Autenticación de Tarjetas de Crédito por medio de Ultrasonido y el Algoritmo MAVG-14

Miguel A. Alejos y Victor J. González

***Resumen*—El sistema de autenticación de tarjetas de crédito por medio de ultrasonido funciona gracias a las partículas de acero encontradas dentro de la tarjeta las cuales fueron alojadas de forma aleatoria durante la fundición del plástico en la fabricación. Se presenta una imagen de dos colores, blanco y negro, generada por el ultrasonido. El color blanco representa las zonas donde se encuentran alojadas las partículas de acero. El comportamiento de este sistema funciona bajo el concepto de cifrado híbrido debido a que la clave se encuentra en la fuente y el destino así como también en códigos generados que se transmiten con la carga útil. Se propone un algoritmo, de nombre MAVG-14, para evitar una congestión en la red y la inseguridad del medio de transmisión, basado en el cambio de los parámetros de cifrado dependiendo del mes, año, ID tarjeta e ID punto de servicio.**

***Palabras claves*— Acero, Cifrado, Plástico, Ultrasonido**

I. Introducción

El sistema de autenticación de tarjetas de crédito funciona gracias a la propiedad de las ondas en la banda ultrasónica, al poder enviar una señal y esperar su retorno, es decir; una respuesta de eco, la cual es analizada desde que fue transmitida hasta que fue recibida para generar un patrón entre el tiempo más corto, largo y medio.

El tiempo de retorno depende de la impedancia acústica de los materiales de fabricación de las tarjetas, para el presente estudio en particular se considera el acero y el plástico.

El sistema de ultrasonido posee la capacidad de discriminar en tres patrones: El primero en donde se encuentra la pintura y recubrimiento de la tarjeta, el segundo donde se encuentra el metal y el tercero donde solo existe plástico, generando t(1), t(2) y t(3) donde t representa la respuesta de eco del la onda acústica. [1]

Las partículas de acero encontradas dentro de la tarjeta son alojadas de forma aleatoria durante la fundición del plástico en la fabricación.

Artículo recibido el 04 de Diciembre de 2009.

M.A A. Cabudare, Estado Lara, Venezuela. Telf +58-0414-573-7644, E-mail: miguelangelalejos@gmail.com

V.J.G. está con la UFT, Urb. Chucho Briceño, Etapa II, Cabudare Edo Lara, Facultad de Ingeniería, Escuela de Telecomunicaciones. Tlf. +58-0251-7100207, E-mail: vjgonzalezg@gmail.com

Después de la fundición se debe entregar un certificado de autenticación para la base de datos del banco el cual es representado por una imagen de dos dimensiones y dos colores generada por el ultrasonido utilizando una técnica de ecografía, la cual discrimina en colores las diferentes respuestas de eco del ultrasonido, el cual representa el color blanco las zonas donde se encuentran alojadas las partículas de acero que son invisibles para el ojo humano y evita que personas externas memoricen esta información como lo hacen con los números de las tarjetas que se encuentran en el relieve.

Esta imagen es tomada en un área de 2,5 cm^2 ubicados en la parte inferior del lado izquierdo de la tarjeta de crédito a un lado de la banda magnética.

El algoritmo propuesto aplica cifrado híbrido, puesto que la clave se encuentra en la base de datos de las entidades bancarias (la fuente) y en el interior de la tarjeta (el destino), por medio de las partículas de acero y variables independientes que se dividen en fijas y dinámicas;

a) Las fijas se encuentran los identificadores de las tarjetas de crédito como también el identificador del punto de servicio los cuales son únicos y muy difíciles de modificar por personas no autorizadas ya que se encuentran en la memoria ROM del sistema, la cual mayormente es de solo lectura.

b) Las dinámicas se puede encontrar la confiabilidad de este sistema a corto, mediano y largo plazo porque cambia el método de selección de autenticación por medio del año y el mes. [2]

II. La Seguridad de las Comunicaciones en las Tarjetas de Crédito.

Actualmente existe la necesidad de implementar sistemas de autenticación robustos aplicando nuevas técnicas las cuales sean inmunes a los ataques causados por las clonaciones. En la actualidad la tecnología es de gran importancia para las personas que buscan seguridad, servicio y confort, sin embargo; existen personas inescrupulosas que la utilizan para cometer actos vandálicos los cuales perjudican a terceros.

