GENERACIÓN LLAVES DE CIFRADO A PARTIR DE PATRONES BIOMÉTRICOS HUMANOS (CASO ESTUDIO: FIRMA Y VOZ)

The production of encryption keys stemming from human biometric patterns (case study: Signature and voice)

MARÍA FERNANDA CUBIDES LOZANO[1], JUAN DAVID PRIETO RODRÍGUEZ[2], VIOLETA SUAREZ HURTADO[3]

Recibido:03 de diciembre de 2017. Aceptado:28 de diciembre de 2017

DOI: http://dx.doi.org/10.21017/rimci.2018.v5.n9.a38

Resumen

La Biometría es una disciplina de fuerte desarrollo y amplia influencia en las más diversas actividades humanas; como tal las líneas de investigación teórica y aplicada se han multiplicado en los años recientes [1]. Gracias a la biometría se genera una mayor confiabilidad al momento de ingresar a un sitio o servicio por medio de esta autenticación, al implementar una llave de cifrado basado en patrones biométricos se busca preservar los principios básicos de la seguridad de la información. Este artículo presenta el desarrollo de llaves de cifrado a partir de patrones biométricos como lo son la firma y la voz, haciendo que las personas sean portadoras de las contraseñas sin que las conozcan.

Palabras clave: Biometría, Cifrado, MATLAB, contraseña, firma, voz, entropía.

Abstract

Biometrics is a discipline of strong development and wide influence in the most diverse human activities; as a result, the lines of theoretical and applied research have multiplied in the latest years [1]. Thanks to biometrics, when entering a site or service through this kind of authentication there is greater reliability. By implementing an encryption key based on biometric patterns, the goal is to preserve the basic principles of information security. This article presents the creation of encryption keys based on biometric patterns such as the signature and the voice, making people carry passwords without knowing them.

Keywords: Biometrics, Encryption, MATLAB, password, signature, voice, entropy.

I. Introducción

Debido a que la sociedad cada día está conectada electrónicamente, se generan problemas de seguridad, en cuanto a transacciones bancarias, transacciones compra y compra, robo de información, perdida de privacidad, mal manejo de la información, falsificaciones entre otros, debido a esto se ha implementado el uso la biometría para la identificación en diversos sitios.

1 Estudiante de último semestre de Tecnología en Redes de computadores y Seguridad Informática de la Corporación Universitaria Minuto de Dios, miembro del semillero de Investigación SERMOV y asistente de investigación del proyecto de Generación de llaves de cifrado a partir de patrones biométricos humanos que puedan ser implementadas en redes de datos que presten servicios sociales a la comunidad.

2 Miembro IEEE; Ingeniero Electrónico y de Telecomunicaciones Universidad San Martin especialista en Seguridad Universidad Piloto, profesor de planta de la Corporación Universitaria Minuto de Dios, Líder del semillero SERMOV e investigador principal del proyecto de Investigación Generación de llaves de cifrado a partir de patrones biométricos humanos que puedan ser implementadas en redes de datos que presten servicios sociales a la comunidad.

3 Miembro IEEE; Ingeniera en Sistemas Pontificia Universidad Javeriana, Aspirante Master en Computer Scienxe University of Houston, profesora de planta de la Corporación Universitaria Minuto de Dios. Líder del grupo de estudio adscrito al semillero SERMOV.

La cifra de delitos informáticos en el país va en aumento. Tanto que Colombia es actualmente, el tercer país en Latinoamérica donde más se cometen [2].

La delincuencia informática mundial tiene un costo de 114 mil millones de dólares anuales, se determinó que más de dos tercios de los adultos en línea (69%) han sido víctimas de la ciberdelincuencia alguna vez en la vida. Cada segundo, 14 adultos son víctimas de un crimen cibernético, lo que deja como resultado más de un millón de víctimas del cibercrimen todos los días [3].

La biometría dominara tanto los aspectos de la economía como nuestra vida diaria ya que el uso de está en cuanto a verificación de autenticidad es un gran avance para no ser blanco fácil de los ciberdelincuentes, que al momento de robar las contraseñas pueden acceder a todos los datos y realizar una suplantación para poder realizar compras, ventas, retiros entre otros hablando del ámbito financiero.

