UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA

PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Simulación de técnicas de enmascaramiento de voz en el dominio de la frecuencia usando MatLab/Simulink

AUTOR:

Jiménez Muñoz, Washington Isaac

Componente práctico del examen complexivo previo a la obtención del grado de **INGENIERO EN TELECOMUNICACIONES**

REVISOR:

Palacios Meléndez, Edwin Fernando

Guayaquil, Ecuador

09 de Septiembre del 2016

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente **componente práctico del examen complexivo**, fue realizado en su totalidad por **Jiménez Muñoz, Washington Isaac** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

REVISOR

_____

Palacios Meléndez, Edwin Fernando

DIRECTOR DE CARRERA

_____

Heras Sánchez, Miguel Armando

Guayaquil, a los 09 del mes de Septiembre del año 2016

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Jiménez Muñoz, Washington Isaac**

DECLARÓ QUE:

El **componente práctico del examen complexivo, Simulación de técnicas de enmascaramiento de voz en el dominio de la frecuencia usando MatLab/Simulink** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 09 del mes de Septiembre del año 2016

EL AUTOR

_____

JIMÉNEZ MUÑOZ, WASHINGTON ISAAC

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Jiménez Muñoz Washington Isaac**

Autorizó a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del **componente práctico del examen complexivo, Simulación de técnicas de enmascaramiento de voz en el dominio de la frecuencia usando MatLab/Simulink**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

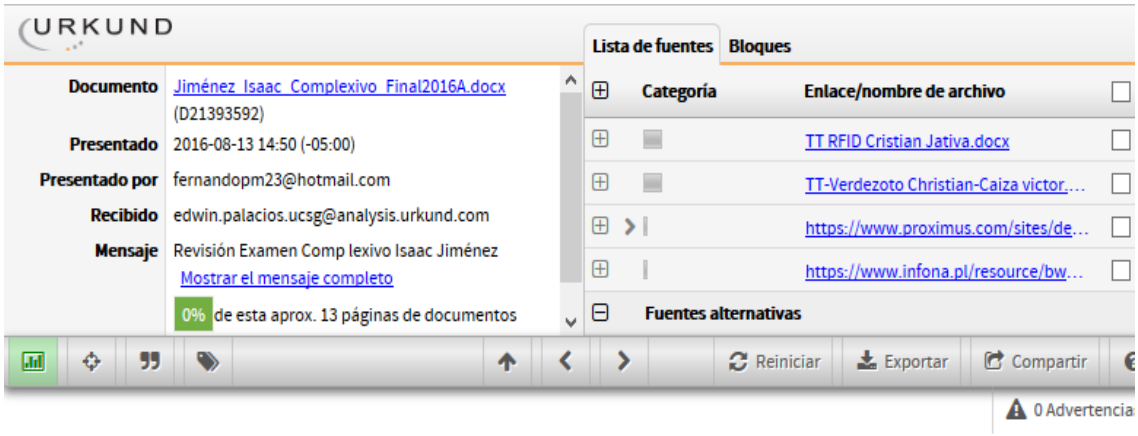
Guayaquil, a los 09 del mes de Septiembre del año 2016

EL AUTOR

_____

JIMÉNEZ MUÑOZ, WASHINGTON ISAAC

REPORTE DE URKUND



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA

DE INGENIERÍA EN TELECOMUNICACIONES TEMA:

Simulación de técnicas de enmascaramiento de voz en el dominio de la frecuencia usando MatLab/Simulink AUTOR: Jiménez Muñoz Washington Isaac Componente práctico del examen complexivo

previo a la obtención del grado de INGENIERO EN TELECOMUNICACIONES REVISOR: Palacios Meléndez, Edwin Fernando Guayaquil, Ecuador 02 de Septiembre del 2016

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA

DEDICATORIA

Este trabajo de titulación va dedicado para mi esposa, Sandra Sosa Calero y a mi hijo Isaac Jiménez Sosa, que gracias a su paciencia he logrado culminar un objetivo planteado en el 2010 cuando ingrese a la Facultad de Educación Técnica para el Desarrollo en la Carrera de Ingeniería en Telecomunicaciones.

A mis padres, Washington Jiménez Montalván y Elena Muñoz Burgos que con su contribución permitieron que siga el rumbo para lograr la tan anhelada meta, el ser Ingeniero en Telecomunicaciones.

A mis suegros, Alfredo Sosa y Carmen Calero, ya que han sabido apoyarme como otro hijo más y brindarnos su respaldo para culminar la carrera.

A los Directivos, Docentes y empleados administrativos de la Facultad de Educación Técnica para el Desarrollo por brindar siempre su apoyo en cada una de las gestiones que realice.

EL AUTOR

JIMÉNEZ MUÑOZ, WASHINGTON ISAAC

AGRADECIMIENTO

En primer lugar, mi agradecimiento a Dios, ya que su ayuda espiritual permitió que continúe y desmaye durante estos 6 años que estudie Ingeniería en Telecomunicaciones.

A la Universidad Católica de Santiago de Guayaquil, a mi querida Facultad de Educación Técnica para el Desarrollo, al Decano Ing. Manuel Romero Paz, al Director de Carrera, Ing. Armando Heras Sánchez y a todos los docentes que me enseñaron durante estos años y que aprendí su humildad.

A mi familia, familiares, amigos y en especial al M. Sc. Fernando Palacios Meléndez, que sin su ayuda durante estas dieciséis semanas no hubiese sido posible culminar el trabajo de titulación modalidad examen complexivo.

EL AUTOR

JIMÉNEZ MUÑOZ, WASHINGTON ISAAC

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f._____

LUIS SILVIO CORDOVA RIVADENEIRA
REVISOR

f._____

MANUEL DE JESUS ROMERO PAZ
DECANO

f._____

EDWIN FERNANDO PALACIOS MELÉNDEZ
COORDINADOR DE TITULACIÓN

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2:

Capítulo 3:

ÍNDICE DE TABLAS

Capítulo 3:

RESUMEN

Los métodos de adquisición y manipulación de información de manera no autorizada han evolucionado mucho en los últimos años por lo que se hace imprescindible conocer y estudiar sistemas que permitan que la información viaje de manera segura a través de canales no seguros. En nuestro trabajo nos enfocaremos en las comunicaciones telefónicas donde la información es la voz del interlocutor y estudiaremos los métodos de enmascaramiento de voz en el dominio de la frecuencia, de los cuales implementaremos en Matlab Simulink el enmascaramiento por inversión de frecuencia y el enmascaramiento por división de banda. En la simulación fueron utilizadas herramientas virtuales con las cuales se puede observar la señal original, la señal ya enmascarada en el canal y la señal desenmascarada en el receptor y se puede constatar de manera visible que el mensaje recuperado es totalmente entendible a la salida del receptor, pero no lo es en el canal de comunicaciones.

Palabras claves: ADQUISICIÓN, COMUNICACIONES TELEFÓNICAS, ENMASCARAMIENTO, VOZ, INVERSIÓN DE FRECUENCIA, DIVISIÓN DE BANDA

CAPÍTULO 1: Descripción básica del Componente Práctico.

1.1. Introducción.

Las comunicaciones seguras han sido siempre cruciales en los sistemas de comunicación comercial, civil y sobre todo en los militares, así como un área de interés y de investigación para científicos e ingenieros. Las amenazas a las comunicaciones han existido desde que el hombre comenzó a intercambiar mensajes, tales como: sistemas de escucha oculta, modificación, rechazo, repetición, repudio, etc.

Los medios y métodos para lograr que estas amenazas sean efectivas han dado lugar al desarrollo de técnicas muy complejas. En presencia de estos esquemas sofisticados se ha incrementado significativamente la gravedad de la inseguridad en las comunicaciones por lo que estos sistemas son más vulnerables que nunca (Jameel, Siyal, & Ahmed, 2007).

Para contrarrestar estas técnicas, la criptografía, que es la ciencia de las comunicaciones seguras, evalúa la seguridad de estos sistemas sobre la base de cuatro indicadores: autenticidad, confidencialidad, integridad y disponibilidad (Sutton, 2002). El enmascaramiento de la voz como parte integrante de la criptografía ha desempeñado un papel fundamental en las comunicaciones seguras. El término “scrambling” (en lo adelante enmascaramiento) se ha utilizado para describir los procesos de encriptado destinados a proteger las comunicaciones verbales tanto si se encuentran en

forma digital o analógica. Esta operación puede efectuarse en el dominio de la frecuencia, en el dominio del tiempo y en ambos (una combinación de estos) (Beker & Piper, 1985).

El nivel de seguridad de estos sistemas se determina por el grado de inteligibilidad residual de la señal enmascarada. Mientras menor sea el grado de inteligibilidad residual mayor será el grado de seguridad y viceversa. En el proceso de las comunicaciones, la calidad de la voz recuperada es también de gran importancia por lo que no puede ser ignorada a la hora de implementar un diseño de este tipo de sistema. Por eso a la hora de diseñar un sistema seguro de comunicaciones, la calidad de la voz recuperada constituye uno de los indicadores fundamentales en los criterios de diseño.

1.2. Objetivo General.

Investigar los principales aspectos teóricos y técnicos de las técnicas de enmascaramiento de voz en el dominio de la frecuencia y la simulación de 2 de estos sistemas.

1.3. Objetivos Específicos.

- ✓ Realizar una búsqueda bibliográfica, procesamiento detallado y asimilación de la información de las técnicas de enmascaramiento de voz en el dominio de la frecuencia.

- ✓ Diseñar y simular 2 técnicas de enmascaramiento de voz teniendo en cuenta los parámetros fundamentales que influyen para su funcionamiento y evaluación de los resultados.

CAPÍTULO 2: Fundamentación Teórica.

Los sistemas de comunicaciones son cada vez más atacados. A lo largo de la historia la seguridad y la comunicación privada han sido de vital importancia para las comunicaciones. En este capítulo se hace una introducción a los tipos de enmascaramiento de voz que existen, además de una descripción de las técnicas empleadas para proteger las comunicaciones de la voz en el dominio de la frecuencia.

2.1 Introducción a la Criptografía.

La palabra criptografía, procedente del griego, significa escritura secreta, es el arte y la ciencia de darle seguridad a los mensajes y la realizan los criptógrafos. Los cripto-analistas son especialistas del criptoanálisis, el arte y la ciencia de descubrir un texto cifrado. La rama de la matemática que se ocupa de la criptografía y del criptoanálisis se denomina criptología y a los que la practican se les llaman criptólogos.

La criptografía permite la transmisión segura de información privada mediante canales inseguros. Existen métodos para minimizar el acceso y el ataque por personas no autorizadas a sistemas seguros de comunicaciones (Jameel et al., 2007). En la figura 2.1 (a) se muestra el flujo normal de la información del transmisor al receptor, no obstante, este inevitablemente puede ser atacado y violado por cualquier medio en cualquier momento, dejando al sistema indefenso.

Existen cuatro métodos principales mediante el cual un intruso puede atacar o amenazar cualquier sistema (Beker & Piper, 1985). Una vía posible puede ser interrumpir la información que ha salido del transmisor de forma que no llegue al receptor como se muestra en la figura 2.1 b, este es un ataque a la información transmitida.

Por otra parte, si la información trasmitida es recibida por el receptor y al mismo tiempo recibida por una persona no autorizada, se está en presencia de una violación de la confidencialidad de datos, siendo un punto débil en la seguridad como se muestra en la figura 2.1 (c). En caso de que la información sea captada por el enemigo, modificada y posteriormente retransmitida al receptor, esto constituiría un ataque a la integridad de la información como se muestra en la figura 2.1 (d).

Finalmente, si cualquier persona no autorizada envía información falsa, entonces será un ataque a la autenticidad como se muestra en la figura 2.1 (e) (Sutton, 2002). Basadas en las características de estos cuatro ataques, la criptografía clasifica la seguridad de un sistema seguro en cuatro tipos:

- ✓ Interrupción (ataque a la disponibilidad).
- ✓ Intercepción (ataque a la confidencialidad).
- ✓ Modificación (ataque a la integridad).
- ✓ Falsificación (ataque a la autenticidad).