Los modelos de cifrado y autenticación cada vez son más robustos, pero siempre existen personas con gran estímulo y curiosidad, con técnicas y equipos para trabajar de forma paralela con fines educativos, personales o a terceros que

ISBN: 978-980-7185-1

puedan interferir en los sistemas de seguridad de las tarjetas de crédito o cualquier modelo de cifrado o autenticación presente.

La clonación de tarjetas de crédito es causado por la vulnerabilidad de copiado y grabado de las cintas electromagnéticas que contienen la información la cual puede ser duplicada (n) cantidad de veces.

Los sistemas de almacenamiento de información actuales se ven afectados por los campos electromagnéticos y por el desgaste causado por la fricción al momento de ser ingresada al punto de servicio o simplemente roce con otras tarjetas dentro de la cartera, perdiendo las características necesarias para un buen funcionamiento.

Los sistemas actuales de cifrado se basan en tener una mayor cantidad de bits para la codificación pero siguen teniendo problemas fundamentales; primero es que inyectan demasiado tráfico en la red y produce congestionamiento; los sistemas simétricos poseen la desventaja de tener una única clave en el origen y en el destino, y si se logra capturar una vez la trama generada, esta puede ser analizada por resoluciones matemáticas o métodos estadísticos. En el caso de ser asimétrico la información se envía junto a la llave para que al momento de llegar sea decodificada.

Se propone un nuevo sistema de cifrado híbrido en donde solo se envíen exactamente píxeles específicos dependiendo de variables en el tiempo (mes, año), locales (ID tarjeta, ID Telecajero).

En el caso de que se capture una trama en un punto se servicio especifico, este pierde la vigencia al mes siguiente, tiempo suficiente para que los sistemas de seguridad bancario utilicen la información en contra de los tarjetahabiente.

II. ULTRASONIDO

El sonido es la sensación producida en el órgano del oído por el movimiento de los cuerpos, transmitidos por un medio material. En los seres humanos, esto ocurre siempre que una vibración con frecuencia comprendida entre unos 15 y 20000 Hz llega al oído interno.

Estas vibraciones llegan al oído interno transmitidas a través del aire, y a veces se restringe el término sonido a la transmisión en este medio. Sin embargo, en la física de hoy día se suele extender el término a vibraciones similares en medios líquidos o sólidos. Los sonidos con frecuencias superiores a unos 20000 Hz se denominan ultrasonidos.

En general, las ondas pueden propagarse de forma transversal o longitudinal. En ambos casos, sólo la energía y la cantidad de movimiento ondulatorio se propagan en el medio; ninguna parte del propio medio se mueve físicamente a una gran distancia.. Por tanto, una onda de sonido es una serie de compresiones y enrarecimientos sucesivos del aire. Cada molécula individual transmite la energía a las moléculas vecinas, pero una vez que pasa la onda de sonido, las moléculas permanecen más o menos en la misma posición.

Se puede decir que los ultrasonidos son sonidos (vibraciones mecánicas) que tienen una frecuencia por encima del nivel audible. Al igual que el sonido, los ultrasonidos viajan a través de un medio con una velocidad definida y en forma de una onda, pero, a diferencia de las electromagnéticas, la onda del sonido es un disturbio mecánico del medio mediante el cual se transporta la energía del sonido.

El diagnóstico por ultrasonidos depende del medio físico en el que el sonido se propaga y de cómo las ondas ultrasónicas interaccionan con los materiales que atraviesan, especialmente con las estructuras de los tejidos blandos del cuerpo humano. [3]

III. CIFRADO

El cifrado se usa con la intención de proteger información para evitar que sea accesible por observadores no autorizados, y a la vez proteger estos datos mediante la modificación de un mensaje, de tal forma que sea completamente ilegible a no ser que se posea la clave para reponerlo en su estado original.

El cifrado permite verificar que un mensaje no ha sido modificado intencionadamente por un tercero y asegura la integridad del mismo.

A. Tipos de Cifrado

Actualmente existe el cifrado simétrico, también conocida como criptografía clásica o de llave privada. Este tipo de criptografía es anterior al nacimiento de los ordenadores.

El cifrado asimétrico, también conocida como criptografía moderna o de llave pública. Este tipo de cifrado se desarrolló en los años 70 y utiliza algoritmos matemáticos relacionados con números primos y curvas elípticas.

