ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica
ISSN: 2007-5448
recibe@cucei.udg.mx
Universidad de Guadalajara
México

Caballero Hernández, Héctor; Muñoz Jiménez, Vianney;
Ramos Corchado, Marco A.; Romero Huertas, Marcelo

Algoritmo para transmisión de información segura en dispositivos NFC

ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, vol. 7, núm. 2, 2018, Noviembre-, pp. 47-64
Universidad de Guadalajara
México

Disponible en: https://www.redalyc.org/articulo.oa?id=512257487003

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

Sistema de Información Científica Redalyc
Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Recibido 11 Sep 2018
Aceptado 29 Sep 2018
ReCIBE, Año 7 No. 2, Noviembre 2018

Algoritmo para Transmisión de Información Segura en Dispositivos NFC

Algorithm for secure information transmission in NFC devices

Héctor Caballero Hernández[1]
hcaballeroh240@profesor.uaemex.mx

Vianney Muñoz Jiménez[1]
vmunozj@uaemex.mx

Marco A. Ramos Corchado[1]
maramosc@uaemex.mx

Marcelo Romero Huertas[1]
mromeroh@uaemex.mx

[1]Dept. Posgrado en Ciencias de la Ingenieria
Universidad Autónoma del Estado de México, México.

Resumen: En este artículo se presenta un nuevo algoritmo para la transmisión de información segura en dispositivos NFC (Near Field Communication), debido a la facilidad de uso de esta tecnología, se han desarrollado aplicaciones para la adquisición de bienes y servicios, así como implementaciones de redes de sensores en ecosistemas naturales, aplicaciones médicas, entre otras. Por lo tanto, es de gran importancia implementar mecanismos de seguridad que permitan el resguardo de información transmitida vía NFC. El algoritmo que se presenta, manipula técnicas de esteganografía combinadas con técnicas de criptografía para garantizar la transmisión de información segura en los dispositivos NFC.

Palabras clave: Criptografía, esteganografía, Vernam, Arduino, matrices.

Abstract: This article presents a new algorithm for the transmission of secure information in NFC (Near Field Communication) devices, due to the ease use of this technology, applications have been developed for the acquisition of goods and services, as well as network implementations of sensors in natural ecosystems, medical applications, among others. Therefore, it is of great importance for implement security mechanisms that allow the protection of information transmitted via NFC. The algorithm presented consists of manipulating steganography techniques combined with cryptography techniques guarantee the transmission of secure data in NFC devices.

Keywords: Cryptography, steganography, Vernam, Arduino, matrix.

1. Introducción

El uso de estándares inalámbricos permite la comunicación entre dispositivos electrónicos para facilitar las actividades humanas en distintos ámbitos (Coskun, Ok & Ozdenizci, 2012). Hoy en día se cuenta con una gran cantidad de estándares para la transmisión inalámbrica de datos y con ello atender necesidades específicas, tales como: alta velocidad de transferencia de datos en corta o larga distancia, con o sin prioridad al consumo energético, transmisión segura de datos, entre otras.

Una de las aplicaciones específicas para la transmisión de datos en corta distancia es NFC (*Near Field Communication*), esta tecnología permite el envío y recepción de información en distancias cortas con bajas tasas de datos, lo cual la hace ideal para transmitir información en aplicaciones de comercios, medicina, lectura de códigos, etc. Debido a su concepción original la tecnología NFC no fue pensada para soportar de forma nativa algún protocolo de seguridad, lo cual le hace susceptible a la manipulación intencional de terceros o al robo de datos.

En este artículo se presenta una propuesta innovadora para la transmisión de información segura mediante la tecnología NFC, aplicando la combinación de técnicas de criptografía y esteganografía para garantizar la seguridad los datos que se transmiten canales de comunicación. Adicionalmente se propone la generación de un análisis léxico de las cadenas de texto que se transmitan con NFC para tarjetas de almacenamiento de datos.

1.1 Conceptos teóricos

NFC es una tecnología de comunicación tipo semi-dúplex de corto alcance, fue desarrollada por Philips y Sony en 2002 para transmisión de datos sin contacto, y esta basada en el acoplamiento inductivo entre dispositivos. NFC, generalmente se ha utilizado para sustituir códigos de barras, transferencia de datos en teléfonos inteligentes (Akyildiz, Su, Sankarasubramaniam & Cayirci, 2002), entre otros, así como formar redes de sensores como son WSN (*Wireless Sensor Networks*), y se encargan, por ejemplo de monitorear incendios forestales mediante una red inalámbrica de sensores y actuadores WSAN (*Wireless Sensor and Actuator Network*). El estándar NFC maneja una frecuencia de transmisión de 13.56 MHz, con velocidades de transferencia de 106, 212, 424 y 848 Kbit/s y está especificado en la norma ISO/EC 18000-3.