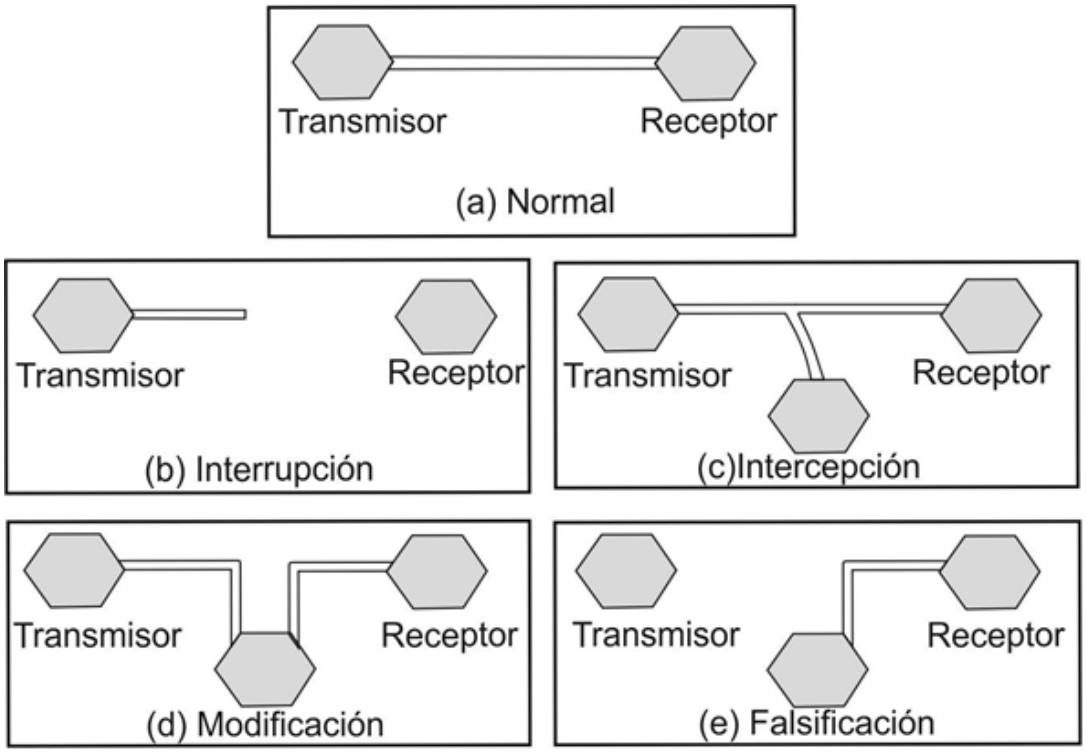


Figura 2. 1: Amenazas a la seguridad en los sistemas de comunicaciones
Elaborado por: Autor

2.2 Enmascaramiento de voz.

El enmascaramiento y desenmascaramiento de la voz ha sido siempre una pieza clave en los sistemas seguros de comunicación. Las técnicas utilizadas en este ámbito están directa o indirectamente relacionadas con el campo de la criptografía, algunos autores la denominan criptografía de voz (Goldburg & Sridharan, 1993).

El enmascaramiento describe los procesos de cifrado que hacen segura la comunicación de la voz por métodos analógicos o digitales; es la técnica que proporciona seguridad de la voz y que se logra mezclando los contenidos de la señal de voz original de una manera determinada antes de la transmisión de forma que apenas sea entendible para el interceptor.

Para que la voz sea segura, su estructura debe ser modificada por un proceso que garantice que cuando ese mismo mensaje sea escuchado nuevamente sea ininteligible al interceptor. El objetivo fundamental del enmascaramiento es lograr poca o ninguna inteligibilidad para el intruso y al mismo tiempo lograr que sea perfectamente comprensible para el receptor (Jameel et al., 2007).

Al diseñar un enmascarador de voz eficiente, hay que reducir al mínimo la correlación entre tres parámetros: tiempo, frecuencia y amplitud. Si sólo uno de estos parámetros es modificado se le denomina enmascaramiento de una sola dimensión; correspondientemente cuando se modifican dos o tres parámetros, se le llama enmascaramiento bidimensional o tridimensional, respectivamente (Nichols & Lekkas, 2002).

Se puede decir que el enmascaramiento ha sido satisfactorio cuando un número suficiente de usuarios pueden comprender el mensaje recibido, pero no el mensaje transmitido. También es deseable que el ancho de banda del sistema no sea mayor que el de la señal. Si el ancho de banda del sistema es demasiado grande, puede aceptar más ruido del necesario y esto por consiguiente va a reducir la relación señal a ruido (Beker & Piper, 1985).

Por esto los especialistas recomiendan que el ancho de banda del sistema y el de la señal sea el mismo. Una excepción es la utilización de las técnicas de espectro ensanchado donde la señal ensanchada ocupa un

ancho de banda mayor que el mínimo necesario (que exige el método de modulación) para enviar la información. El enmascaramiento de la voz puede ser tanto analógico como digital.

2.2.1. Enmascaramiento de voz analógica.

En este caso tanto la señal de entrada como la de la salida son analógicas, sin embargo, el procesamiento completo se efectúa digitalmente. La señal de entrada es digitalizada, pasa por un proceso algorítmico y se enmascara, se convierte en analógica y entonces se transmite al receptor. En el receptor la señal se vuelve a digitalizar, procesándose inversamente y reconvirtiéndola en su forma analógica para su reconstrucción. En la figura 2.2 se muestra un diagrama esquemático de un codificador y un decodificador de voz analógica.

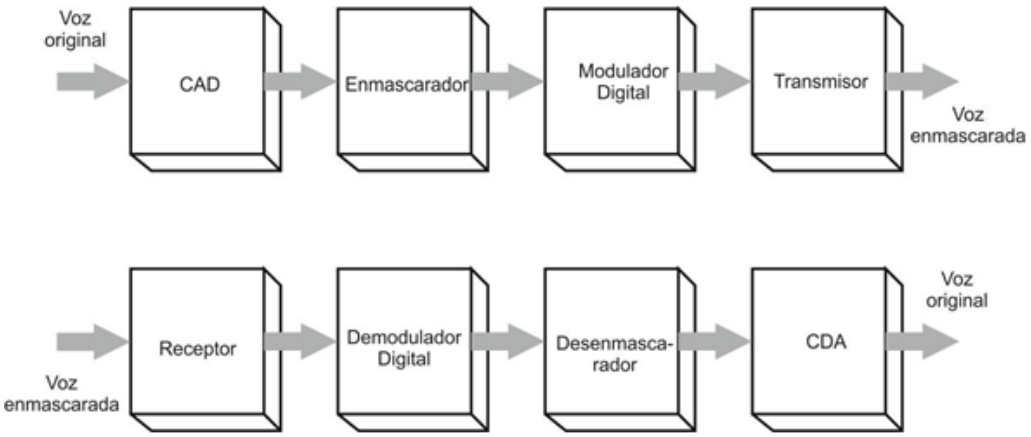


Figura 2. 2: Esquema de un enmascarador y un desenmascarador de voz analógica
Elaborado por: Autor

En el dominio analógico hay tres parámetros básicos de la señal de voz sobre los cuales el procesador opera para dale seguridad a esta: tiempo, frecuencia y amplitud. Existen enmascaradores dimensionales en el dominio

del tiempo, en el de la frecuencia e híbridos en el dominio del tiempo y en el de la frecuencia (Goldburg & Sridharan, 1993).

En general los enmascaradores no ocultan ni eliminan ninguna información de la voz, simplemente reordenan la información para crear una nueva señal con una relación unívoca con la original. Los enmascaradores analógicos son similares a los cifrados de transposición en texto, donde un bloque de valores de un parámetro se toma y se intercambia. Estos sistemas se clasifican como de banda estrecha y se pueden utilizar en un canal telefónico (Ahmed & Ikram, 2003).

2.2.2. Enmascaramiento de voz digital.

En el cifrado digital, la señal de voz se digitaliza y se comprime para lograr una señal con una baja tasa de bit. La técnica de cifrado se aplica por métodos de bloques de cifrado o métodos de flujos de cifrado. La secuencia cifrada se transmite a través de una modulación digital; en otras palabras, la señal de entrada y de salida son digitales. En la figura 2.3 se ilustra un diagrama esquemático de un enmascarador y un desenmascarador digital de voz.

La técnica digital usada para darle seguridad a la voz consiste en cifrar la voz utilizando una secuencia pseudoaleatoria. Los bits digitalizados de la voz se agregan a la secuencia pseudoaleatoria de manera similar al flujo cifrado para un texto (Jameel et al., 2007).

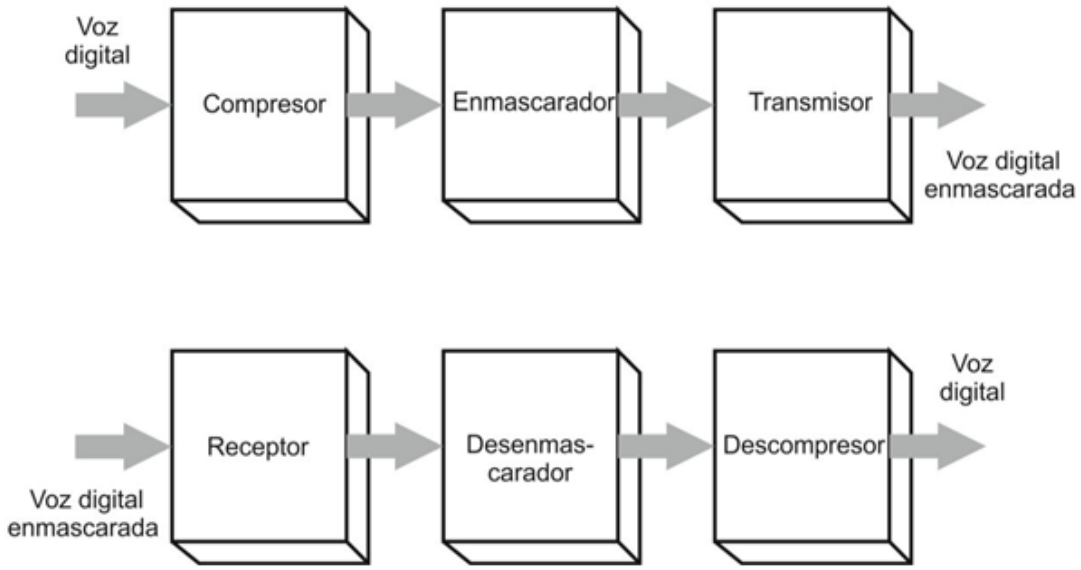


Figura 2. 3: Esquema de un enmascarador y un desenmascarador de voz digital
Elaborado por: Autor

2.3 Técnicas de enmascaramiento de voz.

Tomando en consideración las características antes mencionadas, las técnicas de enmascaramiento de voz se dividen en las siguientes categorías:

1-Enmascaramiento de voz en el dominio de la frecuencia.

2-Enmascaramiento de voz en el dominio del tiempo.

3-Enmascaramiento de voz en el dominio bidimensional.

4-Enmascaramiento de voz en el dominio de la transformada.

2.4 Técnicas de enmascaramiento de voz en el dominio de la frecuencia.

En estas técnicas la manipulación de la señal de voz se lleva a cabo con respecto a la componente de frecuencia. Las técnicas principalmente utilizadas en esta categoría son: inversión de frecuencia, inversión por salto de frecuencia, inversión por desplazamiento de banda, salto de frecuencia

aleatoria y división de banda. A continuación, se definen cada una de estas categorías.

2.4.1. Inversión de frecuencia.

El esquema de inversión de frecuencia simplemente invierte las componentes de frecuencia de la señal de voz, de modo que las bajas frecuencias son desplazadas hacia las componentes de altas frecuencias y las altas frecuencias son desplazadas hacia las componentes de bajas frecuencias.

El sistema toma una gama de la señal de audio que va de 300 Hz a 3,3 kHz y en este caso la inversión de frecuencia se logra multiplicando (modulando) la entrada de audio con la portadora Fp y luego se multiplica de nuevo (demodula) utilizando como portadora una señal de Fp + 3300 Hz, lo que origina un cambio del espectro de frecuencia con las bandas laterales, superiores e inferiores.

En la banda lateral inferior que representa el rango de voz audible, los tonos inferiores son tonos superiores y viceversa. En las figuras 2.4 (a) y (b) se representa la técnica en el dominio de la frecuencia.