En cuanto al robo de contraseñas de redes sociales o correos electrónicos lo hacen con el fin de generar insultos, amenazas, acoso, chantaje, videos que ridiculizan, fotografías que desprestigian, con el objetivo de destruir su honor en acciones que afectan su intimidad [4].

II. Marco de referencia

Contraseña: Cadena de caracteres alfanuméricos de longitud arbitraria, usada como herramienta básica de autenticación de identidad [5].

Biometría: Biometría es una ciencia que analiza las distancias y posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas. La palabra biometría deriva del griego **bios** (que quiere decir vida) y **metria** (que quiere decir medida). Los rasgos biométricos son medidas extraídas del cuerpo humano vivo. Y, además, todos los rasgos biométricos son una combinación de anatomía y de comportamiento [6].

Para ser utilizadas como elementos de identificación deben cumplir con los siguientes requisitos:

a. *Universalidad:* Todas las personas tienen o presentan una característica.

b. *Singularidad:* Dos personas cualesquiera son distinguibles una de la otra en base de sus características.

c. *Estabilidad:* La característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas.

d. *Cuantificable:* La característica tiene que ser mesurable cuantitativamente.

e. *Aceptabilidad:* El nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico.

f. *Rendimiento:* El nivel de exactitud requerido debe ser elevado para que la característica sea aceptable.

g. *Usurpación:* Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.

En función de las características se dividen en dos áreas:

- *Biometría Estática:* Es el estudio de las características físicas del ser humano. Por ejemplo la huella dactilar, características de la cara, iris, retina, ojo, etc [7].

- Biometría dinámica: Estudia las características de la conducta del ser humano. Por ejemplo firma, tecleo, gestos, voz, movimientos corporales [7].

Biometría voz: Los sistemas de reconocimiento del locutor tienen por objeto discriminar locutores a partir de características diferenciadoras obtenidas mediante el análisis y el tratamiento de la señal de voz. El estudio de los mecanismos de producción de ésta se incluye dentro de disciplinas tales como la acústica de cavidades, la anatomía humana, la física de los fluidos o la propagación de las ondas acústicas [8].

***Biometría Firma**: La firma* manuscrita es el medio más cotidiano que se usa para la verificación de la identidad de una persona, ya sea para indicar la autoría de un documento por una persona en particular, o para la certificación de la conformidad de una persona en cualquier tipo de transacción. Por ello, a la firma se le considera como una característica biométrica confiable para la identificación de una persona o para la verificación de su personalidad; sin embargo, la frecuencia de los intentos de falsificación de la firma en la actualidad es relativamente grande.

***Cifrado por bloques**: La* información a cifrar se divide en bloques de longitud fija (8,16,... bytes) y luego se aplica el algoritmo de cifrado a cada bloque utilizando una clave secreta. Ejemplos: DES, AES.

Existen distintos modos de operación dependiendo de cómo se mezcla la clave con la información a cifrar:

- *Modo ECB (Electronic Codebook):* El texto se divide en bloques y cada bloque es cifrado en forma independiente utilizando la clave. Tiene la desventaja que puede revelar patrones en los datos.

- *Modo CBC (CBC):* El texto se divide en bloques y cada bloque es mezclado con la cifra del bloque previo, luego es cifrado utilizando la clave.

- *Modos CFB (Cipher FeedBack) y OFB (Output FeedBack) [9].*

III. Metodología

El algoritmo general está compuesto por la implementación de otros, para realizar el procesamiento digital de la firma, extracción de la voz y generación llave de cifrado a partir de patrones biométricos de la voz y la firma. Ver Fig. 1.

A. Digitalización de la imagen

Por medio de Scaner es posible realizar la digitalización de las firmas, seguido de esto se cargan las imágenes a MATLAB. Ver Fig. 2.