NFC normalmente maneja tres tipos de dispositivos, estos son: teléfonos inteligentes, etiquetas (*tags*) y lectores, los cuales cumplen con tres tipos de funcionamiento: lector/escritor, *peer-to-peer* y emulación de tarjeta. La Figura 1 ilustra los tres modos de transmisión (funcionamiento) del NFC (Coskun, Ok &

Ozdenizci, 2013), resaltando que el último modo de funcionamiento consiste en establecer comunicación entre un teléfono inteligente y un lector NFC.

La tecnología NFC incorpora los modos de comunicación activo y pasivo, en el primero, ambos dispositivos usan su propia energía para generar un campo de Radio Frecuencia (RF) para transmisión de datos, en el segundo modo de comunicación, el primer dispositivo inicia generando el campo RF, mientras que el segundo dispositivo hace uso de la energía que ya esta generada por el primer dispositivo (ECMA, 2018).

La técnica de modulación empleada en un dispositivo activo o pasivo es ASK (*Amplitude Shift Keying*) con codificación Manchester o Miller. Algunos de los sistemas de codificación que se emplean además de ASK son: sin retorno a cero (NRZ-L) y PSK (*Phase Shift Keying*) (Yi & Saniie, 2013).

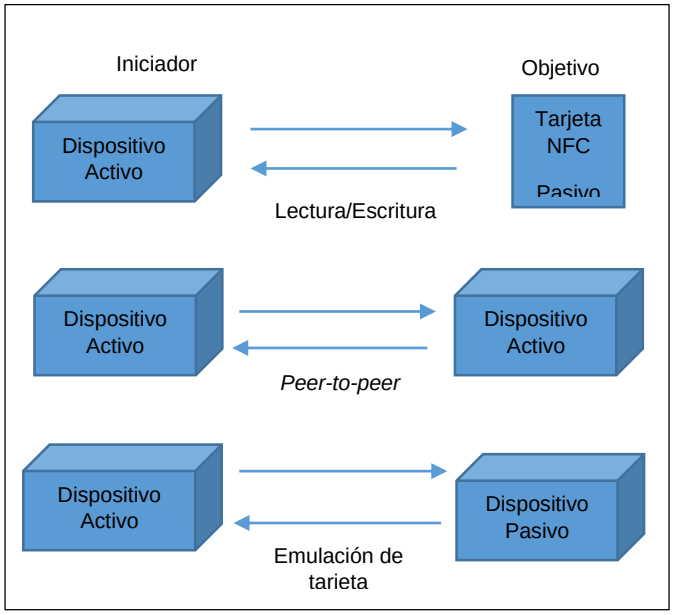

Figura 1. *Modos de transmisión de NFC.*

Para garantizar la transmisión de información de forma segura, en telecomunicaciones generalmente se emplean técnicas de criptografía y esteganografía. La esteganografía se define como un conjunto de técnicas para ocultar la información. Los elementos más importantes que se utilizan en esteganografía son: el objeto de cubierta, el estego-objeto y el objeto a ocultar. El objeto de cubierta es el medio en el que se embeberá la información a transmitir. El estego-objeto, se obtiene al combinar el objeto de cubierta con el mensaje oculto y finalmente, el objeto a trasmitir que representa la información que debe viajar sin ser descubierta (Choudry & Wanjari, 2015).

En el área de la esteganografía, se utilizan técnicas o métodos en el dominio del espacio y frecuencial. Los métodos espaciales son responsables de generar modificaciones sobre los bits del objeto de cubierta para incrustar el objeto a transmitir (la información) y así dar origen al estego-objeto. A continuación se enlistan las técnicas más empleadas de esteganografía:

- Bit menos significativo (LSB, por sus siglas en inglés)
- Diferenciación del valor del píxel (PVD, por sus siglas en inglés)
- Método de incrustación de datos basado en los bordes (EBE, por sus siglas en inglés)

De la lista anterior, la técnica más explotada es la LSB, consiste en insertar información a través de la modificación del bit menos significativo que conforman el objeto de cubierta, con la finalidad de interferir lo menos posible con su calidad (Yi & Saniie, 2013). PVD es otra técnica ampliamente utilizada para esteganografía, permite seleccionar dos píxeles consecutivos para insertar datos, los datos insertados se obtienen cuando se determina la diferencia escalar entre dos píxeles consecutivos correspondientes a un área de borde o a una área lisa de una imágen (Dhruw & Tiwari, 2016).

