Gobierno	Sensitiva, pero no clasificada	DES	Adversarios Sofisticados
El Ejército	Protección	460	Terroristas Criminales
Policía Nacional	Vigilancia de Seguridad		Terroristas Política
Policía	Fuerzas Antidrogas, Fuerzas de la Ley, Vigilancia, Negociación de Rehenes		Criminal
Policía, Bomberos, Ambulancias, Carceles	Desastres, Accidentes, Disturbios, Vigilancia	430	Prensa, Competencia Técnico
Comercial	Negocios, Exploración Minera, Disputas Laborales	410/416	Competencia no autorizada
Seguridad Pública	Población General		Scanners
Comercial	General	400	Empleados

ANEXO 2

IMAGEN	MODELO	COSTO	DESCRIPCION
	TK3170K*A	$ 327.00	Radio Portátil UHF Scrambler de, 450-490 MHz,
	**TK2170K**	$ 639.00	Radio Portátil VHF Scrambler de, 136-174 MHz
	**TK2170KIS**	$ 769.00	Radio Portátil VHF Scrambler de, 136-174 MHz
	**TK3170K**	$ 649.00	Radio Portátil UHF Scrambler de, 450-490 MHz,
	**TK3173KIS**	$ 829.00	Radio Portátil Troncal LTR Scrambler de, 450-490 MHz
	**TK8360HK*A**	$ 396.00	Radio Móvil Scrambler de 450-520 MHz
	**FSU1083**	$ 0.50	TARJETA D/SCRAMBLER P/FTH2070
	**VPU11*A**	$ 5.00	CODIFICADOR /DECOFICADOR D/VOZ POR INVERSIÓN (SCRAMBLER)
	**MOT-VPU-15-C**	$ 224.00	Inversión Scrambler de voz para radios Motorola Serie Comercial

ANEXO 3

CODIFICACION DE LA SEÑAL

```
%*****************************************************************

fs=8000;                    %Frecuencia de muestreo en Hz.
Tamano=512;
clave={5 3 1 4 2}';         %Determina la secuencia de envió
seg=1.92;

%*****************************************************************

%Funcion que permite calcular TONOS fácilmente manipulables
[BufferTotales_Tonos] = Calculo_Tonos2(Tamano, seg);
X=BufferTotales_Tonos;

%*****************************************************************

%SEÑAL ARTIFICIAL
%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=400;  %En Hertz
freq2=1500;  %En Hertz
freq3=3200; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{1,1}=BufferTotal_Synthetic;

%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=500;  %En Hertz
freq2=1600;  %En Hertz
freq3=3300; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{2,1}=BufferTotal_Synthetic;

%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=600;  %En Hertz
freq2=1700;  %En Hertz
freq3=3400; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{3,1}=BufferTotal_Synthetic;

%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=700;  %En Hertz
freq2=1800;  %En Hertz
freq3=3500; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{4,1}=BufferTotal_Synthetic;
```

```
%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=800;  %En Hertz
freq2=1900;  %En Hertz
freq3=3600; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{5,1}=BufferTotal_Synthetic;

%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=900;  %En Hertz
freq2=2000;  %En Hertz
freq3=3700; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{6,1}=BufferTotal_Synthetic;

%Funcion que permite calcular LA VOZ SINTETICA fácilmente
manipulables
freq1=1000;  %En Hertz
freq2=2100;  %En Hertz
freq3=3800; %En Hertz
fase=pi/4;  %Angulo de Fase
[BufferTotal_Synthetic] = Calculo_Voz_Sintetica(Tamano, freq1,
freq2, freq3, fase, seg);
X_temp{7,1}=BufferTotal_Synthetic;

[X] = One_Funtion(X_temp);

%*****************************************************************

fs=8000;                    %Frecuencia de muestreo en Hz.
Tamano=512;
seg=1.92;

tmp = Escucha_Archivo(fs);

Y = tmp(1:512*floor(length(tmp)/512));
X=Y;

%*****************************************************************

%INICIALIZANDO VALORES
Tamm=51;
despla=0;
Voice_Codificatedd=1;
N=size(X,1);              %N debe ser multiplo de 512
Cell_Tam_Subbuffer{1,1}=1;

for K=1:N/512
    Buffer= X(512*(K-1)+1:512*K);
    c1=randperm(5);
    clave = {c1(1) c1(2) c1(3) c1(4) c1(5)}';
    SClave(:, K) = c1(:)';

%*****************************************************************
```

```
%Calcula Transformada de Fourier
BufferTotal_Synthetic=Buffer;
[Frec, Positions_Save] = Fourier_Permuta(BufferTotal_Synthetic);

%*****************************************************************

%PRUEBA
%for Cuenta=1:512
    %Frec(Cuenta,1)=Cuenta;
%end

%*****************************************************************

%Función que permuta los Sub-bufers
Tamm=51;
[Buffer_Tx, Cell_Tam_Subbuffer] = Permutacion(Frec, Tamm,
Cell_Tam_Subbuffer, clave, Positions_Save);

%*****************************************************************

%Calcula Transformada Inversa de Fourier
[Voice_Codificated] = Inversa_Fourier_Permuta(Buffer_Tx);
Voice_Codificated=Voice_Codificated(:);

COD(512*(K-1)+1:512*K) = Voice_Codificated;

[Voice_Codificatedd, despla] =
One_Data5(Voice_Codificated,Voice_Codificatedd, despla);
end

%*****************************************************************

Y=Voice_Codificatedd;    %Permite escuchar la Voz Codificada
Escucha_Voz(Y, fs)

%Graba la Voz Codificada
Graba_Archivo(fs, Voice_Codificatedd);


%Graficas de las señales
%BufferTotal_Synthetic=X;
%Graficas_Tx(Voice_Codificated, BufferTotal_Synthetic, seg);

%Grafica del Espectrograma
%[Similarity_COD] = Resultados_Experimentales_COD(Voice_Codificated,
BufferTotal_Synthetic, fs);
```