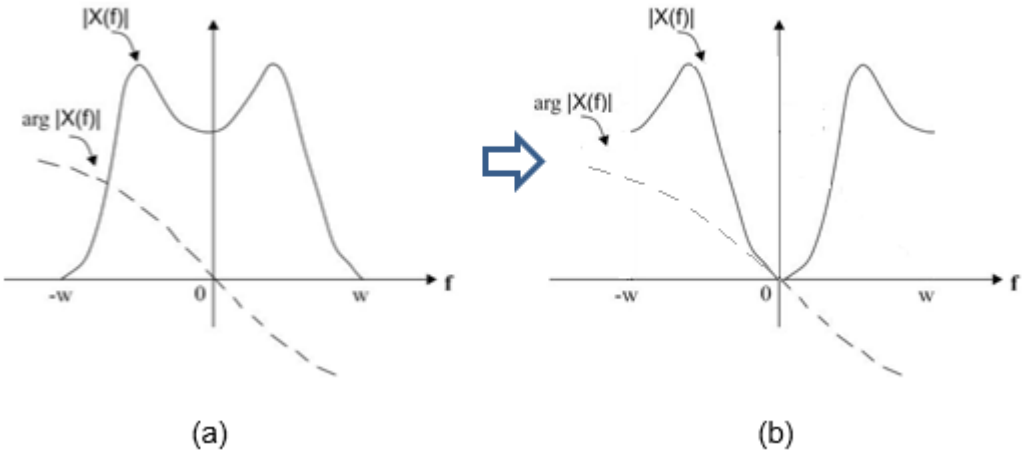


Figura 2. 4: (a) Señal del mensaje (b) Señal enmascarada usando la técnica de enmascaramiento por inversión de frecuencia.
Elaborado por: Autor

2.4.2. Inversión por salto de frecuencia e inversión de desplazamiento de banda.

El esquema de inversión de desplazamiento de banda se basa en el concepto de inversión de frecuencia, pero con el objetivo de aumentar el nivel de seguridad se introduce una clave que el usuario puede variar a voluntad. Existe otra técnica, la inversión por salto de frecuencia que es muy similar a la técnica inversión de desplazamiento de banda, esta utiliza un conjunto de varias frecuencias portadoras. En ambas se cambia la frecuencia pseudoaleatoriamente, con lo que se alcanza un alto grado de seguridad (Ahmed & Ikram, 2003).

Un nivel más alto de seguridad se obtiene cambiando continuamente la frecuencia de inversión, por lo que exige cambiar esta en una secuencia predefinida. Para hacer esto se necesita que los dispositivos transmisores y receptores cambien la frecuencia de inversión. Tanto el transmisor como el

receptor conocen la secuencia de saltos, así como los enmascaradores a cuál frecuencia saltar. Sin embargo, esta técnica requiere que tanto transmisor como receptor estén sincronizados para que ambos puedan empezar la secuencia al mismo tiempo (Beker & Piper, 1985).

Esta técnica tiene la desventaja que la sincronización puede perderse durante la transmisión y el receptor no puede recuperar exitosamente la señal. También la secuencia de saltos puede ser identificada como un patrón reconocible por cualquier intruso. El esquema de inversión por salto de frecuencia se muestra en la figura 2.5.

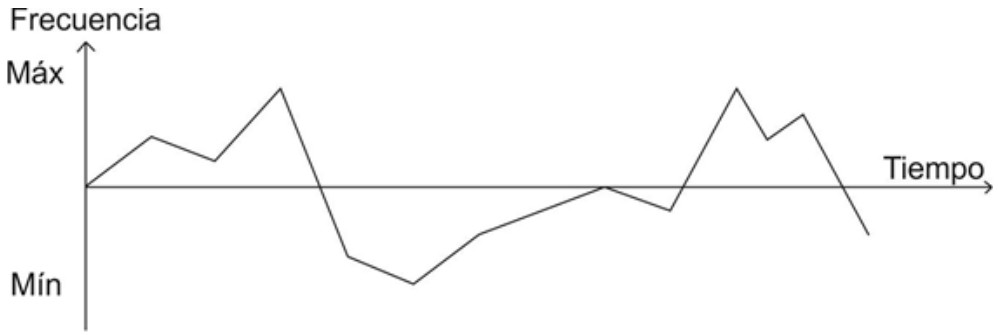


Figura 2. 5: Inversión por salto de frecuencia.
Elaborado por: Autor

2.4.3. Salto de frecuencia aleatoria.

En la técnica de salto de frecuencia aleatoria, la frecuencia con que se realiza esta inversión se mantiene constante. Cuando en estas inversiones, el cambio de frecuencias se realiza suficientemente rápido se tiene la impresión de que no hay discontinuidad. En la misma, la inversión de frecuencia se mantiene en dirección creciente hasta que alcanza el límite superior, a partir de este punto la inversión de frecuencia empieza a

disminuir hasta que llega al límite inferior. La salida resultante es una onda en forma de diente de sierra. Esta técnica es mucho más segura que las dos técnicas descritas anteriormente.

En esta técnica el transmisor selecciona aleatoriamente una frecuencia de inversión a saltos. Esta información tiene que ser enviada de alguna manera al receptor de una forma tal que sea descifrada por este. Esto se logra transmitiendo conjuntamente con la señal el código de la frecuencia seleccionada. El receptor separa este código y decodifica la señal.

En el caso de que la señal estuviera siendo escuchada por un intruso, no le sería posible descifrar la secuencia de salto dado que no existe una frecuencia específica de salto, ya que esta es aleatoria. Para que un tercero no autorizado pueda entender la señal, tendría que conocer como aislar el código y la frecuencia correspondiente a ese código (Jameel et al., 2007). En la figura 1.6 se muestra el esquema correspondiente.

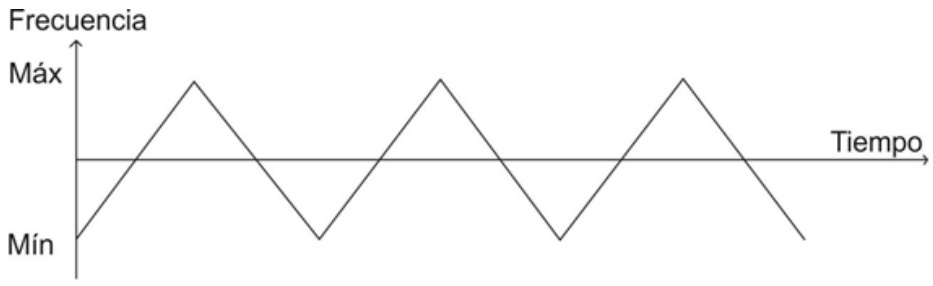


Figura 2. 6: Salto de frecuencia aleatoria.
Elaborado por: Autor

2.4.3.1. División de banda.

En esta técnica el espectro de la señal se divide en una cantidad determinada de sub-bandas como se muestra en la figura 2.7 (a) que posteriormente se van a mezclar, intercambiando su orden original. Para incrementar el orden de seguridad del sistema, algunas de estas sub-bandas pueden invertirse. En la figura 2.7 (a) se ilustra un ejemplo sencillo con 5 sub-bandas en las cuales se han desplazado todas las sub-bandas; mientras que en la figura 2.7 (b) las sub-bandas 2 y 5 no solamente han sido desplazadas, sino que también han sido invertidas.

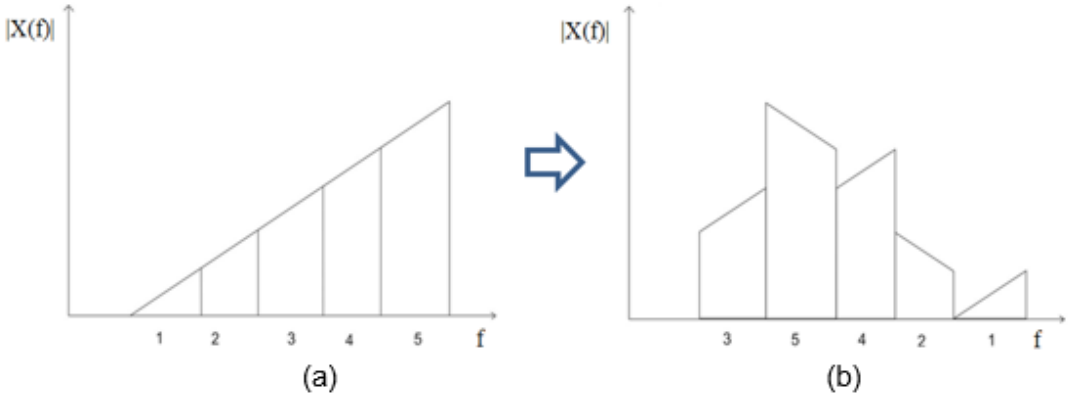


Figura 2. 7: (a) Señal del mensaje (b) Señal enmascarada usando la técnica de enmascaramiento por división de banda
Elaborado por: Autor

En términos de permutación, cuando se tienen 5 sub-bandas existen $5!$ posibles formas de reordenarlas y 25 formas de decidir cuál o cuáles sub-bandas se va a invertir. De esta manera hay $5! * 25 = 3840$ formas posibles de reordenar las sub-bandas. Desde el punto de vista matemático, si el espectro se divide en B sub-bandas, entonces el número de reordenamientos posibles de sub-bandas sería $B! * 2B$.

Después de haber analizado las técnicas de enmascaramiento de voz en el dominio de la frecuencia, en la Tabla 1.1 se ilustra una breve comparación de estas.

Tabla 2. 1: Comparación de las técnicas en el dominio de la frecuencia.

Técnicas de enmascaramiento en el dominio de la frecuencia	**Grado de Inteligibilidad residual**	**Calidad de la voz recuperada**	**Complejidad circuital**
Inversión de frecuencia	Alto	Buena	Menor
Inversión por salto de frecuencia	Medio	Media	Media
Inversión de desplazamiento de banda	Medio	Media	Media
División de banda	Bajo	Menor	Alta
Salto de frecuencia aleatoria	Bajo	Menor	Alta

Elaborado por: Autor

Puede apreciarse según la tabla anterior, el compromiso existente entre la seguridad (menor grado de inteligibilidad residual) y la calidad de la voz recuperada; mientras que con la construcción de circuitos más complejos se obtendrá una señal enmascarada más difícil de interpretar por una tercera no autorizada.

CAPÍTULO 3: Simulación de enmascaradores de voz.

En este capítulo se realizará la simulación de las técnicas de enmascaramiento de voz por inversión de frecuencia y por división de banda utilizando el software profesional Matlab Simulink (2014a). Los sistemas simulados fueron preparados para funcionar a través de una línea telefónica la cual según los estándares internacionales tiene un ancho de banda de 300 Hz a 3300 Hz.

3.1. Simulación de la técnica de enmascaramiento de voz por inversión de frecuencia.

La técnica de enmascaramiento por inversión de frecuencia consiste en invertir el espectro (como si de un espejo se tratara) de manera que las componentes frecuenciales que están en la parte alta del espectro se intercambien con las que están en la parte baja, esto queda ilustrado en la figura 3.1.

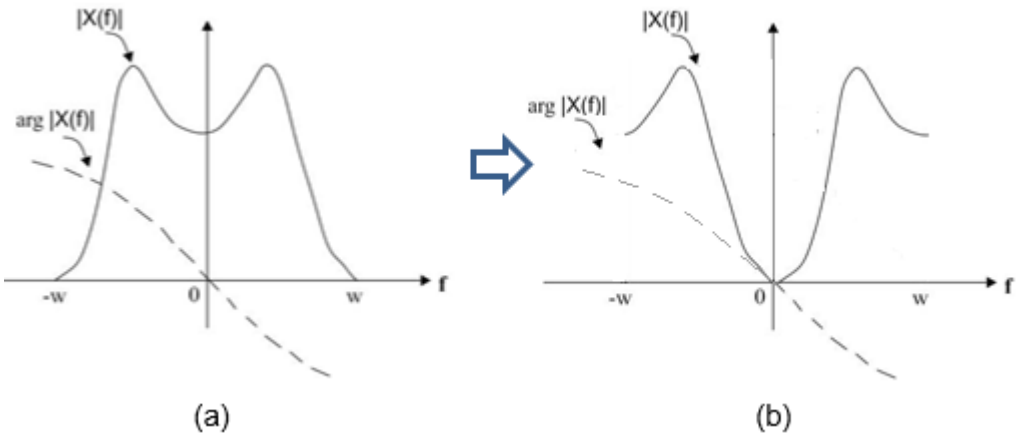


Figura 3. 1: (a) Señal del mensaje (b) Señal enmascarada usando la técnica de enmascaramiento por inversión de frecuencia.
Elaborado por: Autor

En este apartado se analizará la simulación de la técnica de enmascaramiento de voz por inversión de frecuencia. La figura 3.2 muestra el sistema desarrollado. Todos los bloques del sistema trabajan con una frecuencia de muestreo de 50 kHz, valor que garantiza el cumplimiento de la integridad de la señal en el sistema ya que como se verá ninguna de las operaciones realizadas están por encima de los 25 kHz, por lo que se cumple el criterio de Nyquist.