Los métodos basados en el dominio de la frecuencia emplean transformaciones del espacio utilizando funciones tales como (Vaithiyanathan, Karthikeyan, Anischin, Reddy, Priyanka & Abinaya, 2015), (Djebba, Ayad, Meraim & Hamam, 2012), (Di Laura, Pajuelo & Kemper, 2016):

- Técnica discreta de transformación de Fourier (DFT, por sus siglas en inglés)
- Técnica de transformación discreta del coseno (DCT, por sus siglas en inglés)
- Técnica de transformación discreta de Wavelet (DWT, por sus siglas en inglés)

Las técnicas de esteganografía actualmente se aplican para archivos de video (Choudry & Wanjari, 2015), comunicación de voz IP (Tian, Qin, Huang, Chen & Wang, 2015), transmisión de datos en teléfonos inteligentes (Chappleand & Solomon, 2005), entre otros.

Por otro lado, la criptografía es la rama de la seguridad informática con mayor auge en la actualidad, debido a que permite transmitir información de forma eficiente y eficaz, se basa en los principios de confiabilidad, autenticación, integridad de datos, no rechazo y control de acceso (Delfs & Helmut, 2007). La criptografía refiere a una serie de procesos para transformar los mensajes en otros, pero sin perder la lógica del mensaje, su etimología proviene de la palabra griega *Kryptos*, que significa oculto, y *graphikos*, que significa escribir.

En criptografía existe el texto claro, el cual representa al mensaje original y *cipher* es el algoritmo utilizado para cifrar el mensaje (Childs, 2000). Las técnicas criptográficas que actualmente son mas extendidas son:

AES (*Advanced Encryption Standard*). Es un estándar de encriptación de acceso público, se basa en sustituciones, permutaciones y transformaciones lineales, cada una ejecutada en bloques de datos de 16 bytes. Esas operaciones se repiten varias veces, y se denominan rondas. Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos (Dworkin, Barker, Nechvatal, Foti & Bassham, 2016).

RSA (*Rivest Shamir Adleman*). Trabaja con dos claves, una pública y una privada. Ambas claves trabajan como complementarias entre sí. La clave privada no puede calcularse a partir de la clave pública, ésta está generalmente disponible para el público (Rivest, Shamir & Adleman, 1978).

Tanto la criptografía como la esteganografía se pueden combinar para generar comunicación entre sistemas, ya sea utilizando técnicas espaciales como LSB en combinación con AES y RSA (Mishra & Tripathi, 2015), o basadas en el dominio de la frecuencia que combinen técnicas como DWT y RSA (Tripathi, Singh & Singh, 2016). Cualquiera de ellas puede ser aplicadas en archivos multimedia que se reproducen en computadoras y teléfonos inteligentes (Mazurczyk & Caviglione, 2014), con la finalidad de aumentar la complejidad matemática de la criptografía para evitar que la información sea entendida en forma clara (desde la perspectiva de un atacante) y la imperceptibilidad que provee la esteganografía, para evitar que un atacante se de cuenta de la existencia de un mensaje oculto en un objeto.

1.2 Revisión del estado del arte

El incremento de la aplicación de la tecnología NFC ha despertado el interés de investigadores para formular técnicas y métodos que garanticen la confiabilidad de este tipo de tecnología, a continuación se presentan investigaciones que han abordado con distintas técnicas la transmisión segura de información con dicha tecnología.

En Dragan (2015) se propone un nuevo modelo para incrementar la seguridad en dispositivos NFC mediante un sistema de encriptación, empleando un código de autenticación con SHA1 (*Secure Hash Algorithm* 1), AES y ECB (*Electronic Code Book*). Las pruebas se ejecutaron en el sistema operativo Android de forma exitosa.