DECODIFICACION DE LA SEÑAL

```
%*****************************************************************

fs=8000;                    %Frecuencia de muestreo en Hz.
despla=0;
Voice_Codificatedd_Dec=1;
%Tamano=512;
%clave={4 1 3 5 2}';        %Determina la secuencia de envió
%seg=1.92;

for K=1:N/512
    c1 = SClave(:, K);
    clave = {c1(1) c1(2) c1(3) c1(4) c1(5)}';

    Voice_Codificated = COD(512*(K-1)+1:512*K);

Buffer_Dec=Voice_Codificated(:);

%*****************************************************************

%Función que devuelve la Transformada de Fourier.
Buffer_Time_Dec=Voice_Codificated;
[Buffer_Organized_Dec, Data_Positions_Dec] =
Voice_Rx5(Buffer_Time_Dec);
 Buffer_Organized_Dec=Buffer_Organized_Dec(:);

%*****************************************************************

%Función que permuta de forma Inversa
[Buffer_Rx] = Permuta_Inversa(Buffer_Organized_Dec,
Cell_Tam_Subbuffer, Data_Positions_Dec, clave);

%*****************************************************************

%Función que devuelve la transformada inversa de Fourier.
[Senal_Recuperada] = Inversa_Frecuency(Buffer_Rx);

SREC(512*(K-1)+1:512*K) = Senal_Recuperada(:);

[Voice_Codificatedd_Dec, despla] = One_Data_Dec3(Senal_Recuperada,
Voice_Codificatedd_Dec, despla);

end

%*****************************************************************

Y=Voice_Codificatedd_Dec;          %Permite escuchar la Voz
Codificada
Escucha_Voz(Y, fs)

%Graba la Voz DecCodificada
Voice_Codificatedd=Voice_Codificatedd_Dec;
Graba_Archivo_Dec(fs, Voice_Codificatedd);

%Distancia Euclidiana
[Similarity_DEC] = Resultados_Experimentales_DEC(Senal_Recuperada,
BufferTotal_Synthetic);
```

```
%[Similarity_DEC] = Resultados_Experimentales_DEC(SREC, COD, fs);

figure; spectrogram(X, 512, 256, 8000, 'yaxis');
title('Señal Original');
xlabel('Tiempo de Muestreo (Seg)');
%ylabel('Frecuencia (Hz)');

figure; spectrogram(COD, 512, 256, 8000, 'yaxis');
title('Señal Codificada');
xlabel('Tiempo de Muestreo (Seg)');
%ylabel('Frecuencia (Hz)');

figure; spectrogram(SREC, 512, 256, 8000, 'yaxis');
title('Señal Recuperada');
xlabel('Tiempo de Muestreo (Seg)');
%ylabel('Frecuencia (Hz)');

figure; plot( abs(X(:) - SREC(:))); title(' |Señal Original - Señal
Recuperada|');
xlabel('Tiempo (Seg.)')
                        ylabel('Amplitud')
```