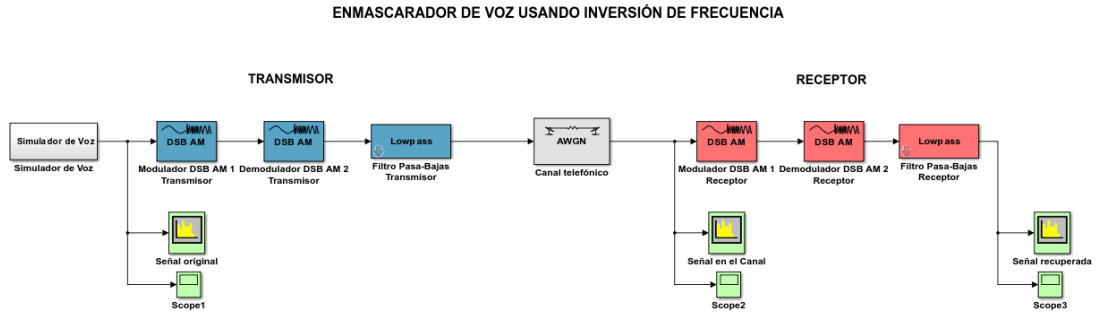


Figura 3. 2: Espectro de salida del LED.
Elaborado por: Autor

3.1.1. Transmisor.

En este sub-apartado analizaremos el transmisor del sistema que se muestra en la figura 3.3.

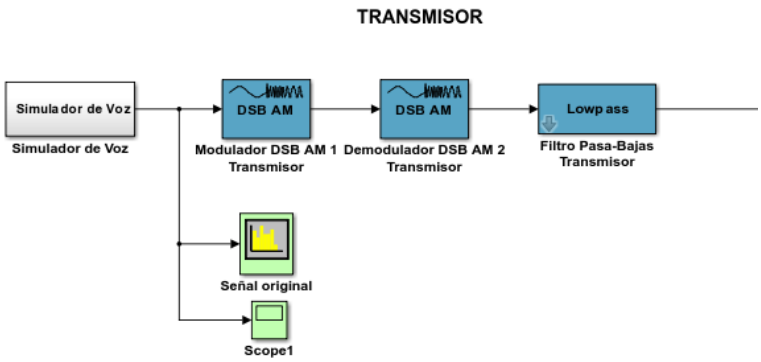
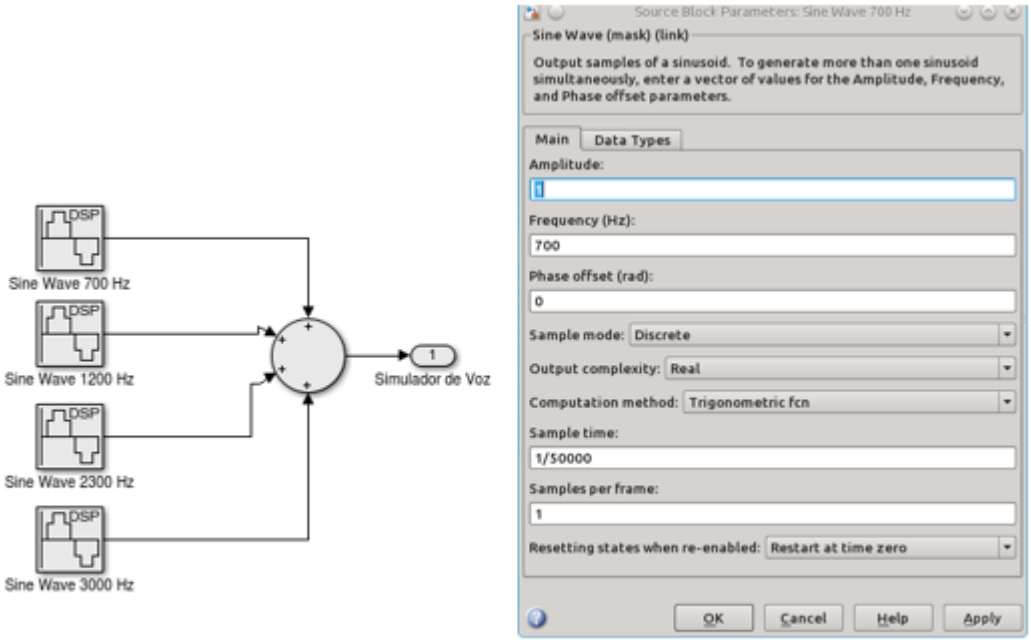


Figura 3. 3: Transmisor usado en la simulación de la técnica de enmascaramiento de voz por inversión de frecuencia.
Elaborado por: Autor

La voz es una señal aleatoria y compleja con la cual sería muy difícil mostrar los resultados del presente trabajo, por lo que para las simulaciones se utilizará un bloque predefinido llamado “Simulador de Voz” que en la salida retorna una señal multitono la cual llamaremos x(t), el interior del bloque es mostrado por la figura 3.4 (a). La señal multitono está formada por cuatro generadores de señales sinusoidales con frecuencias de 700 Hz, 1200 Hz, 2300 Hz y 3000 Hz, las amplitudes son 1, 0.1, 0.01, 0.001 respectivamente, las mismas son medidas en unidades arbitrarias (ua) del propio Matlab. La figura 3.4 (b) muestra como ejemplo la ventana de configuración del primer generado sinusoidal.



(a) (b)

Figura 3. 4: (a) Simulador de voz que genera una señal multitono. (b) Ejemplo la ventana de configuración del primer generado sinusoidal.
Elaborado por: Autor

Para lograr el efecto deseado de la inversión de frecuencia se utiliza un modulador de amplitud modulada (AM) del tipo doble banda lateral con

portadora suprimida (DBLPS) con una frecuencia portadora de 20 kHz y para demodular, se utiliza un demodulador de AM del tipo DBLPS fijando que la portadora en 20 kHz – 3.3 kHz esto permite que al demodular el espectro de la señal se encuentre centrado en 3.3 kHz. En la figura 3.5 se muestran los bloques del modulador y demodulador, así como las ventanas de configuración de los mismos.

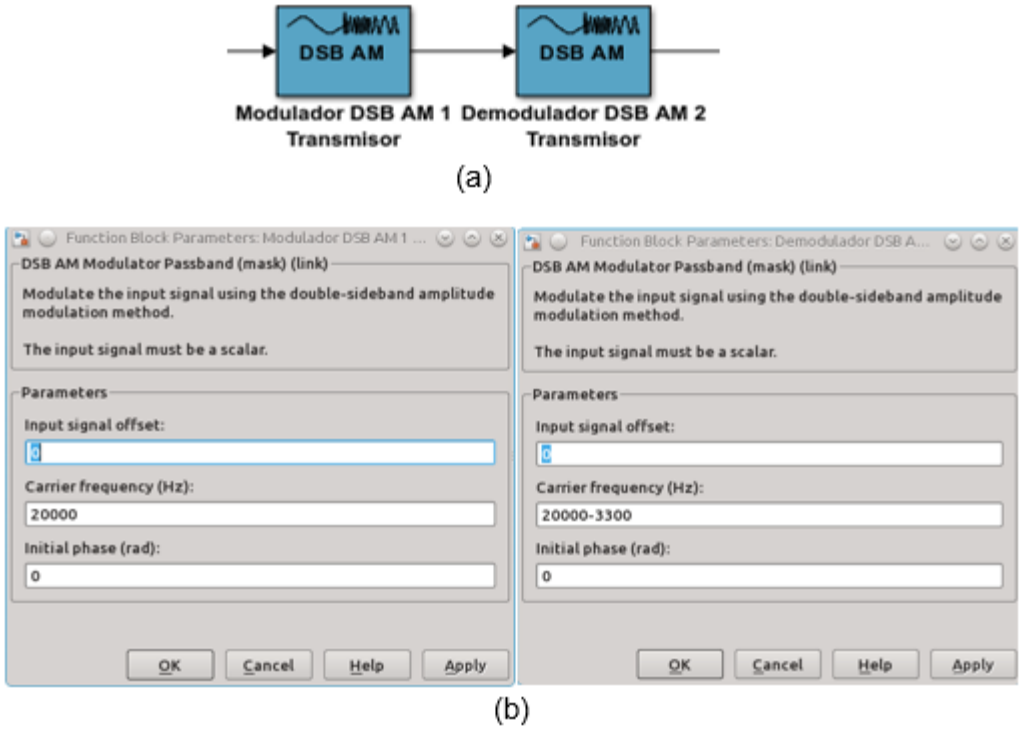
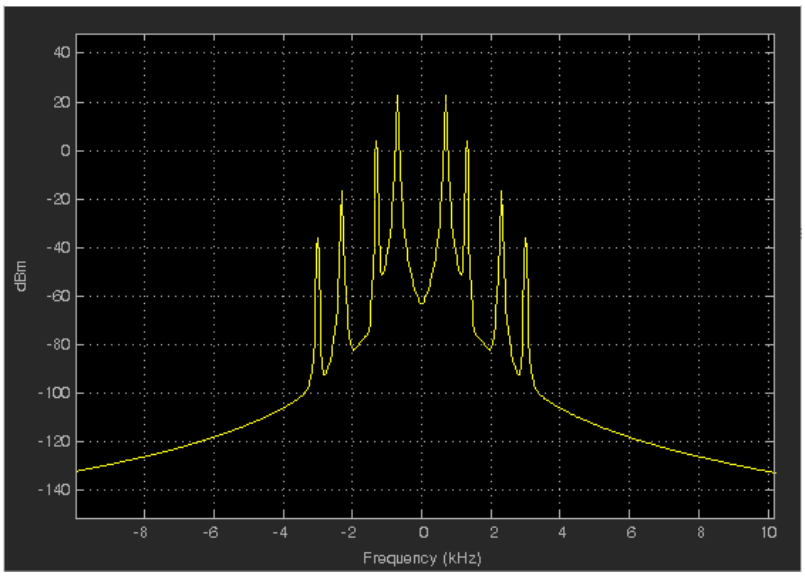


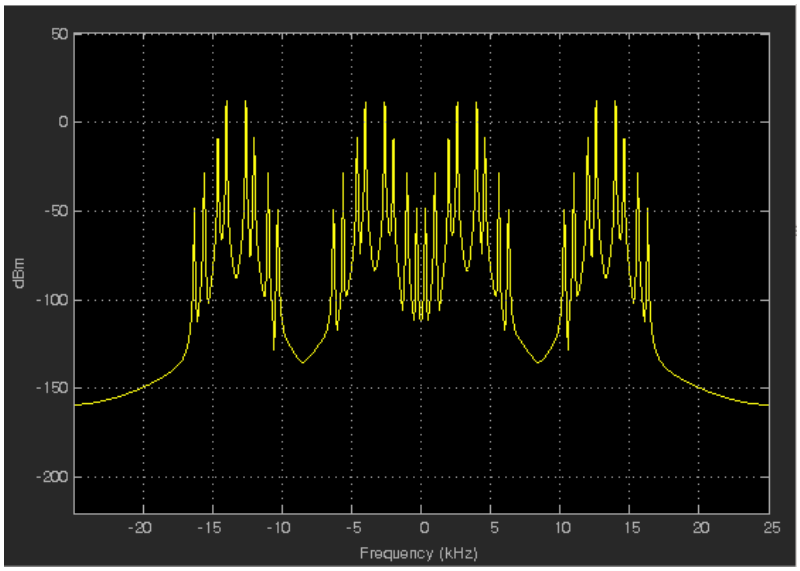
Figura 3. 5: (a) Bloques modulador y demodulador del trasmisor. (b) Ventanas de configuración del modulador (izquierda) y el demodulador (derecha).
Elaborado por: Autor

El efecto de inversión de frecuencia de la señal x(t) puede ser observado en la figura 3.6. En la figura 3.6 (b) se muestra la salida del demodulador, se puede apreciar que el espectro esta cuadruplicado ya que al pasar por el modulador se duplica y al pasar por el demodulador se vuelve a duplicar, pero en la banda de -3.3 kHz a 3.3 kHz se puede observar como

el espectro de la señal ya se encuentra invertido con respecto a la señal original.