En el trabajo de Sankpal, Mundhe, Kotwal, Machale & Malchikare (2017) se propone una metodología en la cual se genera un control de permisos de acceso, y posteriormente, la información se oculta embebiendo el código de acceso en

una fotografía que está almacenada en un teléfono celular. El hardware empleando es un smartphone con sistema operativo Android y un Arduino para el control de lectura de tarjetas NFC.

Por otro lado Kim (2016) propone un sistema de autenticación que utilice un algoritmo simétrico de cifrado, y un código de detección de modificaciones. El algoritmo de cifrado es AES, tanto el código de cifrado como el de autenticación se envían de forma independiente. El sistema propuesto utiliza un teléfono inteligente con un lector y grabador de tarjetas NFC y un estego-objeto para acceder a los datos grabados en la tarjeta. De forma similar en Muke, Shinde, Mistry & Jawalkar (2015) proponen un sistema de autenticación para acceso, empleando el ocultamiento de claves en imágenes a escala de gris mediante esteganografía en combinación de teléfonos inteligentes con la capacidad de manejar NFC.

Schürmann, Dechand & Wolf (2017) implementaron criptografía para la transmisión de información con NFC mediante Android, además de emplear criptografía de clave pública. Con la arquitectura de clave pública lograron diseñar un sistema al cual pudieran acceder un máximo de 100,000 usuarios, los cuales pueden enviar correos electrónicos, mensajes y administración de contraseñas a través de tarjetas NFC empleando un sello de anillo. El sistema propuesto fue evaluado en una empresa para medir la facilidad de configuración y el uso de las tarjetas NFC en un ambiente real con cuarenta participantes, los resultados obtenidos fueron exitosos.

Kavya, Pavithra, Rajaram, Vahini & Harini (2014) presentan un estudio sobre las vulnerabilidades de NFC, obteniendo como resultado los elementos del sistema que deben de analizarse, como es el caso del mecanismo de modulación de la onda que se genera en el dispositivo para aprovechar de forma satisfactoria las técnicas de cifrado.

Haselsteiner & Breitfub (2016) analizan los tipos de ataques que pueden ser efectivos para NFC, tales como: denegación de servicio, alteración de las codificaciones Miller y Manchester empleadas en ASK y captación de señal con otro dispositivo receptor. De acuerdo con su investigación, los ataques *man in the middle* no son efectivos debido a las cortas distancias que maneja esta tecnología y la velocidad a la que se envían los datos. Concluyen que es conveniente emplear técnicas de claves de autenticación, así como los mecanismos de emparejamiento y cifrado para establecer conexiones seguras que no demanden grandes cantidades de energía y procesamiento.

2. Metodología propuesta

En esta investigación se propone un nuevo algoritmo para transmisión de datos seguros para la tecnología NFC. El Algoritmo 1, consiste en generar una distribución de datos a través del reordenamiento del alfabeto extraído de las cadenas de texto que se deseen almacenar. Cada conjunto de símbolos únicos es almacenado en matrices cuadradas, las cuales se guardan en una memoria, cuyo acceso a sus localidades es a través del NFC. El Algoritmo 1 propuesto se especifica a continuación.

Algoritmo 1 Distribución de símbolos y reglas en memoria
1. Leer la cadena *C* a insertar 2. Extraer los símbolos de *C* 3. Introducir el texto en una matriz cuadrada cuyo número base se aproxime a la longitud de la cadena de texto *L(C)* 4. Generar un número de matrices igual a la cantidad de símbolo obtenidos de la cadena *C* 5. Insertar únicamente un sólo tipo de símbolo por matriz representado por *1* o *0* 6. Generar el mapeo de matrices 7. Grabar cada matriz en la tarjeta NFC 8. Cifrar las reglas de extracción 9. Grabar las reglas de extracción 10. Finalizar secuencia

El proceso propuesto en el Algoritmo 1 permite distribuir la información extrayendo los símbolos de una cadena de texto como se observa a continuación en el ejemplo del Cuadro 1.

Cadena de texto: Prueba de inserción
Alfabeto obtenido: P,r,u,e,b,a, ,d,i,n,s,c,o,´
Longitud de la cadena: 19
Cantidad de elementos del alfabeto: 14
Matriz cuadrada de 5x5: 25 celdas

Cuadro 1. *Ejemplo de distribución de información.*

De acuerdo con los datos que se presentan en el Cuadro 1, la información estará distribuida en una matriz cuadrada (primera fase), como se muestra en la Figura 2, siendo de 5x5 celdas, aunque los últimas localidades de la matriz no se empleen, una matriz de 4x4 no sería suficiente para almacenar los datos de la cadena.