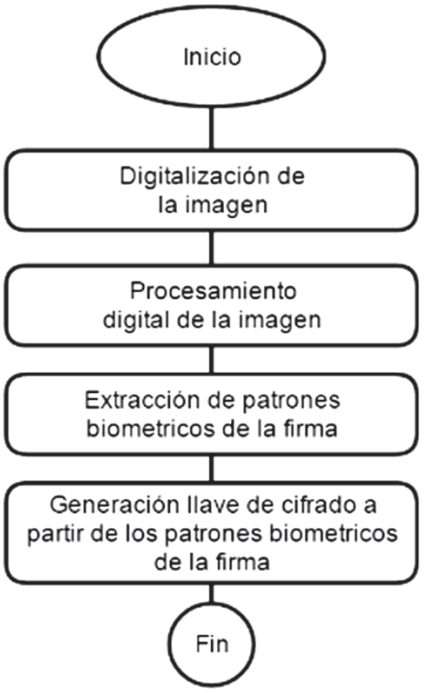

Fig. 1. Algoritmo general propuesto para la firma.

Fig. 2. Firma digitalizada y cargada en MATLAB.

B. Procesamiento Digital de la Imagen

Para la extracción de patrones biométricos se usó la función RGB2Gray y Binarización para minimizar el ruido propio de la imagen como se muestra en la Fig. 3. Para la generación de llave, se usa el resultado de la Binarizacion de la imagen para obtener debidamente los patrones biométricos.

C. Extracción de Patrones Biométricos

La imagen resultante después de binarizar es una matriz binaria donde negro es la representación de un cero lógico y blanco por un uno.

Fig. 3. Firma Binarizada.

Por lo tanto se extrae la posición de que un 1 ocupa en la matriz, almacenando en dos vectores i, j para usar en la llave de cifrado.

D. Extracción Muestras aleatorias

Por medio de la función Randi de MATLAB se extraen 16 valores aleatorios en cada vector i, j para así poder generar la llave de cifrado de 128 bits.

E. Generación llave de cifrado a partir de patrones biométricos

Se realiza una operación lógica "OR" con los 16 valores aleatorios de cada vector generado por medio de la función Randi de MATLAB. Ver Fig. 4.

1. Grabación de voz

Por medio del software MATLAB es posible grabar voz con el fin de extraer los patrones biométricos para generar la llave de cifrado. Ver Fig. 5.

2. Transformada de Fourier

$$g(\xi) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(x) e^{-i\xi x} dx \quad (1)$$

Por medio de MATLAB la transformada de Fourier de x(n) Ecuación 1. se calcula con el comando fft(x) gracias a esa transformada es posible extraer los patrones biométricos para generar la llave de cifrado. Ver Fig. 6.

3. Extracción patrones biométricos

Gracias a la transformada de Fourier se pueden extraer los 16 valores puntuales ya que detecta cada minucia de la grabación de voz para poder generar la llave de cifrado.