(a)

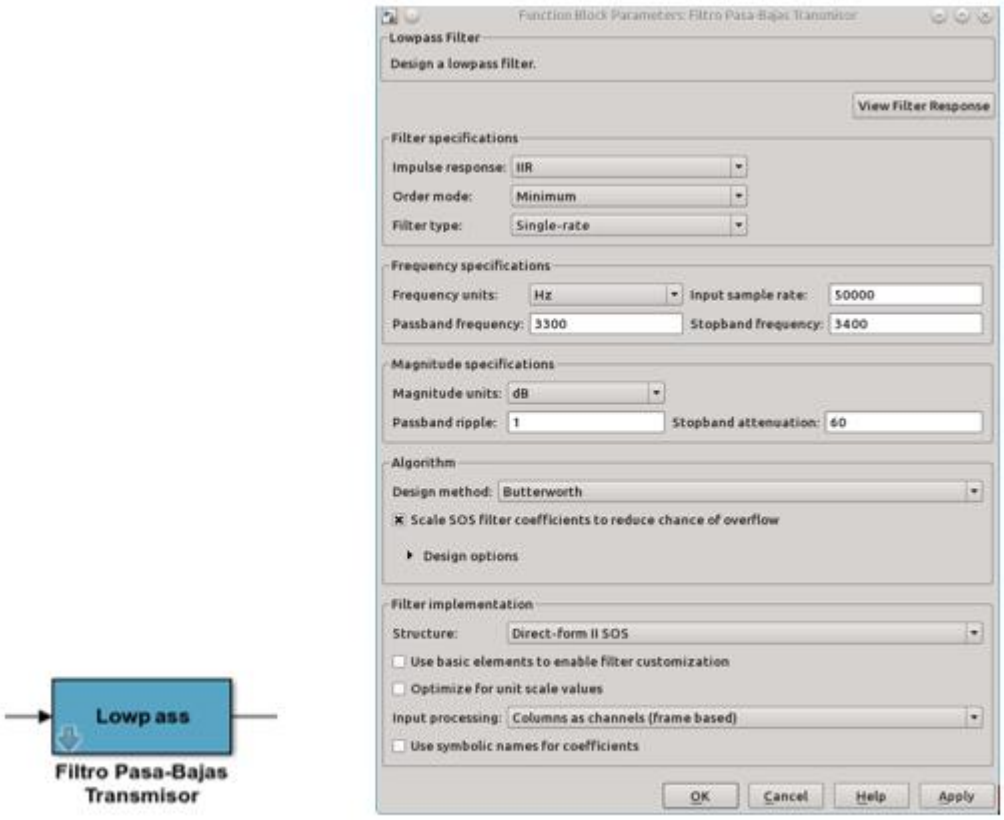


(b)

Figura 3. 6: (a) Espectro de amplitud de la señal original. (b) Espectro de amplitud de la señal a la salida del demodulador.
Elaborado por: Autor

Para la eliminación de las componentes frecuenciales que no son de nuestro interés utilizamos un filtro tipo IIR pasa bajas con una frecuencia de

corte de 3.3 kHz y frecuencia de muestreo de 50 kHz, los coeficientes del filtro son calculados por Matlab. En la figura 3.7 se muestra el bloque del filtro en el transmisor, así como la ventana de configuración del mismo.



(a) (b)

Figura 3. 7: (a) Bloque del filtro pasa bajas (b) Ventana de configuración del filtro pasa bajas.
Elaborado por: Autor

En la figura 3.8 puede observarse la señal a la salida del filtro pasa bajas en el transmisor, puede observarse como las componentes están invertidas con respecto a la señal original (véase la figura 3.6 (a)).

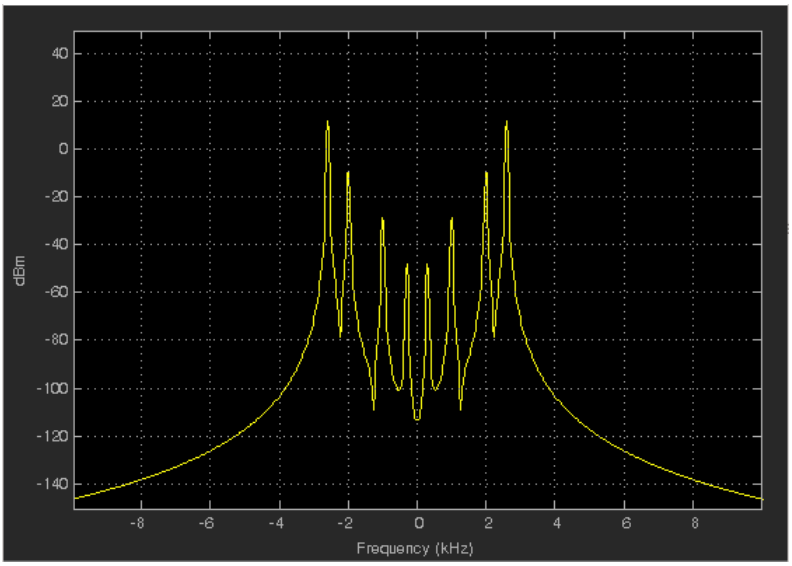
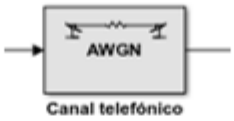


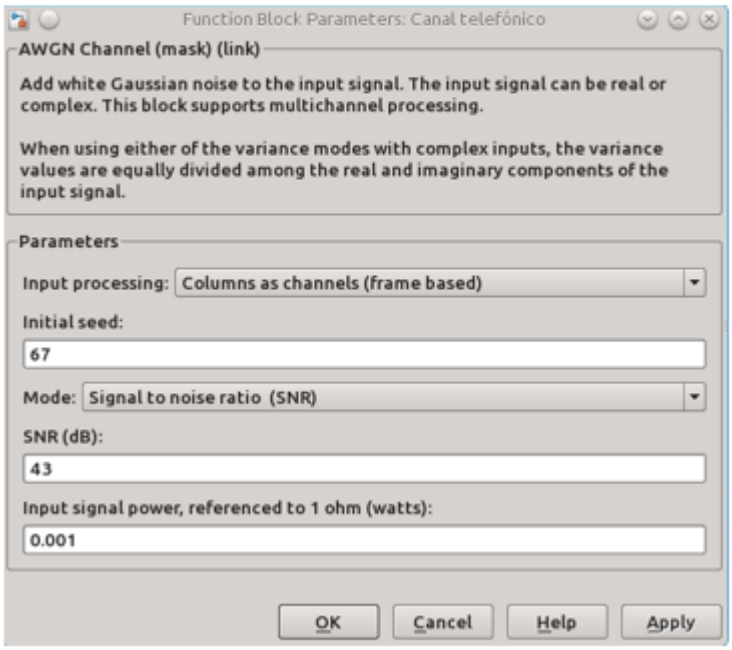
Figura 3. 8: Espectro de la señal a la salida del filtro pasa bajas en el transmisor.
Elaborado por: Autor

3.1.2. Canal de comunicaciones.

Para simular el canal telefónico usamos un bloque que añade ruido blanco gaussiano con el que pueden modelarse los ruidos crosstalk (interferencia generada por la señal de otro par telefónico) según el Comité Consultivo Internacional Telegráfico y Telefónico (ITU-T por las siglas en inglés) los niveles máximos de este tipo de ruido deben ser de 43 dB (ITU-T, 1988), en nuestro trabajo asumimos que los niveles de eco son mínimos o que no existen, esta consideración es totalmente válida debido al gran avance de los sistemas de telefonía actuales. En la figura 3.9 se muestra el bloque del canal telefónico y la ventana de configuración del mismo.



(a)



(b)

Figura 3. 9: (a) Bloque que simula el canal telefónico (b) Ventana de configuración.
Elaborado por: Autor

3.1.3. Instrumentos de medidas.

En la simulación utilizamos 2 tipos de herramientas para observar los resultados: el espectrómetro virtual y el osciloscopio virtual que permiten observar la señal en el dominio de la frecuencia y en el dominio del tiempo respectivamente, ambas son de gran ayuda durante el proceso de puesta a punto ya que se pueden colocar en cualquier punto de la simulación y se puede observar lo que está ocurriendo lo cual permite encontrar las fuentes de errores de manera más sencilla. En la Figura 3.10 se muestra el bloque del espectrómetro, así como la ventana donde se muestra la señal en el dominio de la frecuencia, a modo de ejemplo mostraremos la señal x(t).

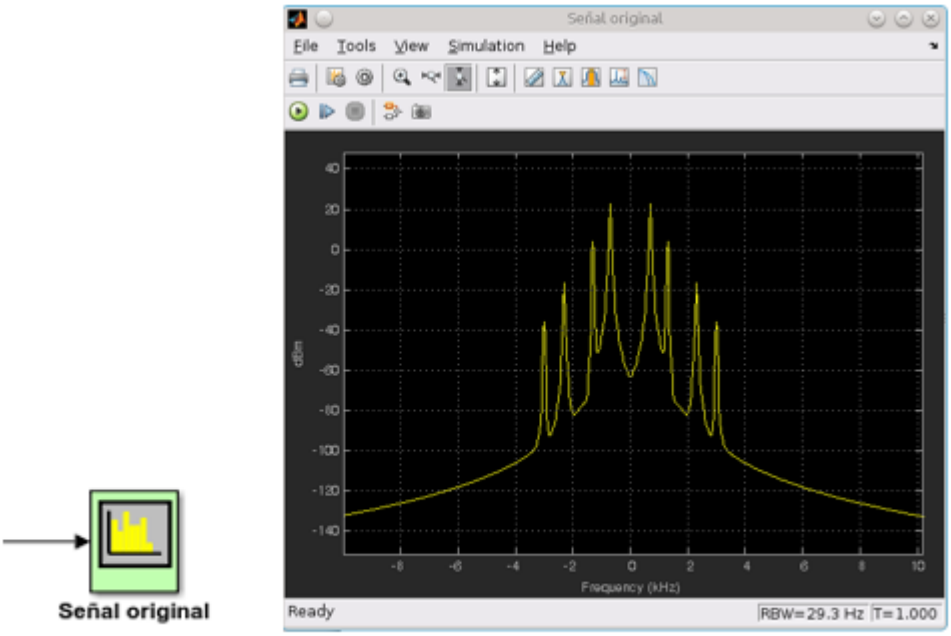


Figura 3. 10: (a) Bloque del espectrómetro (b) Ventana donde se muestra la señal en el dominio de la frecuencia.
Elaborado por: Autor

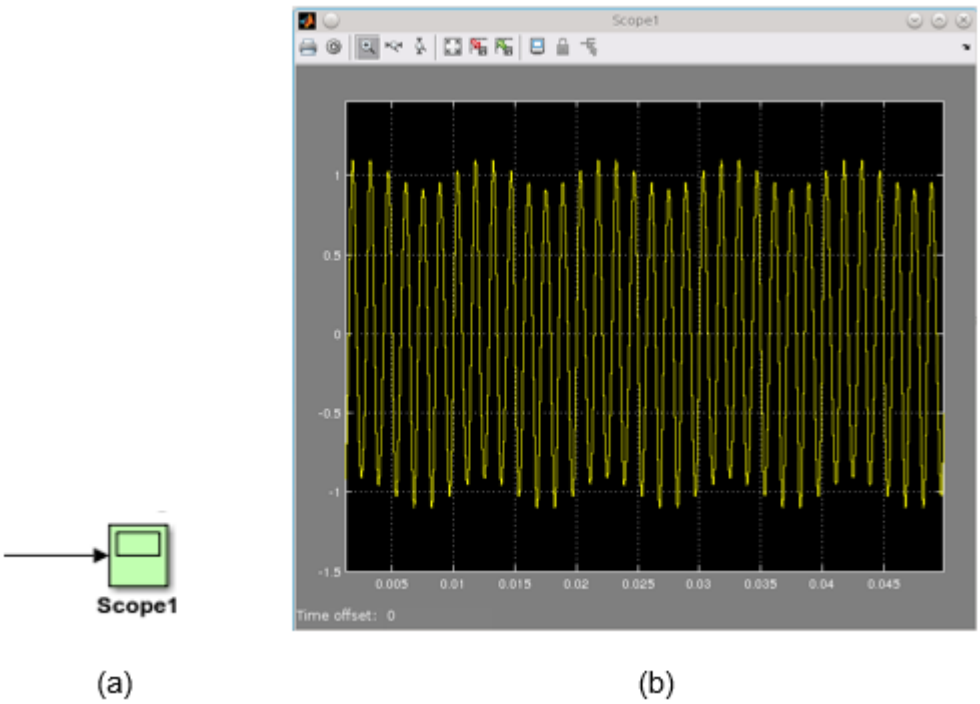


Figura 3. 11: (a) Bloque del osciloscopio (b) Ventana donde se muestra la señal en el dominio del tiempo.
Elaborado por: Autor

En la figura 3.11 se muestra el bloque del osciloscopio, así como la ventana donde se muestra la señal en el dominio del tiempo, a modo de ejemplo mostraremos la señal x(t).