P	r	u	e	b
a		d	e	
i	n	s	e	r
c	i	o	‘	n

Figura 2. *Distribución de información en una matriz cuadrada.*

En la Figura 3 se puede observar que se forma una matriz por cada conjunto de símbolos únicos (por cada símbolo del alfabeto), para este ejemplo, el primer símbolo es “P” y se le asigna su matriz de 5x5, posteriormente se ha tomado el símbolo “r” y se asigna de igual forma su matriz de 5x5, lo mismo con el símbolo “u”. Observando el contenido de las matrices existe un sólo tipo de símbolo, además de que la referencia de ubicación de lo símbolos con respecto a la matriz de la primera fase se mantiene.

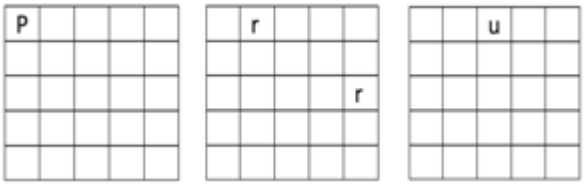

Figura 3. *Distribución de datos en matrices.*

La memoria de una tarjeta NFC se mapea en su totalidad para almacenar los símbolos en sus espacios correspondientes, y al momento de realizar su escritura, todos los símbolos son sustituidos por un sólo símbolo el cual puede ser “1” o “0” para evitar que se identifique el tipo de dato almacenado. La Figura 4 muestra gráficamente lo descrito anteriormente.

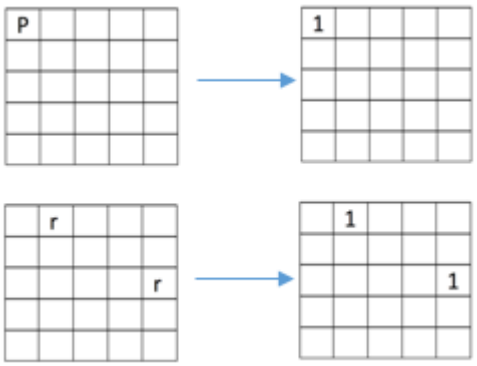

Figura 4. *Asignación de valores para cada matriz.*

Siguiendo las indicaciones del Algoritmo 1, se generan las reglas de extracción, las cuales son la representación de los datos almacenados, para ello se selecciona una zona de memoria de la tarjeta para almacenar los símbolos, estos deben de estar cifrados, y el orden de almacenamiento de los símbolos determina la secuencia de las matrices en que fueron insertadas. El dispositivo encargado de generar tanto el proceso de escritura y lectura de datos de la tarjeta deberá contener el alfabeto ASCII para interpretar los símbolos y su cifrado.

En esta propuesta se utiliza el cifrado (Vernam, 1926) para codificar el alfabeto, el cual consiste en convertir el mensaje original en binario y realizar una operación XOR con una palabra clave, la cual está también en binario, al final la cadena resultante es el mensaje cifrado. La palabra secreta es la cadena de identificación (UID) de la tarjeta NFC (todas las tarjetas cuentas con un número de identificación), además este identificador único, al ser una cadena alfanumérica, puede ser procesada por una operación de permutación, la cual este programada en el dispositivo encargado de procesar el Algoritmo 1, aumentando la complejidad de extracción de datos.

El proceso de recuperación de la información de la tarjeta NFC consiste en leer los datos en el área reservada para el alfabeto (AMR), posteriormente a la obtención de la cadena del área reservada (CAR) se procede a leer la cadena de identificación de la tarjeta (UID). A la cadena obtenida, se le aplica una función de permutación de datos (determinada por el usuario) y se realiza el proceso inverso de Vernam, para obtener los símbolos que se han empleado. Al obtener el alfabeto del mensaje original, se genera el mapeo de la memoria para reconstruir las matrices, las cuales están distribuidas a lo largo de la memoria, además de omitir la zona que está reservada para el alfabeto, una vez reconstruidas las matrices, se sustituyen los símbolos que contienen el símbolo correspondiente con base al alfabeto obtenido. Al finalizar el proceso se superponen las matrices y se extrae el texto, el cual fue distribuido como en el ejemplo de la Figura 2. En este proceso, la fase de esteganografía se puede

observar en la lectura de los símbolos que son representados por 0 o 1, dado que es la unidad mínima de representación en sistemas computacionales, y su impacto sobre la memoria de la tarjeta es mínima debido a que lo ocupan un bit, y se aplica el principio del bit menos significativo (LSB). La parte del cifrado se observa en la técnica Vernam, en donde el proceso de transformación del mensaje original es transformado por operaciones XOR. El proceso anteriormente descrito se ilustra en la Figura 5.