La Esteganografía, cuando se trata de ocultar información sensible a simple vista contenida en otro tipo de información. Por ejemplo en un archivo gráfico utilizar el bit menos significativo del color de todos y cada uno de los puntos de la imagen para transmitir una información. Alguien que vea la imagen no se dará cuenta de nada ya que el cambio que se produce en la imagen no es significativo.

B. Elementos de los Sistemas de Cifrado

Se llama texto plano al texto que se quiere proteger mediante el uso de técnicas de cifrado. Se denota el conjunto de todos estos textos como “M”. El criptograma representa el texto una vez que ha sido transformado mediante alguna técnica de cifrado. Este texto resulta ilegible a no ser que se conozca la clave para volver a recuperar el texto plano

original. Se denota el conjunto de todos estos textos como "C".

Se denota por cifrado al proceso que transforma un texto plano en un criptograma. El proceso llamado descifrado es el encargado de recuperar el texto plano de un criptograma. Se denota "K" a todo el conjunto de claves que se pueden utilizar para descifrar mensajes utilizando un determinado sistema criptográfico.

El dispositivo de cifrado genera códigos aleatorios, y lo denotaremos como "E", a cualquier dispositivo que transforme un elemento de "M" en un elemento de "C".

Se llama dispositivo de descifrado el encargado de separar la fuente de información con los datos de cifrado, y lo denotaremos como "D", a cualquier dispositivo que transforme un elemento de "C" en un elemento de "M".

El criptosistema, sistema criptográfico o sistema de cifrado al conjunto (M,C,K,E,D).

Tanto los textos planos como los criptogramas están formados por palabras, y estas están constituidas por símbolos. Por ejemplo en la escritura estos símbolos son las letras, números y signos de puntuación.

Se llama alfabetos al conjunto de símbolos utilizados en los textos planos o en los criptogramas. Los símbolos utilizados en los textos planos y en los criptogramas no tienen que ser los mismos. Se denota como $\sum M$ al alfabeto utilizado en los textos planos y $\sum C$ al alfabeto utilizado en los criptogramas. [2]

IV. ALGORITMO MAVG-14

Se propone un algoritmo, denominado MAVG-14 (Miguel Alejos Víctor González -14) para contrarrestar las siguientes situaciones:

a) Los sistemas de autenticación actuales se basan en aumentar la cantidad de bits de cifrado en las comunicaciones para tener mayor seguridad, en este caso se tiene una imagen la cual es muy rica en información y muy difícil de memorizar por el ser humano.

b) El algoritmo tiene la capacidad de seleccionar píxeles específicos de la imagen para evitar un congestionamiento en la red, actualmente una tecnología de transición como este proyecto debe aplicarse realizando mínimos cambios en la infraestructura actual, el ancho de banda de los cajeros automáticos varían de 128 Kbps a 512 Kbps máximo sin importar el medio, ya sea fibra óptica, satelital o microonda.

La congestión de redes es el fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede cursar, es decir que en un sistema de comunicación que soporta actualmente transacciones con tarjeras de banda a 128 bit ingresar repentinamente un sistema de 8Kb produce un colapso, es decir que mientras se procesa una transacción con una Imagen de alto contenido estamos utilizando su equivalente a 68 transacciones con banda magnética.

Realizando esta selección se puede bajar el nivel de información y disminuir la inseguridad del medio de transmisión con el uso software pasivos que pueden capturar las tramas en el momento de la comunicación.

c) Los sistemas actuales de almacenamiento en las tarjetas de crédito envían toda la información, ya sea de la cinta magnética o el chip electrónico para sincronizarse con la base de datos bancaria, lo cual es muy inseguro porque el sistema de autenticación no varía en ningún momento y si capturan la información de la tarjeta de crédito sería peligroso, puesto que estos datos no caducan.

d) El algoritmo posee la capacidad de cambiar el cifrado o el modelo de selección de píxeles dependiendo de los bits menos significativos del identificador de la tarjeta y el identificador del punto de servicio para enviar píxeles específicos y para realizar un sistema más robusto.

Este puede cambiar el comportamiento de autenticación tomando variables dinámicas en el tiempo como el mes y el año al momento de la transacción.

La capacidad de este algoritmo crear una llave inmune a los sistemas actuales de falsificación, su funcionamiento es seleccionar pixeles específicos de la imagen la cual al estar en extensión JPEG (*Joint Photographic Experts Group*) representa un formato digital.