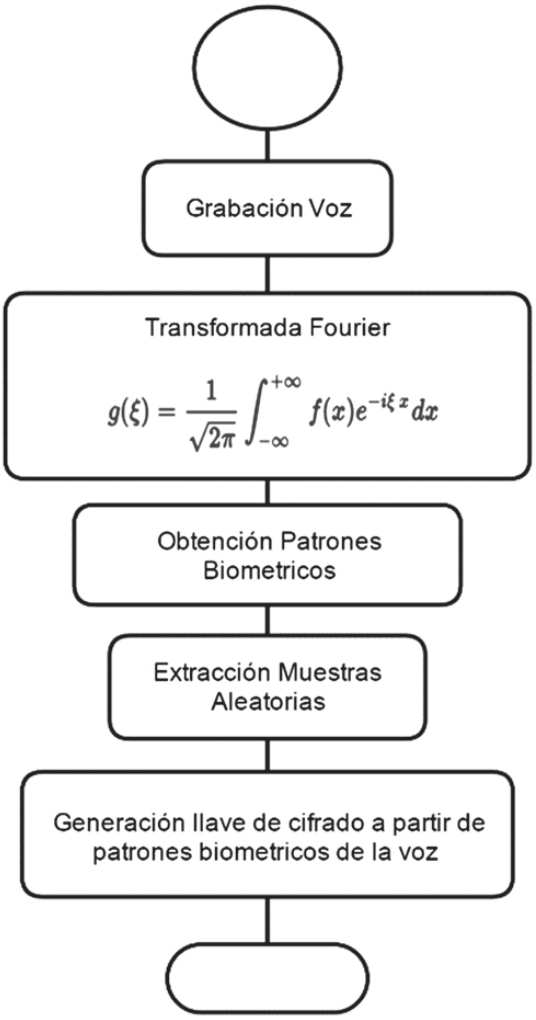

Fig. 4. Algoritmo general propuesto para la voz.

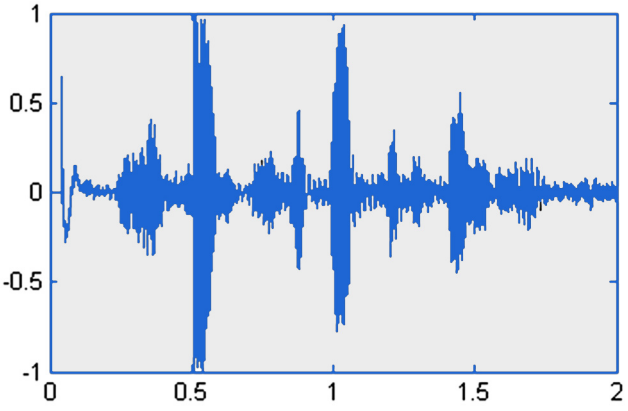

Fig. 5. Grabación de voz.

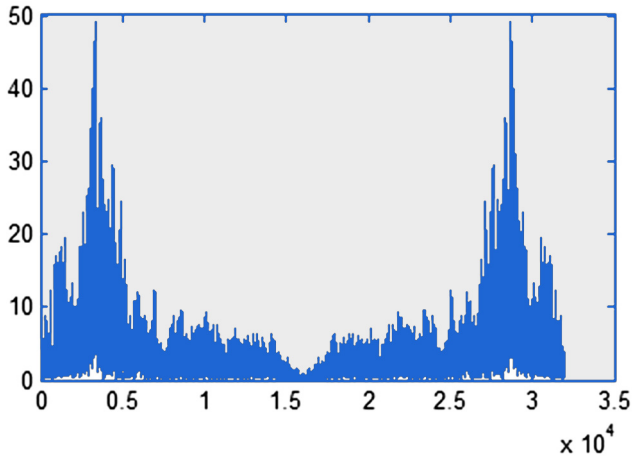

Fig. 6. Valor absoluto de la grabación de voz transformada.

4. *Extracción muestras aleatorias*

Por medio de la función Randi de MATLAB se extraen 16 valores aleatorios del vector z que se generó de la transformada de Fourier, para así poder generar la llave parcial.

5. *Generación llave de cifrado a partir de patrones biométricos*

Se generó el vector z, el cual se almacena ya que es la llave parcial y será utilizado más adelante para la generación de llave de cifrado de 128 bits.

A continuación se muestra el algoritmo propuesto de manera completa en la fig. 7.

6. *Extracción Muestras Aleatorias*

Función Randi MATLAB:

X = randi(imax) devuelve un número entero pseudoaleatorio escalar entre 1 y imax [10].

Gracias a la función Randi de MATLAB descrita anteriormente se extraen los 3 vectores cada uno con 16 números aleatorios para poder generar la llave de 128 bits.

7. *Concatenación vectores patrones biométricos firma y voz*

Se realiza una operación lógica "OR" con los 16 valores resultantes de la llave de cifrado de la firma y los 16 valores de la llave parcial de la voz.