3.1.4. Receptor.

En este sub-apartado analizaremos el receptor del sistema que se muestra en la figura 3.12. El receptor está compuesto por los mismos elementos que el transmisor y colocados de la misma forma por lo que el receptor se comporta de la misma forma que el transmisor invirtiendo el espectro de la señal que recibe, así el mensaje es desenmascarado y vuelve a tener su forma original.

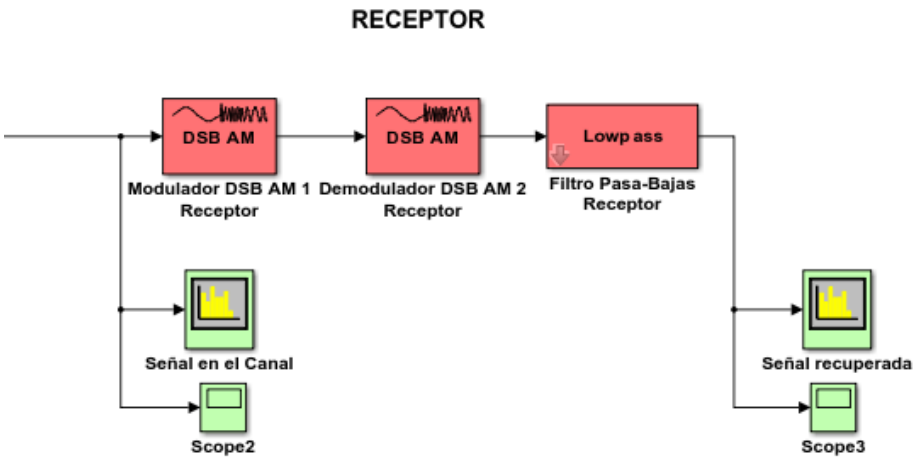


Figura 3. 12: Receptor usado en la simulación de la técnica de enmascaramiento de voz por inversión de frecuencia.
Elaborado por: Autor

La figura 3.13 muestra la seña recibida en la entrada del receptor, se puede apreciar que está contaminada por ruido de banda larga debido al canal telefónico.

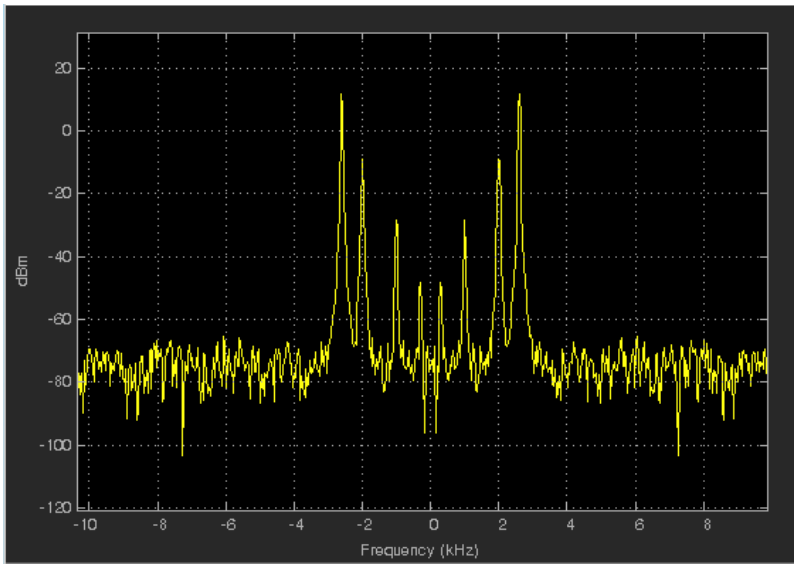


Figura 3. 13: Señal enmascarada contaminada con ruido de banda larga recibida por el receptor.
Elaborado por: Autor

En la figura 3.14 se muestra el resultado a la salida del receptor donde se puede apreciar el mensaje ya desenmascarado con un poco de ruido de banda larga que fue adquirido en el canal.

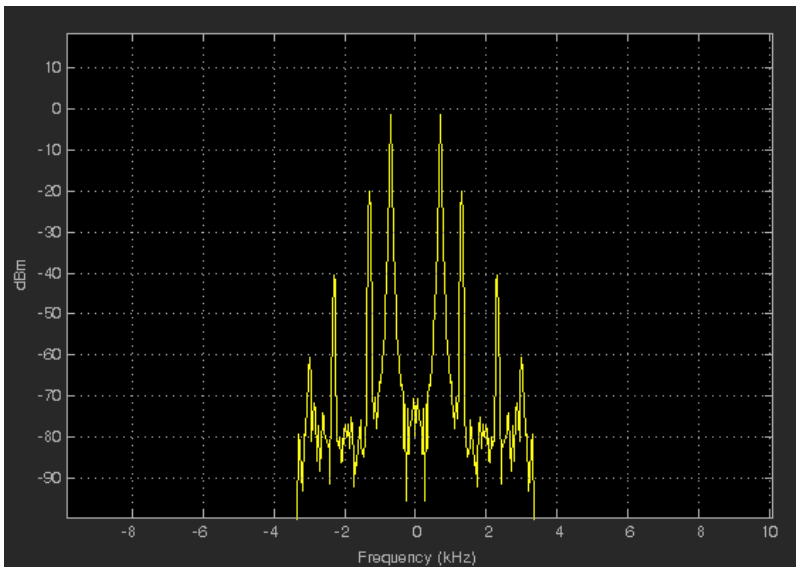


Figura 3. 14: Señal a la salida del receptor ya desenmascarada.
Elaborado por: Autor

En la figura 3.15 se muestra en el dominio tiempo la señal a la salida del receptor ya desenmascarada, como puede observarse existe gran similitud con la señal original.

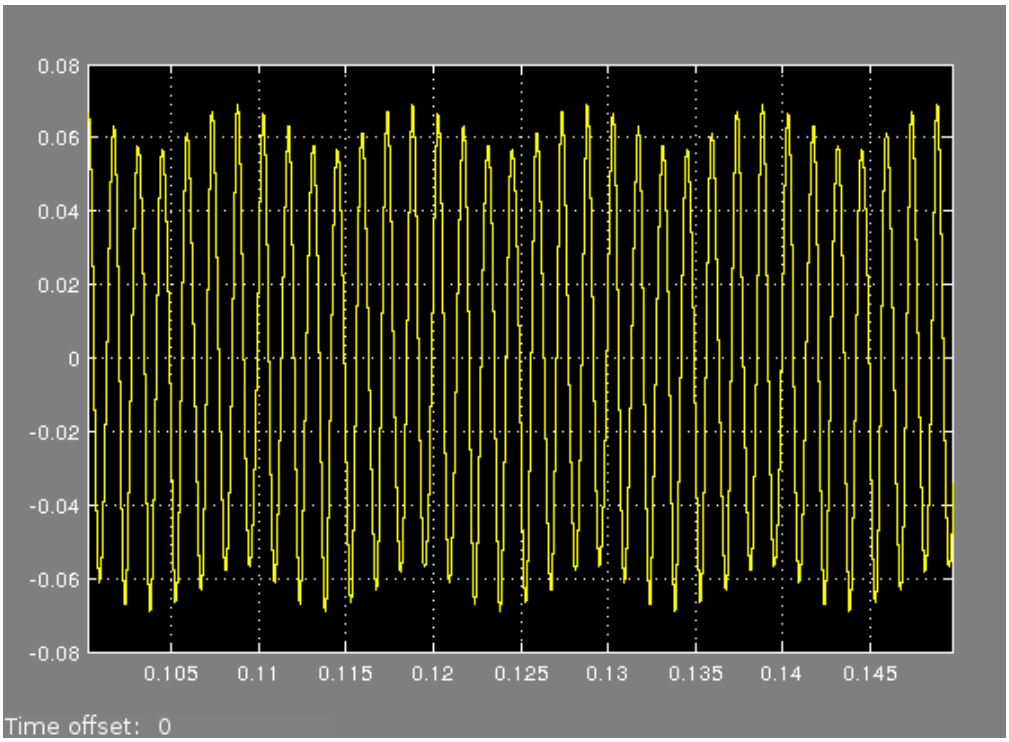


Figura 3. 15: Señal en el dominio tiempo a la salida del receptor ya desenmascarada.
Elaborado por: Autor

3.2. Simulación de la técnica de enmascaramiento de voz por división de banda.

La técnica de enmascaramiento por división de banda consiste en dividir el ancho de banda del mensaje en varias sub-bandas e intercambiar la información que estas contienen, a cada una de esas sub-bandas se le puede invertir o no la frecuencia. La figura 3.16 explica gráficamente la técnica.

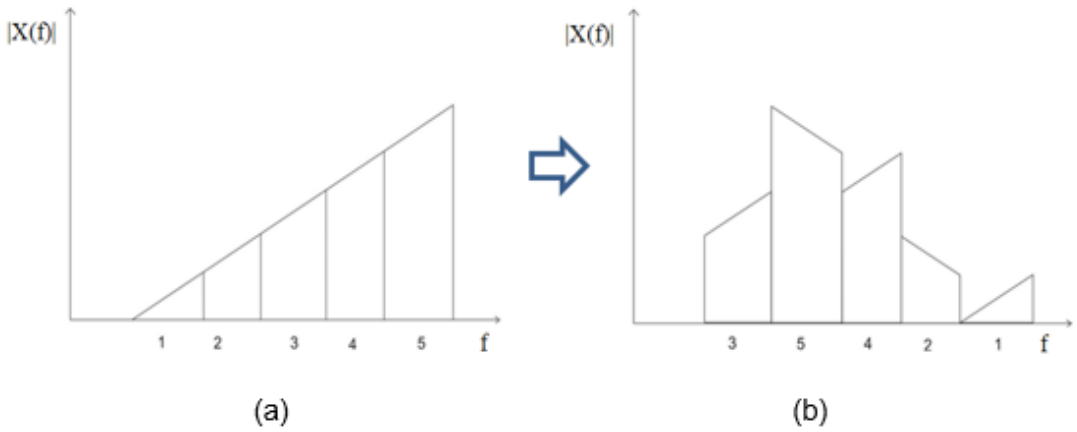


Figura 3. 16: (a) Señal del mensaje (b) Señal enmascarada usando la técnica de enmascaramiento por división de banda.
Elaborado por: Autor

En la figura 3.17 se muestra la simulación de la técnica de enmascaramiento por división de banda en Matlab/Simulink, al igual que en el sistema anteriormente explicado utilizaremos una frecuencia de muestreo de 50 kHz. Observando la figura 3.16 (a) se puede observar que, en términos de permutación, cuando se tienen 5 sub-bandas existen 5! posibles formas de reordenarlas y 25 formas de decidir cuál o cuáles sub-bandas se va a invertir. De esta manera, hay $5! * 25 = 3840$ formas posibles de reordenar las sub-bandas.

Desde el punto de vista matemático, si el espectro se divide en B sub-bandas, entonces el número de reordenamientos posibles de sub-bandas sería $B! * 2B$. En nuestra simulación utilizaremos 4 sub-bandas en los rangos de frecuencia mostrados en la tabla 3.1. De los 384 posibles reordenamientos solo implementaremos 1, cuyo esquema se encuentra en la tabla 3.1.