Esta selección de pixeles específicos puede copiar dichas celdas de información dentro del formato JPEG en una matris de 60 por 60 celdas, lo cual genera $5.10x10^{1083}$ combinaciones posibles.

Al seleccionar solo pixeles específicos de la imagen para la autenticación, es necesario que un algoritmo decida cuales son los pixeles que se envían por medio de variables que estén presente siempre en un sistema sin importar la ubicación geográfica ya que un tarjetahabiente siempre está realizando transacciones en distintas ubicaciones.

Es por ellos que las variables escogidas son; el ID (identificador) del cajero, numero de cedula del tarjetahabiente y la fecha, estas variables al estar en formato numérico el algoritmo las toma y las procesa en formato binario, dependiendo de la combinación de 1 y 0 el algoritmo cambia el comportamiento de los pixeles específicos a enviar y de esta forma es inmune a los ataques de clonación tradicionales.

Lo más importante de la variable FECHA, esta garantiza que el algoritmo cambia a medida que pasa el tiempo, lo cual lo

hace recuperarse ante una situación de vulnerabilidad debido a estudios estadísticos en un mismo punto o cajero automáticos, esto ayuda a lo siguiente:

a) Los Hacker se basan en hacer estudios repetitivos a los sistemas para averiguar su comportamiento, en algunos casos esta información puede hacer que un sistema estándar como EMV [4] (Europa Visa Mastercard) a futuro con el paso de los años puede ser vulnerable.

b) Debido a los sistemas estándares siempre tendrán más personas inescrupulosas buscando la forma de vulnerarlo, hay que crear un mecanismo que sea inmune al análisis de proceso estadísticos repetitivos, experiencias pasadas de protocolos estándar vulnerados tenemos, DVD con chip para leer copias, Tarjetas de Chip CANTV, encriptación WEP en Wiffi, tarjetas de crédito con bandas magnéticas entre otros.

c) La variable Tiempo es un factor fundamental en este proyecto, este algoritmo no busca ser mejor que otros si no trabajar de forma paralela de manera que si un protocolo estándar es vulnerado quede un sistema inmune trabajando perfectamente mientras se realicen modificaciones de hardware o software necesarias y de esta forma evitar un fraude financiero.

Se muestra a continuación la Figura 1 el algoritmo el cual explica de forma grafica el proceso de elección de pixeles así como la forma condicional para aprobar o negar transacciones.

V. METODOLOGÍA

El proceso de autenticación por medio de ultrasonido y el algoritmo MAVG-14 debe cumplir una serie de procesos para poder convertir una tarjeta la cual es un material físico, tangible y análogo en un sistema totalmente digital, que pueda funcionar paralelamente con los sistemas actuales, permita ser una opción de tecnología de transición.

Brevemente se describen cinco etapas las cuales muestran el proceso de diseño e implementación del sistema, estas etapas son:

1. Fabricación de la tarjeta.
2. Simulación del ultrasonido.
3. Generación de una imagen.
4. Implementación del algoritmo.
5. Codificación y decodificación.

En la primera etapa se escogen los materiales para elaborar la tarjeta e ingresar las virutas de metal dentro del plástico de forma aleatoria, en una zona en la cual no se tenga problema con los espacios ya utilizados por los métodos de autenticación tradicionales, estas virutas van a ser movidas con la ayuda de un campo magnético generado por un yugo de TV para alojar de manera aleatoria y sin un patrón definido.