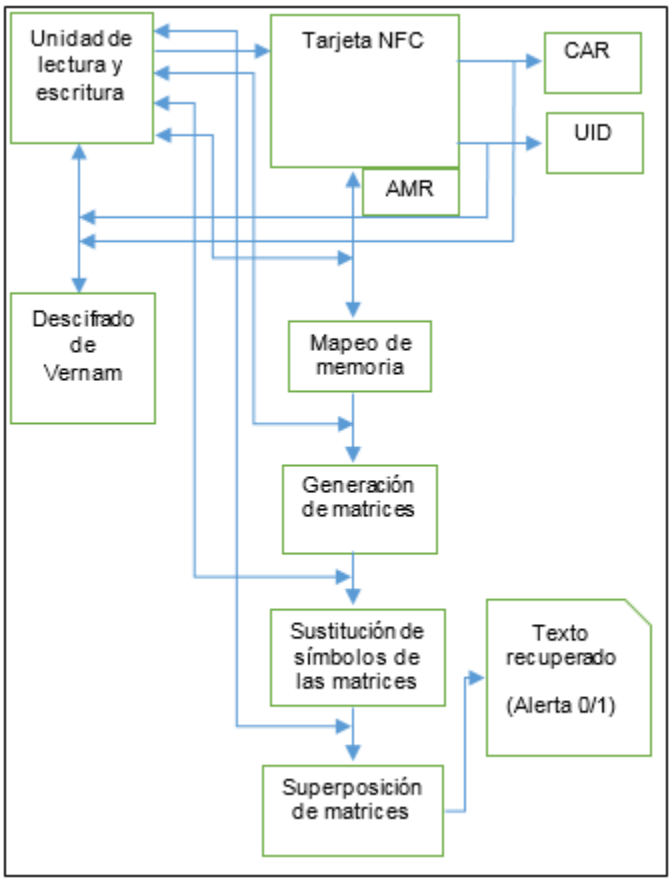

Figura 5. *Proceso de extracción de datos de memoria.*

Si el proceso de extracción no se concluye exitosamente, se envía una alerta indicando que existe modificación sobre los datos extraídos. Las condiciones de un fallo implican que los símbolos se superpongan en la misma posición al momento de generar el traslape de todas las matrices, o bien, cuando se detecta un símbolo distinto a 0 o 1.

Para esta propuesta el Algoritmo 1 se codificó en un Arduino Mega para corroborar su funcionamiento practico. Al Arduino se le ha conectado un módulo PN532 para lectura y escritura de tarjetas NFC, este dispositivo puede realizar las acciones de escritura, lectura y verificación de integridad de los sectores de la memoria. La elección del Arduino para ejecutar las tareas de procesamiento

se debe a que el sistema sólo ejecutará operaciones de lectura y escritura sobre tarjetas NFC, además del bajo consumo energético que presenta (puede trabajar con baterías de 3v y 5v), además es una plataforma electrónica de bajo costo, multiplataforma y de código fuente abierto. El módulo PN532 es un hardware ampliamente utilizado para este tipo de tareas por lo tanto presenta fiabilidad para ejecutar operaciones de lectura y escritura de dispositivos NFC. La combinación de ambos dispositivos cumple con el objetivo de implementar el Algoritmo 1 de seguridad propuesto en este trabajo. El diagrama general de los componentes electrónicos se muestra en la Figura 6.

Figura 6. *Diagrama de distribución de componentes.*

3. Análisis de resultados y discusión

Para validar los resultados de la propuesta, el Algoritmo 1 se implemento en un Arduino Mega, el cual es fue programado mediante un equipo Macbook Air con sistema operativo macOS High sierra versión 10.13.6. Las pruebas realizadas están orientadas a corroborar la eficacia del algoritmo propuesto, desde una perspectiva general, para la transmisión de datos seguros en tarjetas NFC. Los recursos empleados en la ejecución de las pruebas son:

1.- Cuatro tarjetas NFC de 1 KB.
2.- Modulo de grabado PN532.
3.- Arduino Mega

Todas las tarjetas fueron grabadas a una distancia de 3 cm para evitar perdidas de datos o constantes repeticiones de grabaciones.