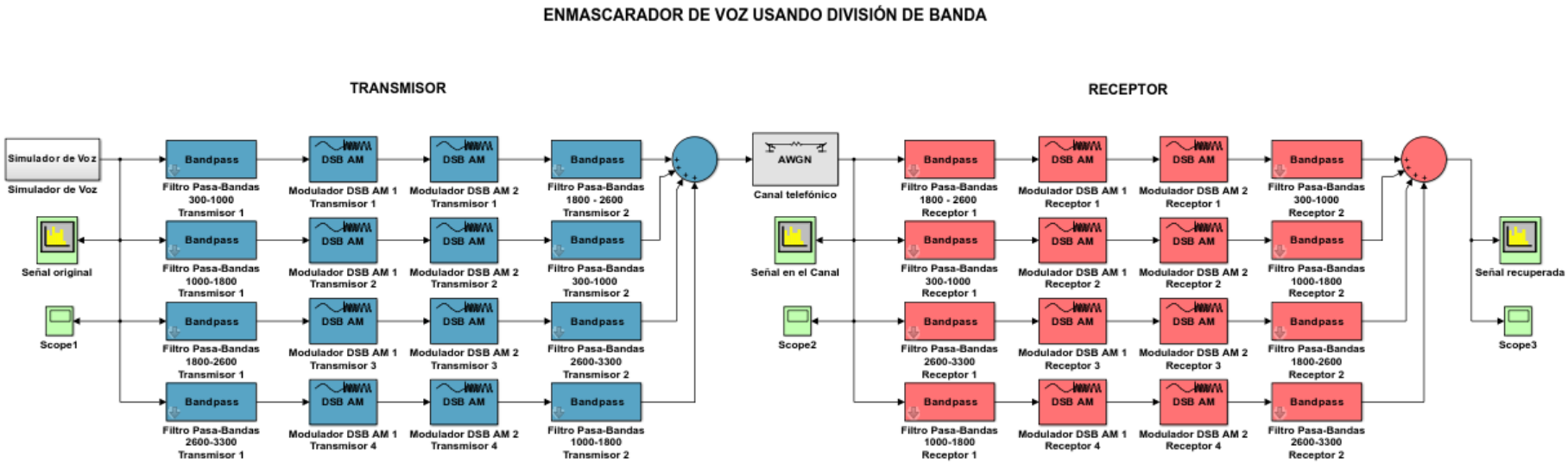


Figura 3. 17: Simulación de la técnica de enmascaramiento de voz por división de banda.
Elaborado por: Autor

Tabla 3. 1: Esquema de reordenamiento utilizado en la simulación

Distribución de la señal de voz	Sub-banda (300-1000 Hz)	Sub-banda (1000-1800 Hz)	Sub-banda (1800-2600 Hz)	Sub-banda (2600-3300 Hz)
Inicial	1ra	2da	3ra	4ta
Enmascaramiento seleccionado	3ra	1ra invertida	4ta invertida	3da

Elaborado por: Autor

3.2.1. Transmisor.

En este sub-apartado analizaremos el transmisor del sistema que se muestra en la figura 3.18. En este sistema utilizaremos el mismo simulador de voz utilizado en el sistema anterior ya que como se explicó dicho simulador de voz permite observar el efecto del enmascaramiento que sufre la señal de entrada o mensaje.

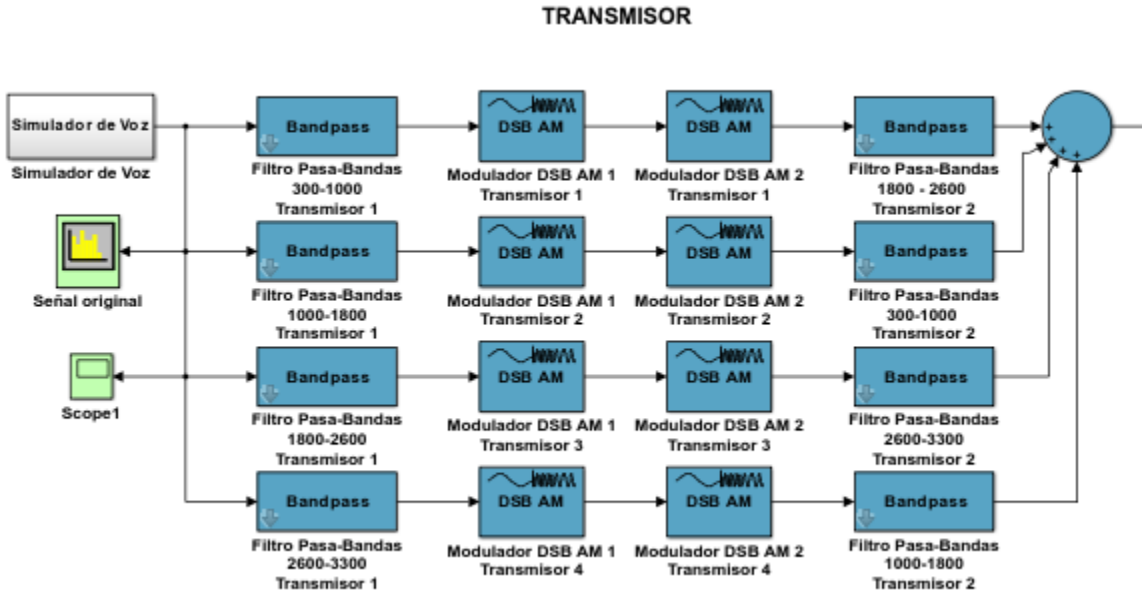


Figura 3. 18: Transmisor usado en la simulación de la técnica de enmascaramiento de voz por división de banda.

Elaborado por: Autor

Para dividir el espectro en sub-bandas se tiene un banco de filtros (véase la figura 3.19) a los cuales se les fijo los valores de la forma es que aparece reflejado en la tabla 3.2, como puede ser observado las bandas que están contiguas tienen un solapamiento de 25 Hz ya que los tamaños de las bandas de transición de los filtros se fijaron en 50 Hz el cual es un valor para la distorsión es pequeña y el costo computacional no es alto.

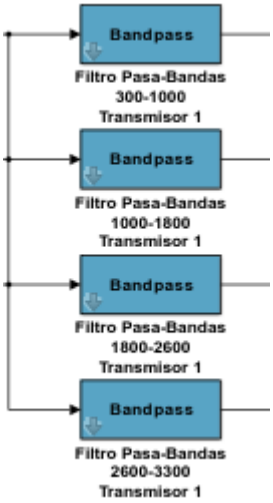


Figura 3. 19: Primer banco de filtros pasa banda en el transmisor.
Elaborado por: Autor

Tabla 3. 2: Valores fijados en los filtros pasa bandas del primer banco, F1 representa la parte baja de la banda y F2 representa la parta alta de la banda.

	Filtro 1 Sub-banda 1 (300-1000 Hz)		Filtro 2 Sub-banda 2 (1000-1800 Hz)		Filtro 3 Sub-banda 3 (1800-2600 Hz)		Filtro 4 Sub-banda 4 (2600-3300 Hz)	
	F1 (Hz)	F2 (Hz)	F1 (Hz)	F2 (Hz)	F1 (Hz)	F2 (Hz)	F1 (Hz)	F2 (Hz)
Banda de atenuación	250	1025	975	1825	1775	2625	2575	3350
Banda de paso	300	975	1025	1775	1825	2575	2625	3300

Elaborado por: Autor

Para trasladar el contenido espectral de una banda otra la operación es prácticamente la misma que la usada en la técnica de inversión de frecuencia solo que de esta ver no se traslada todo el espectro del mensaje

sino solamente la banda en cuestión, para trasladar todas las bandas se necesita un banco de moduladores y demoduladores cuyo tamaño será igual al número de bandas en nuestro caso seria 4, véase la figura 3.20.

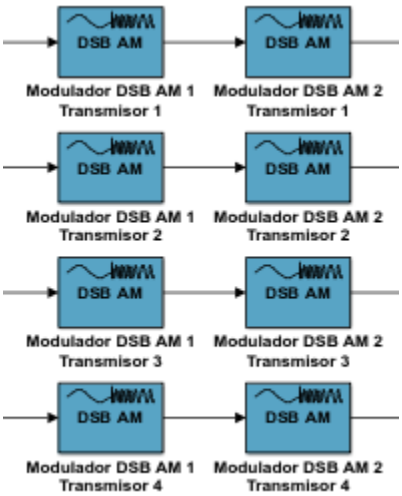


Figura 3. 20: Primer banco de filtros pasa banda en el transmisor.
Elaborado por: Autor

La tabla 3.3 muestra los valores usados en cada modulador u cada demodulador del banco, los valores que se suman o restan en el demodulador dependen de la banda inicial y hacia donde se quiere ir y además si esa banda será invertida o no. Como ejemplo tomemos la primera fila del banco donde se desea trasladar contenido de la primera banda hacia la tercera sin inversión, lo que hacemos es determinar el centro de cada una de las bandas 650 Hz para la primera y 2200 Hz para la segunda luego restamos el valor del centro de la banda que queremos llegar menos el valor del centro de la banda de partida seria 2200 Hz – 650 = 1550 Hz si deseáramos invertir la frecuencia bastaría con invertir el signo del resultado anterior.

Tabla 3. 3: Valores fijados en los moduladores y demoduladores.

	Frec. portadora 1	Frec. portadora 2	Frec. portadora 3	Frec. portadora 4
Modulador	20 kHz	20 kHz	20 kHz	20 kHz
Demodulador	20 kHz + 1550 Hz	20 kHz + 800 Hz	20 kHz – 750 Hz	20 kHz – 1500 Hz

Elaborado por: Autor

Lo siguiente es un segundo banco de filtros los cuales se encargan de filtrar las señales a la salida de cada uno de los demoduladores de manera que sea extraído el contenido el contenido de llegada. La Figura 2.20 muestra el banco de filtros. La configuración de los filtros en este segundo banco se muestra en la tabla 3.4.

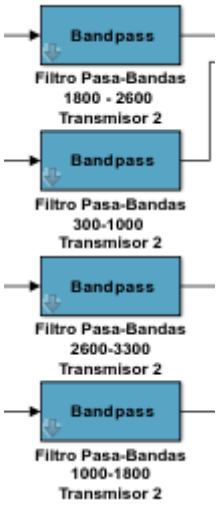


Figura 3. 21: Segundo banco de filtros pasa banda en el transmisor.
Elaborado por: Autor

Tabla 3. 4: Valores fijados en los filtros pasa bandas del segundo bando, F1 representa la parte baja de la banda y F2 representa la parta alta de la banda.

	Filtro 1 Sub-banda 3 (1800-2600 Hz)		Filtro 2 Sub-banda 1 (300-1000 Hz)		Filtro 3 Sub-banda 4 (2600-3300 Hz)		Filtro 4 Sub-banda 2 (1000-1800 Hz)	
	F1 (Hz)	F1 (Hz)	F1 (Hz)	F1 (Hz)	F1 (Hz)	F2 (Hz)	F1 (Hz)	F2 (Hz)
Banda de atenuación	1775	250	2575	975	975	2625	2575	3350
Banda de paso	1825	300	2625	1025	1025	2575	2625	3300

Elaborado por: Autor

La etapa final del transmisor es un sumador (véase la figura 3.22) el cual suma las señales de las salidas de cada uno de los filtros del segundo banco para conformar la señal enmascarada que será transmitida a través del canal telefónico cuyas características ya fueron explicadas en el apartado anterior.

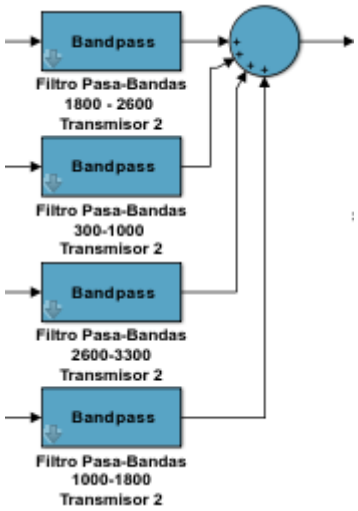


Figura 3. 22: Segundo banco de filtros pasa banda en el transmisor y sumador.
Elaborado por: Autor

3.2.2. Receptor.

El receptor presenta los mismos bloques que el transmisor, dispuestos de una manera similar que permite realizar los cambios en la señal en el transmisor de manera inversa, permitiendo recuperar la señal con la menor distorsión posible. En el receptor el primer banco de filtros toma los valores del segundo banco de filtros del transmisor (véase la tabla 3.4) y el segundo banco de filtros del receptor toma los valores del primer banco de filtros del transmisor (véase la tabla 3.2). Los valores del banco de moduladores y demoduladores del receptor se mantienen iguales al banco análogo en el

transmisor (véase la tabla 3.3). En la figura 3.23 se muestra el receptor implementado.