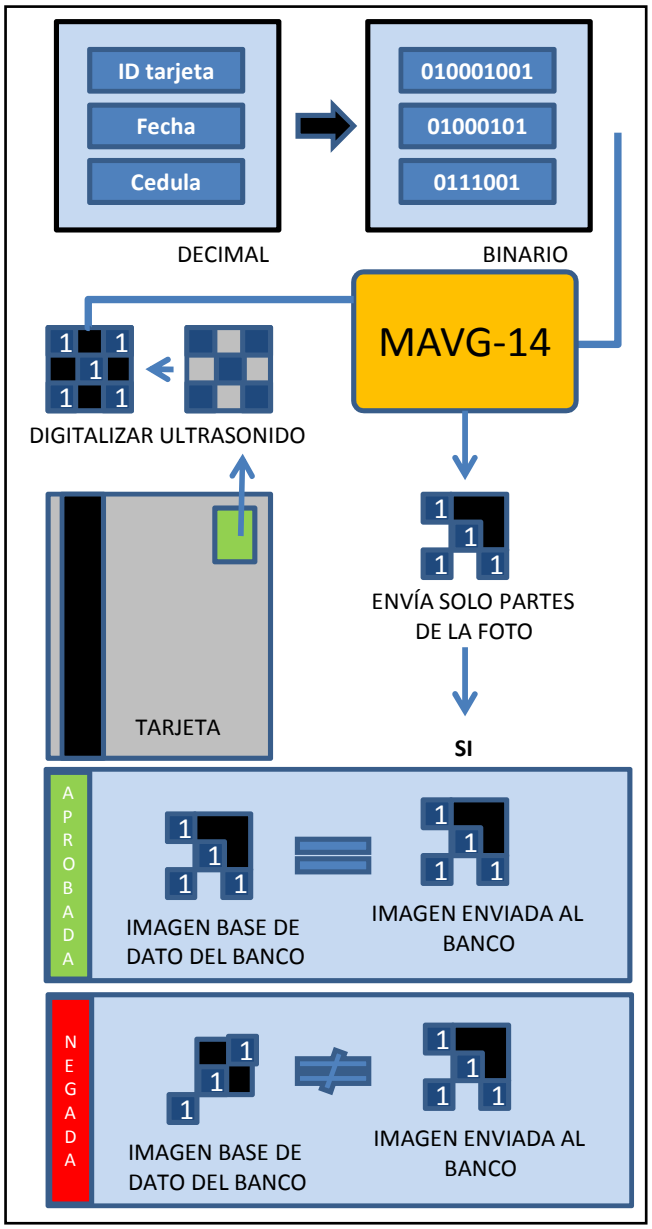

FIG. 1 Funcionamiento del Algoritmo MAVG-14

En la segunda etapa, se procede a la simulación del ultrasonido para generar señales, las cuales serán captadas en tiempos distintos debido a la impedancia acústica de los elementos que se encuentran dentro de la tarjeta.

Por medio del eco de los diferentes tiempos de reflexión de la señal se discriminan los tipos de elementos que integran la tarjeta de crédito, y dependiendo de las variables arrojadas por la discriminación del proceso anterior, se procede a generar una imagen en formato JPEG (Joint Photographic Experts Group**)** de dos colores, un color representando las zonas donde se encuentren las virutas de metal y el otro donde se encuentra solo el plástico.

ISBN: 978-980-7185-1

Después se implementa el algoritmo MAVG-14 con sus funciones básicas las cuales van a transmitir solo píxeles específicos de manera dinámica. Luego de esto, se toman las variables caducas en el tiempo para aplicarle la última etapa de cifrado y descifrado de los datos antes de transmitir a la capa de presentación del modelo OSI.

1. *Fabricación de la tarjeta:*

La tarjeta debe cumplir con las medidas de los estándares actuales los cuales comprenden 8,5 cm de alto por 5,5 cm de ancho y 0,18 cm de espesor. Posee una banda magnética del lado derecho y en algunos casos un microchip, como se puede observar en la Fig. 2.

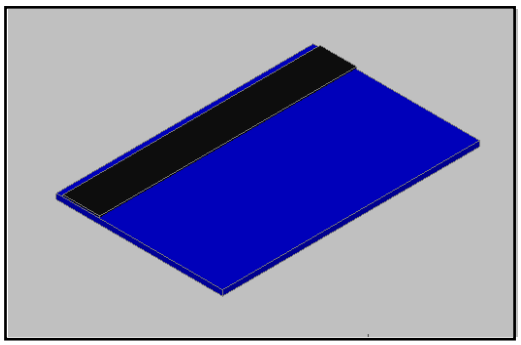

FIG. 2. Tarjeta de crédito

Los pasos para la fabricación de la tarjeta son los siguientes:

- Se elije un área de la tarjeta de 121,07 mm por 207,3 mm la cual no interfiere con ninguno de los dispositivos de seguridad actuales de las tarjetas de crédito. A continuación se muestra en la Fig. 3 las medidas a utilizar.