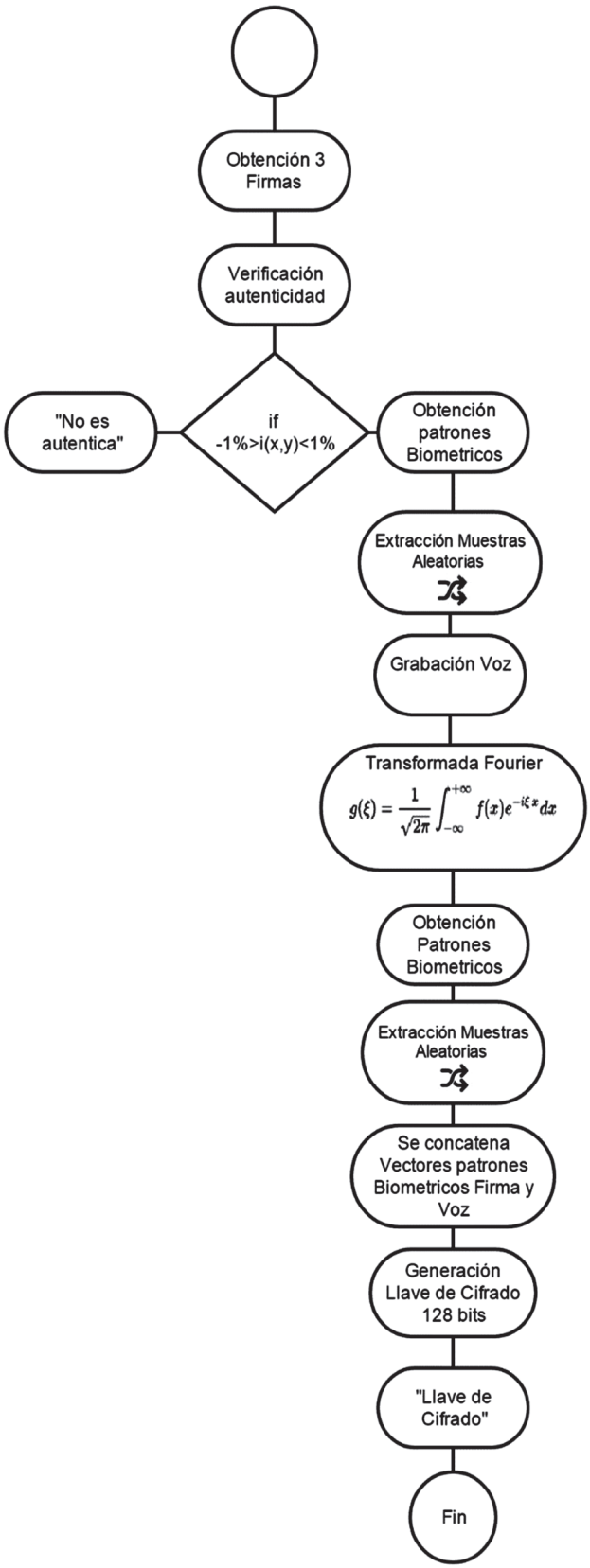

Fig. 7. Algoritmo propuesto generación llave de cifrado.

8. Generación llave de cifrado de 128 bits

Se tomaron 16 valores aleatorios de cada vector y se realizó las operaciones lógicas OR para generar la llave de cifrado ya que a esto equivale la clave de 128 bits.

16 bytes pueden representar 16 caracteres de nuestro abecedario u otros símbolos según la codificación (UTF, Base64, etc) que se use [11].

Una clave de 128 bits tiene:

340.282.366.920.938.463.463.374.607.431.768.211.456 posibles combinaciones. Son más de 340 millones de mil millones de mil millones de mil millones de combinaciones [11]. Ver Fig. 8.

IV. Caracteristicas de la llave de cifrado

El algoritmo planteado en este proyecto de investigación busca ofrecer una solución a los problemas de seguridad que tiene una llave de cifrado, haciendo que una persona sea la portadora de su llave sin que la conozca propiamente.

Una vez binarizadas las imágenes es posible realizar la comparación entre las 3 firmas y así se verifica la autenticidad que tiene un porcentaje de error de solo el 1%, en cuanto a la voz es posible tomar cada minucia gracias a la transformada de Fourier.