En la Figura 7 se muestra el prototipo implementado con el Arduino Mega y el lector PN532 en funcionamiento.

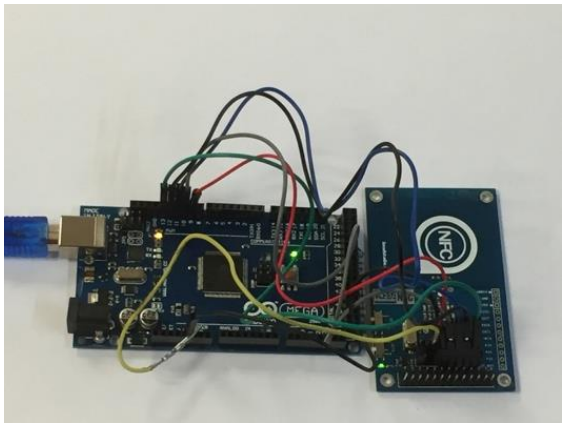

Figura 7. *Prototipo de NFC en funcionamiento*.

El proceso de validación de datos en las tarjetas NFC consiste en embeber cadenas con una longitud de 30 caracteres, para posteriormente validar el funcionamiento del Algoritmo 1. Las tarjetas NFC reciben las siguientes acciones.

- En la tarjeta 1, se inserta la cadena C1="Prueba de almacenamiento de 22", y no se modifica su contenido.
- En la tarjeta 2, se inserta la cadena C2="qwertyuiopasdfghjklñ´<zxcvbnm,", y se modifica al menos un bit en memoria.
- En la tarjeta 3, se inserta la cadena C3="Desbordamiento en memoria B450", y se modifican varios bits de forma aleatoria.
- En la tarjeta 4 y en C4 no se escribieron datos.

Conforme a las pruebas que se ejecutaron en proceso de validación, se realizó la Tabla 1 para presentar las observaciones sobre los resultados obtenidos.

Número de prueba	Acción	Resultado
1	Validar la cadena C1	El software reconoció correctamente la cadena grabada en la tarjeta NFC
2	Validar la cadena C2	El software detectó la modificación de la cadena
3	Validar la cadena C3	El software detectó la modificación de la cadena
4	Validar la cadena C4	Se retorna error de contenido, sin datos

Tabla 1. *Resumen de resultados de las pruebas efectuadas.*

Con base a los datos escritos en la Tabla 1, el software logró detectar correctamente las modificaciones cuando se alteraron las cadenas en las pruebas 2 y 3, mientras que en la cadena sin alteraciones (prueba 1) se validó correctamente. En la prueba 4, el software detectó que no existía contenido por analizar, por lo tanto indicó un mensaje controlado de “sin datos”. En base a las pruebas realizadas se pudieron reproducir los casos de cuando los datos son correctos, cuando los datos son corrompido por una entidad externa (prueba 2 y 3) de forma específica o aleatoria, así como el control de excepciones cuando no existen datos.

La combinación de los principios de esteganografía y criptografía propuestos en este trabajo, muestran de forma eficaz que el empleo de información expresada a través de la reducción de datos (representación por un sólo símbolo) para la validación de datos en la tecnología NFC, permite generar validaciones correctas sobre los datos que se han grabado en un medio de almacenamiento. Como puede observarse en la revisión literaria, las mayoría de los trabajos expresan que es necesario la implementación de criptografía para la transmisión de datos como es el caso de Dragan (2015), Kim (2016) y Schürmann, Dechand & Wolf (2017) para evitar el robo o manipulación de datos en texto plano, mientras que en Sankpal, Mundhe, Kotwal Machale & Malchikare (2017) y Muke, Shinde, Mistry & Jawalkar (2015) proponen enviar los datos ocultos en imágenes utilizando teléfonos inteligentes, para sistemas de autenticación. En esta propuesta el diseño se desarrolló para aplicarse, de forma general, para transmitir datos en NFC, debido a que no solo esta enfocada a aplicaciones de autenticación para acceso a datos o lugares físicos, si no que también para el intercambio de información entre dispositivos pares, aplicaciones comerciales, entre otras.