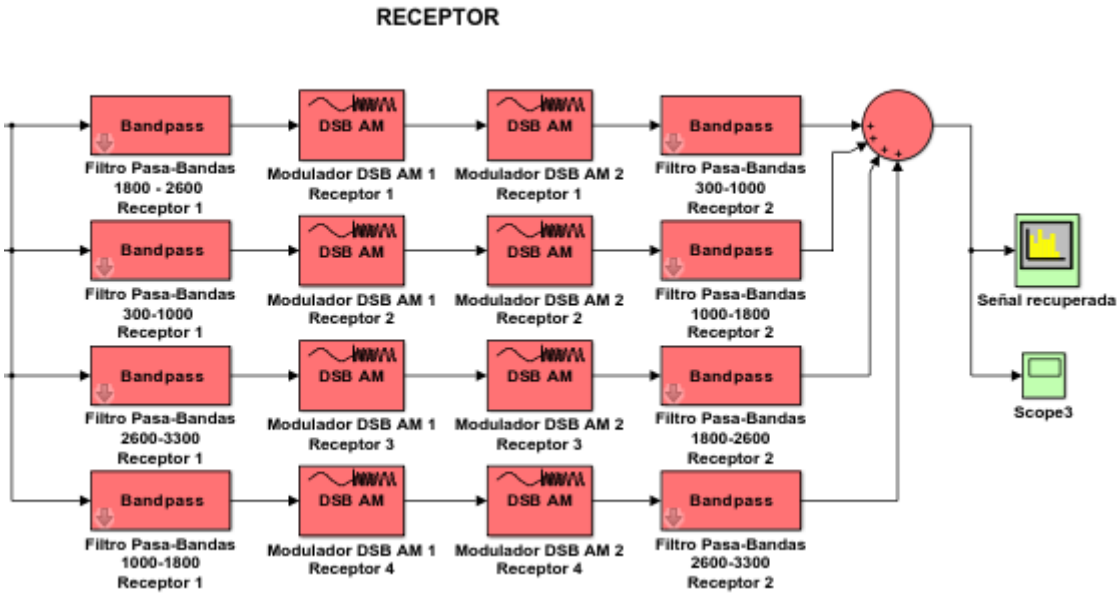


Figura 3. 23: Receptor usado en la simulación de la técnica de enmascaramiento de voz por división de banda.
Elaborado por: Autor

En la figura 3.24 se muestra el espectro de la señal original a la salida del simulador de voz.

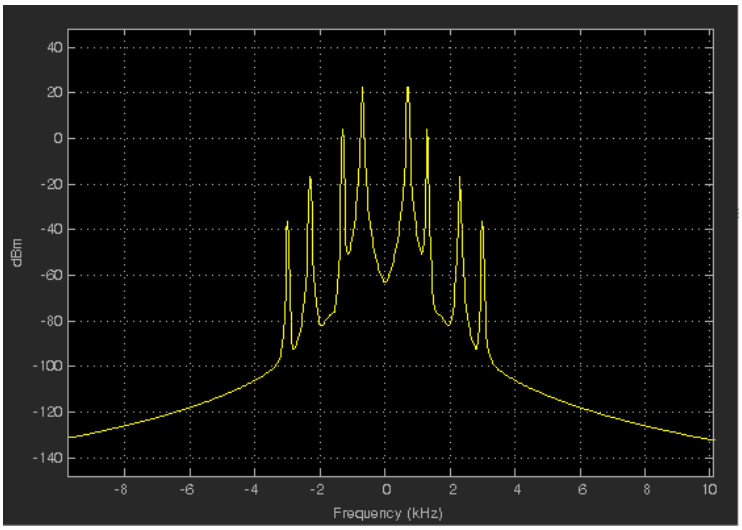


Figura 3. 24: Espectro de la señal generada por el simulador de voz.
Elaborado por: Autor

En la figura 3.25 se muestra el espectro de la señal enmascarada donde se puede observar cómo se han intercambiado las posiciones de los tonos con respecto a la señal original.

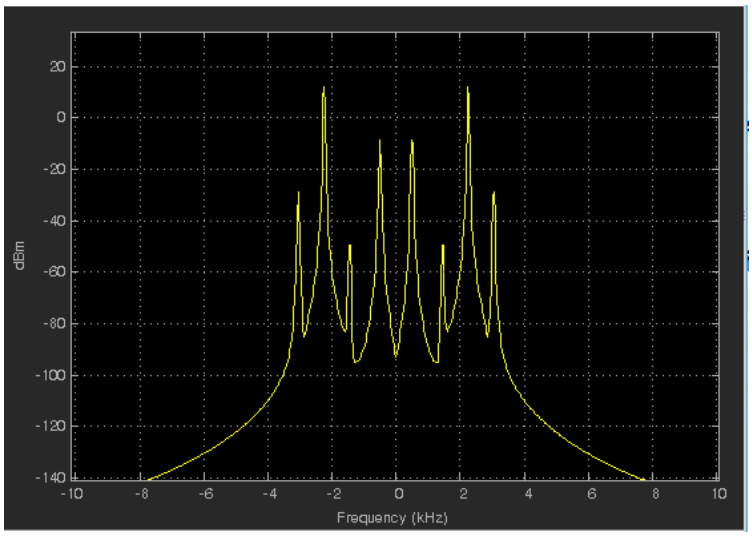


Figura 3. 25: Espectro de la señal enmascarada.
Elaborado por: Autor

La figura 3.26 muestra el espectro de la señal a la entrada del receptor contaminada con ruido de banda ancha.

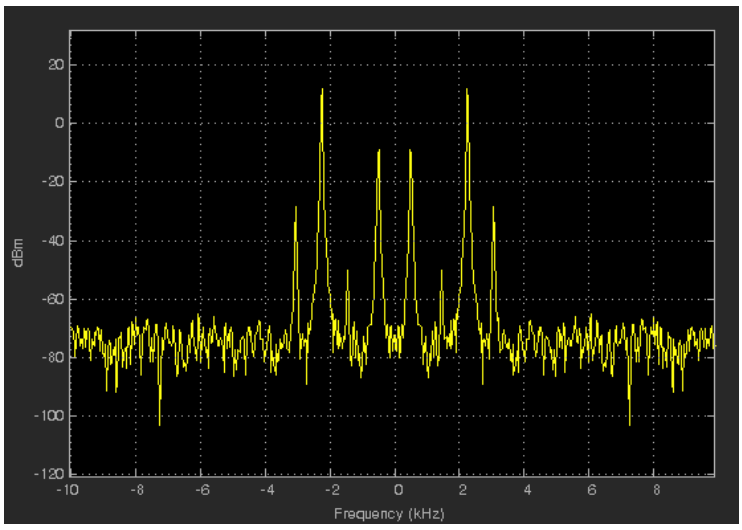


Figura 3. 26: Espectro de la señal a la entrada del receptor.
Elaborado por: Autor

La figura 3.27 muestra el espectro de la señal ya desenmascarada con un poco ruido que fue adquirido en el canal telefónico.

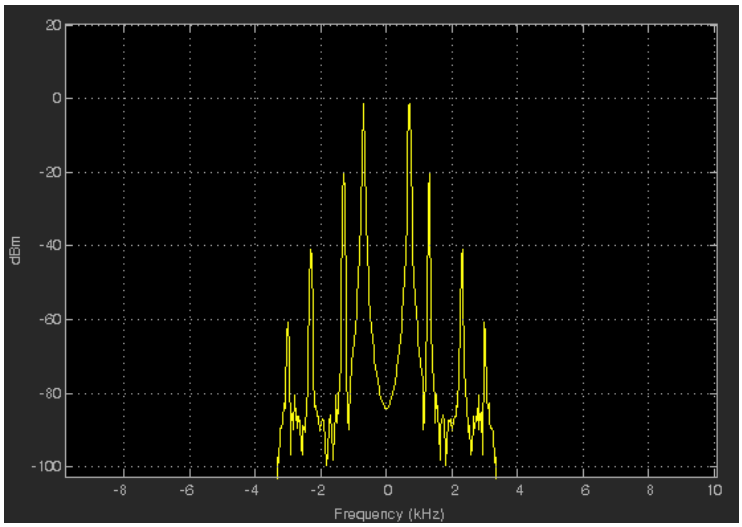


Figura 3. 27: Espectro de la señal recuperada.
Elaborado por: Autor

Conclusiones

- En este trabajo se realizó un estudio profundo de las técnicas de enmascaramiento de voz en el dominio de la frecuencia en el que quedó demostrado que mientras mayor es la complejidad circuital (en el caso de los sistemas analógicos) o mayor la complejidad algorítmica (en el caso de los sistemas digitales), menor es la inteligibilidad residual de la señal que viaja en el canal.
- Se realizó la simulación de 2 técnicas de enmascaramiento de voz en el dominio de la frecuencia, la primera por inversión de frecuencia y la segunda por división de banda, la segunda más compleja y costosa computacionalmente que la primera pero brinda una inteligibilidad residual menor por lo que aumenta la seguridad del mensaje, a esto se suma a que la técnica de inversión de frecuencia puede ser detectada y reproducida de manera sencilla por un tercero no autorizado, por el contrario la técnica de división de banda es mucho más robusta ya que es prácticamente imposible detectar la forma en que fueron reordenadas las bandas.
- A través del estudio de la teoría y de las simulaciones realizadas en Matlab Simulink podemos concluir que las técnicas de enmascaramiento de voz en el dominio de la frecuencia brindan seguridad suficiente para mandar información por canales no seguros ya que la misma no es inteligible por una tercera parte no autorizada y a su vez el sistema es capaz de recuperar la información de manera que el mensaje (en este

caso la voz del interlocutor) es entendida por el que escucha en el receptor.

Referencias bibliográficas.

Ahmed, J., & Ikram, N. (2003). Frequency-domain speech scrambling/descrambling techniques implementation and evaluation on DSP. *7th International Multi Topic Conference, 2003. INMIC*. Retrieved from https://www.infona.pl/resource/bwmeta1.element.ieee-art-000001416613

Beker, H. J., & Piper, F. C. (1985). *Secure Speech Communications*. Academic Pr.

Goldburg, B., & Sridharan, S. (1993). Design and cryptanalysis of transform-based analog speech scramblers. *IEEE Journal on Selected*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=223875

ITU-T. (1988). General performance objectives applicable to all modern international circuits and national extension circuits.

Jameel, A., Siyal, M. Y., & Ahmed, N. (2007). Transform-domain and DSP based secure speech communication system. *Microprocessors and Microsystems*, *31*(5), 335–346. http://doi.org/10.1016/j.micpro.2006.12.001

Nichols, R., & Lekkas, P. (2002). Wireless security. Retrieved from http://sutlib2.sut.ac.th/sut_contents/H106096.pdf

Sutton, R. (2002). Voice Security in Military Applications. *Communications: Applications and Management*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/0470845996.ch3/summary

DECLARACIÓN Y AUTORIZACIÓN

Yo, **JIMÉNEZ MUÑOZ, WASHINGTON ISAAC** con C.C: # 0922076401 autor del Trabajo de Titulación: **SIMULACIÓN DE TÉCNICAS DE ENMASCARAMIENTO DE VOZ EN EL DOMINIO DE LA FRECUENCIA USANDO MATLAB/SIMULINK** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 09 de Septiembre de 2016

f. _____

Nombre: JIMÉNEZ MUÑOZ, WASHINGTON ISAAC

C.C: 0922076401

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	SIMULACIÓN DE TÉCNICAS DE ENMASCARAMIENTO DE VOZ EN EL DOMINIO DE LA FRECUENCIA USANDO MATLAB/SIMULINK		
AUTOR(ES)	JIMÉNEZ MUÑOZ, WASHINGTON ISAAC		
REVISOR(ES)/TUTOR(ES)	M. Sc. EDWIN F. PALACIOS MELÉNDEZ		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	09 de Septiembre de 2016	**No. DE PÁGINAS:**	55
ÁREAS TEMÁTICAS:	Fundamentos de Comunicación, Centrales Telefónicas, Conmutación		
PALABRAS CLAVES/ KEYWORDS:	ADQUISICIÓN, COMUNICACIONES TELEFÓNICAS, ENMASCARAMIENTO, VOZ, INVERSIÓN DE FRECUENCIA, DIVISIÓN DE BANDA		

RESUMEN/ABSTRACT (150-250 palabras):

Los métodos de adquisición y manipulación de información de manera no autorizada han evolucionado mucho en los últimos años por lo que se hace imprescindible conocer y estudiar sistemas que permitan que la información viaje de manera segura a través de canales no seguros. En nuestro trabajo nos enfocaremos en las comunicaciones telefónicas donde la información es la voz del interlocutor y estudiaremos los métodos de enmascaramiento de voz en el dominio de la frecuencia, de los cuales implementaremos en Matlab Simulink el enmascaramiento por inversión de frecuencia y el enmascaramiento por división de banda. En la simulación fueron utilizadas herramientas virtuales con las cuales se puede observar la señal original, la señal ya enmascarada en el canal y la señal desenmascarada en el receptor y se puede constatar de manera visible que el mensaje recuperado es totalmente entendible a la salida del receptor, pero no lo es en el canal de comunicaciones.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-3071699 +593-9-82220231	E-mail: washisaac@hotmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez Edwin Fernando **Teléfono:** +593-9-68366762 **E-mail:** edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	