A continuación se muestran las gráficas de 3 pruebas de llave de cifrado, en la figura 9, 10 y 11.

V. Conclusiones

La seguridad en los métodos de identificación de todas las personas se ha convertido en una prioridad en la sociedad en que vivimos, a partir de patrones biométricos es posible diseñar o implementar una llave de cifrado de 128 bits para poder preservar los principios básicos de la seguridad de la información.

La biometría es una herramienta fuerte para la verificación y autenticación de personas a partir de sus rasgos entre los que se pueden citar, la firma, la voz, la huella, el iris, etc, ya sea para transacciones, entrada a diferentes zonas, entre otros.

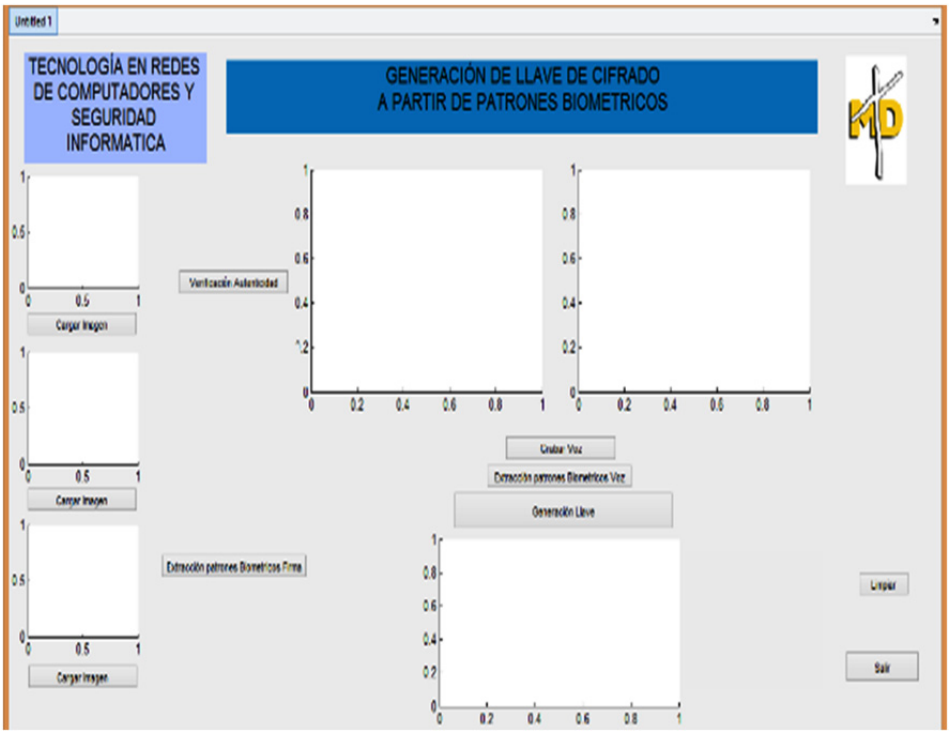

Fig. 8. Interfaz gráfica Generador de llaves de cifrado.

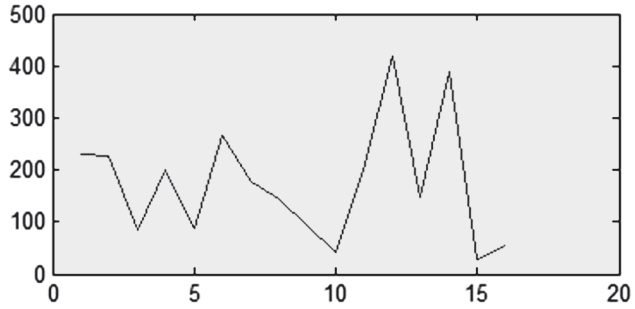

Fig. 9. Llave de cifrado muestra 1.