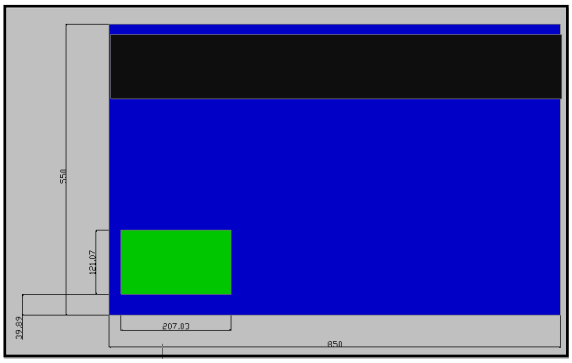

FIG. 3. Medidas del área a utilizar

A esta área de la tarjeta, durante el proceso de fundición, se le agregan entre 100 a 360 virutas de metal, y como el plástico se encuentra en el estado liquido, estas quedaran incrustadas dentro del mismo. Los efectos del campo magnético que se generan en la parte inferior de la tarjeta, con el uso del yugo de TV, van quedando dispuestas las virutas de manera casi paralela al ancho de la tarjeta, como se puede verse a continuación en la Fig. 4.

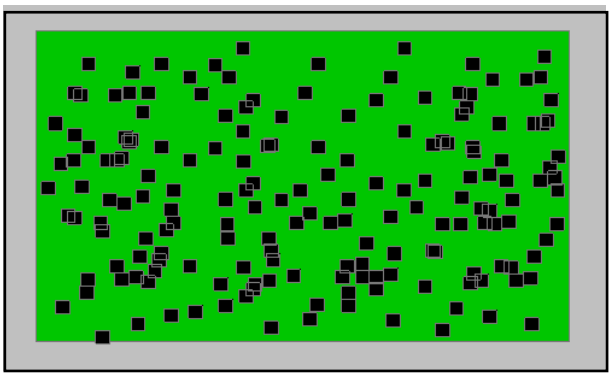

FIG. 4. Ingreso de partículas de metal a la tarjeta

Después que la tarjeta contiene las virutas de metal, se le coloca un recubrimiento de plástico sobre las partículas para asegurar que ninguna se encuentre en contacto con las condiciones medioambientales, este recubrimiento impide la visibilidad total de las partículas por el ojo humano.

Cabe destacar que se utilizó un dispositivo tipo molde, ubicado en la parte superior de la tarjeta al momento de la fundición y cumple la función de seleccionar el área donde las partículas de metal son ingresadas.

Se espera de 10 a 15 minutos para que el plástico regrese a su estado normal (sólido) y para que la tarjeta sea procesada por el ultrasonido, tal como se describe a continuación.

2. *Simulación del Ultrasonido*

Las ondas sonoras viajan en diferentes velocidades dependiendo del medio donde se desplazan, la banda ultrasónica comprende frecuencias entre 20 KHz y 20000 KHz. Para efectos del presente proyecto, se utiliza una señal acústica de 800 KHz para obtener resultados sobre el análisis de los materiales dentro de la tarjeta. [5]

Se dispuso de un palpador de silicona conectado entre el transductor de ultrasonido y la tarjeta de identificación o de crédito, el palpador de silicona brinda un medio de transmisión más efectivo que el aire libre a éstas frecuencias.

Cabe destacar que la tarjeta está diseñada con dos materiales, el primero es plástico y el segundo son partículas de acero con las siguientes velocidades de propagación. [6]

Acero: 4700 a 5100 m/seg.
Plástico: 40 a 150 m/seg.

Como el sistema trabaja por medio de respuestas de eco, es decir el tiempo que tarda la señal en ser enviada y recibida, se puede analizar estas señales y determinar la ubicación de las partículas de acero dentro de la tarjeta.

ISBN: 978-980-7185-1

En este sentido, la velocidad de propagación de las señales sobre el acero y el plástico está condicionada a una impedancia acústica muy diferentes entre ellas, lo que origina diferentes tiempos de retorno o de eco y de esta forma poder discriminar por medio de una matriz de 60 por 60 celdas los diferentes puntos los cuales cubren el área durante la fabricación de la tarjeta.

Esta adquisición de datos en la matriz antes mencionada se logra por medio de una empalmadora de 4 cm por 4 cm con una distancia focal de 5 cm el cual por la parte más angosta se conecta al transductor y por la parte inferior se realiza el contacto con la tarjeta de crédito, después esta matriz de 60 por 60 con diferentes valores de retorno debe ser analizada y convertirla en una imagen formato JPEG.

La formulación matemática es la siguiente:

- F= 800 KHz
- D_1= Distancia Metal
- D_2= Distancia no metal
- E_1= Primer eco de Respuesta
- E_2= Segundo eco de Respuesta
- $E_1 = D_1 + D_1$

Corresponde a dos D_1 por la razón de que la señal viaja y rebota, es decir, el primer tiempo que tarda la señal en llegar a la tarjeta y el segundo tiempo que tarda en devolverse.

$E_2 > 2(E_1)$

Corresponde valores mayores de dos E_1, por la razón de que el ultrasonido donde no se encuentre material rebotará, y el valor de retorno será mayor que el valor donde hay partículas de metal, esto se produce a causa de D_2.

3. *Generación de la imagen*

Para que las señales o la información se pueda adaptar a un medio debe existir un procesamiento digital de la misma, en el caso de la matriz de 60 por 60, cada celda debe ser analizada de forma independiente es decir que se debe analizar 3600 veces.

Cada celda debe ser discriminada en dos valores: E_1 y E_2. Teóricamente, como se tiene una imagen de 60 por 60, cada celda de la matriz formara un píxel con un color en el cual se muestra un color blanco o negro, el blanco corresponde a las áreas donde hay metal y el negro donde no existe. [7]

De esta forma, se aplica la siguiente formulación:

- Color Blanco: Donde E_1 esté presente.
- Color Negro: Donde E_2 esté presente.

Así se logra obtener una imagen de dos dimensiones, generada por el ultrasonido, con la característica de ser una imagen de dos colores que está dentro de una tarjeta, es difícil que el ojo humano o una cámara espía la pueda captar.

Seguidamente, se obtiene una imagen al que se le aplicará el algoritmo que tiene por nombre MAVG-14.

4. *Implementación MAVG-14*

La imagen generada es muy rica en información y posee la desventaja de congestionar la red al momento de ser transmitida, el algoritmo se fundamenta en seleccionar píxeles específicos de la imagen dependiendo de las variables en las cuales se denota:

- ID Cajero
- Fecha
- Cédula del usuario

Es decir, el algoritmo se comportará dependiendo de la cédula del usuario, identidad del telecajero y la fecha, por dos principales razones:

En primer lugar, para evitar que el sistema tenga una sobrecarga en la red debido a la cantidad de información que posee la imagen, una forma de ver este comportamiento del algoritmo es tomar en referencia una foto de una casa y solo transmitir el pedazo de la puerta, una ventana y el color de la pintura, para luego compararla con la base de datos que se encuentra en otro lugar y analizar las características que se transmitieron de la foto son iguales a la que el usuario tiene almacenada en su base de datos.

En segundo lugar, el algoritmo cambia dependiendo del las variables antes mencionadas por la razón de que si en algún momento una trama es analizada y descifrada, este análisis no funcionara en otro punto de venta y a futuro perderá vigencia en el mismo punto de venta a un mes de transcurrida la captura de los datos.

Siguiendo con el ejemplo anterior de la foto de la casa, el sistema puede elegir que parte de la foto quiere mandar y si en algún caso averiguan el color de la puerta o el tamaño de la ventana, este no servirá para otro punto transmisión (en nuestro caso otro punto de venta), y si desean fabricar una tarjeta de crédito con las características físicas de la original esta no servirá de nada el próximo mes porque el algoritmo en vez de mandar el tamaño de la puerta transmitirá el tamaño de una teja.

Esto hace que el algoritmo sea muy robusto y como se maneja en la capa de aplicación del modelo OSI puede ser utilizado por cualquier sistema de comunicación sin importar los enlaces o los protocolos de enrutamiento.

5. *Codificación y decodificación*

La tarjeta antes de ser entregada al cliente debe ser analizada por medio de un ultrasonido y registrar la foto en

una base de datos con información adicional como la cédula del cliente y el número de la tarjeta.

Las variables se conocen tanto en el cajero como en la base de datos, por esta razón el sistema emplea un esquema de cifrado híbrido, aplica cifrado simétrico cuando la imagen se encuentra en dos lugares, la cual es comparada, y el cifrado asimétrico porque la información cifrada varía de acuerdo a las variables dinámicas antes mencionadas y se transporta dentro de la carga útil.

Por esta razón, el sistema propuesto es robusto, el autor se reserva el código fuente y solo adjunta la aplicación con las librerías a utilizar.