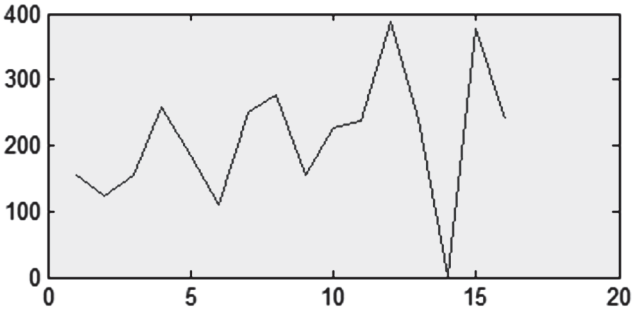

Fig. 10. Llave de cifrado muestra 2.

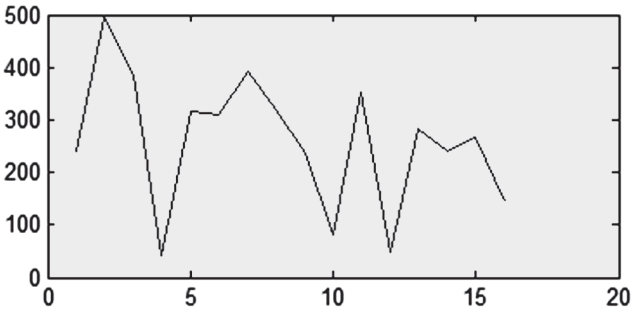

Fig. 11. Llave de cifrado muestra 3.

La firma es una de las técnicas de biometría más utilizada para verificar la autenticidad de la persona, en este proyecto se implementó una comparación entre las mismas, teniendo solo un 1% de error, para garantizar el principio de autenticidad.

La transformada de Fourier es de gran importancia al momento de obtener los patrones biométricos de la voz ya que se toma cada minucia de la grabación de voz y de estas minucias se tomaron los valores absolutos.

Se genera una llave de cifrado de 128 bits equivalente a 16 bytes ya que tiene 340.282.366.920.938.463.463.374.607.431.768.211.456 posibles combinaciones y es más difícil de romper el algoritmo criptográfico a través de un ataque de fuerza bruta para probar todas las claves posibles; no se usó una clave de 256 bits ya que por razones de velocidad en cuanto más larga la clave más tarda en decodificar y el principal objetivo de la criptografía es proteger información con claves simples, pero que sigan siendo seguras.

VI. Referencias

[1] S. F. Juárez y M. M. Ojeda, "Bios metria". Universidad Verecruzana. Boca del Rio, Veracruz, México. 2009.

[2] Colprensa y Redacción de El País. En Colombia las cifras de delitos informáticos van en aumento. El País. (31 de Diciembre de 2012).

[3] M. B. Miguez, "Ciberdelincuencia un mal que afecta a la sociedad actual". 2014.

[4] L. López & L. Antonio, "El Cyberbullying en estudiantes del nivel medio superior en México". In Documento presentado en X Congreso Nacional De Investigación Educativa. México: Área (Vol. 17). 2008.

[5] A. Martinéz-Ballesté, A. Solanas & J. Castellá-Roca (s.f.). Docplayer.es. Obtenido de http://docplayer.es/5454649-Identificacion-autenticacion-y-control-de-acceso.html

[6] F. Serratosa, "La biometría para la identificación de las personas". Universitat Oberta de Catalunya, 8-20. 2008.

[7] J. C. L. Pró Concepción, "Tecnologías Biométricas aplicadas a la seguridad en las organizaciones". Revista de investigación de Sistemas e informatica. 2009.

[8] D. Suárez & E. C. Herrera, "La firma como un método biométrico de identificación". Instituto Politécnico Nacional. Centro de Investigación en Computación. 2008.

[9] A. Pousa, "Algoritmo de cifrado simétrico AES" (Doctoral dissertation, Facultad de Informática). 2011.

[10] MathWorks. (s.f.). Randi. Obtenido de https://es.mathworks.com/help/matlab/ref/randi.html

[11] A. Preukschat, ¿Qué significa un bit, tamaño y longitud en una clave criptográfica? (IX). 20 de Enero de 2014). Obtenido de https://www.oroyfinanzas.com/2014/01/que-significa-bit-tamano-longitud-clave-criptografica/