VI. CONCLUSIONES

El diseño de este proyecto busca la propuesta de un nuevo modelo de autenticación para las tarjetas de crédito, proporcionando una tecnología de transición que con varias modificaciones pueden operar conjuntamente con los dispositivos y métodos actuales de las tarjetas de créditos con el uso de las bandas magnéticas y los microchip.

El nuevo modelo de autenticación de tarjetas de crédito, formado por la tarjeta de plástico con las partículas de metal es inmune a las descargas eléctricas, campos magnéticos, estática, y pueden perdurar más que los sistemas tradicionales de autenticación de las tarjetas de crédito actuales.

Las tarjetas de crédito funcionan como el transporte de la información que posee la cinta magnética así como la información que posee en relieve la cual identifica al usuario, la cual es muy fácil de memorizar por terceros, con el nuevo sistema la tarjeta será única y dejara de ser un transporte de un método de autenticación debido a que la información estará dentro de ella y no en un borde.

Este sistema es inmune a la falsificación causada por la clonación de cintas magnéticas, así como los fraudes causados por revelación de contraseña a causa de cámaras ocultas en los puntos de ventas por parte de personas inescrupulosas.

La característica del algoritmo, de aplicar un modelo de cifrado dinámico y transparente al usuario, logra hacer un sistema robusto que puede ser utilizado por muchos años y no funcionan de la misma forma en un punto de venta.

Esta característica anterior es muy importante porque si en algún momento terceros captan la información por medio de software Sniffer, deben analizar de donde fueron escogidos los píxeles, lo cual es algo muy complicado debido a los métodos matemáticos implementados en el algoritmo y deben hacerlo antes de que culmine el mes porque para el siguiente no serán los mismos píxeles.

El otro inconveniente de los falsificadores es fabricar la tarjeta y colocar las virutas del metal en el punto exacto lo cual es muy poco probable que lo logren en 30 días.

El sistema planteado en el proyecto se basa en integrar diferentes tecnologías para la resolución de un problema el cual afecta a miles de personas a nivel mundial, estas tecnologías están presentes en la industria y han dado resultados factibles en el caso del ultrasonido.

El costo de estudio, estandarización e implementación del sistema de ultrasonido para una institución financiera es costoso y se puede realizarse a largo plazo, caso contrario de utilizar el algoritmo MAVG-14 tomando valores de una fuente de almacenamiento digital como el estándar EMV, el cual puede soportar la imagen JPEG dentro de su memoria, en este caso el algoritmo tomaría dichos pixeles en entornos $DIGITAL_{(chip\text{-}EMV)}$ - $DIGITAL_{(algoritmo)}$ y no ANALÓGICO $_{(tarjeta\ con\ metal\ y\ plástico)}$ -$DIGITAL_{(algoritmo)}$ lo cual lo hace más lento debido que el ultrasonido debe procesar algo físico como una tarjeta con diferentes impedancia acústica para convertir esos valores a digital.

VII. REFERENCIAS BIBLIOGRÁFICAS

[1] Borjas G. Sastres (2007), "**Sistemas de Percepción: Ultrasonido en Aplicaciones Industriales**".
[2] Raúl S. Peláez (2002), "**Análisis de los Protocolos de Seguridad TCI/IP y sus Aplicaciones**".
[3] Ricardo Echevarría (2002), "**Ultrasonido Laboratorio de Ensayos No Destructivos**", Universidad Nacional del Comahue, Facultad de Ingeniería.
[4] "**EMV Integrated Circuit Card Specifications for Payment Systems. Book 1: Application Independent ICC to Terminal Interface Requirements**" Version 4.2, June 2008.
[5] Ricardo Echevarría (2006), "**Laboratorio de Ensayos no Destructivos de la Universidad de Comahue: Ultrasonido**".
[6] Lisa María Jaramillo (2007), "**Ultrasonido: Imágenes Ultrasónicas**". Grupo de Investigación en Ingeniería Biomédica EAI-CES (GIBEC), Colombia.
[7] Lisa María Jaramillo, Sirley Marín y Catalina Pineda, "**Programa de Ingeniería Biomédica**". Grupo de Investigación en Ingeniería Biomédica EAI-CES (GIBEC), Colombia.
[8] Gerardo E. Romero (2005), "**Aplicaciones de NIST para la Extracción de Características de Huellas Dactilares**". México.