4. Conclusiones

De acuerdo con las pruebas realizadas en la sección III y los datos obtenidos, se ha observado que el reordenamiento de información propuesto en el Algoritmo 1 logró validar correctamente la cadena C1, la cual no contenía modificaciones, mientras tanto en C2 y C3 el software detectó que hubo cambios en la cadena debido a que no se logró formar correctamente la matriz final para recuperar la información. En la cuarta prueba se verificó correctamente que no existían datos grabados.

El cifrado Vernam permite incrementar el nivel de seguridad de los datos embebidos, debido a que la permutación ejecutada sobre la palabra clave impide conocerla si no se conoce el código fuente que se está ejecutando en el Arduino. Debido a las capacidades de procesamiento limitadas del Arduino Mega no se emplearon algoritmos avanzados como AES o RSA, dado que esto consume

una mayor cantidad de recursos en el procesador y memoria, por lo cual se determinó evitar retrasos en el accionar del hardware.

El Algoritmo 1, está adaptado para trabajar en el software de codificación de Arduino y en el posible tamaño de memoria de las tarjetas NFC, aunque también es posible su implementación en otras aplicaciones ya sea de esteganografía y/o criptografía.

La propuesta está enfocada a un uso general del algoritmo, lo cual es independiente al tipo de transacción para la que se aplique, como se mencionó en la revisión literaria la tecnología NFC es multipropósito, por consiguiente, el Algoritmo 1, presentado, se ha adaptado a esa característica y puede ser empleado en transacciones comerciales, médicas, de acceso a áreas restringidas, entre otras aplicaciones.

Es importante señalar que el Algoritmo de seguridad propuesto tiene la particularidad de que, cuando el tamaño del alfabeto se incrementa, surge la necesidad de abarcar mayor espacio en memoria. Por lo tanto, como trabajo a futuro se estudiará el cómo realizar solapamiento de matrices y así reducir la cantidad de matrices en el espacio físico. Por otro lado, se implementará el cifrado AES o RSA en un teléfono inteligente, lo cual brindará mayor seguridad, además de que el aprovechamiento del microprocesador del teléfono permitirá ejecutar las sentencias del código con mayor velocidad.

Agradecimientos

Agradecemos a CONACYT por la asignación de la beca con número de registro 445998 para estudios de posgrados.

Referencias

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). A Survey on Sensor Networks. Common. 102-114.

Al Husainy, M. A. F. (2012). Message Segmentation to Enhance the Security of LSB Image Steganography. International Journal of Advanced Computer Science and Applications. 57-62.

Chappleand, M. & Solomon, M. (2005). Information Security Illuminated. Primera edición. Estados Unidos: Jones and Bartlett Publishers.

Childs, J. R. (2000). General Solution of the ADFGVX Cipher System. Estados Unidos: Aegean Park Press.

Choudry, K. N. & Wanjari, A. (2015). A Survey Paper on Video Steganography. IJCSIT.

Coskun, V., Ok, K. & Ozdenizci, B. (2012). Near Field Communication (NFC): From Theory to Practice. Primera edición. UK: John Wiley and Sons.

Coskun, V., Ok, K. & Ozdenizci, B. (2013). Professional NFC Application Development for Android Primera edición. UK: John Wiley Sons, Wrox.

Delfs, D. & Helmut, H. (2007). Introduction to Cryptography: Principles and applications. Segunda edición. Springer & Business Media.

Dhruw, T. & Tiwari, D. N. (2016). Different Method used in Pixel Value Differencing Algorithm. IOSR Journal of Computer Engineering. 102–109.

Di Laura, C., Pajuelo, D., and Kemper, G. (2016). A novel steganography technique for SDTV H.264 AVC encoded video. International Journal of Digital Multimedia Broadcasting. 1–9.

Djebba, F., Ayad, B., Meraim, K. A. & Hamam, H. (2012). Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing. 1–16.

Dragan, A. (2015). Encryptation and Decryption on Messages on Android using NFC Tags. Journal of Mobile, Embedded and Distributed Systems. 130-135.

Dworkin, M. J., Barker, E. B., Nechvatal, R. J., Foti, J., Bassham, L. E., Roback, E. & Dray, J. F. (2016). Advance Encryptatio Standard (AES). NIST publications.

ECMA. (2018). Near Field Communication Interface and Protocol 1 (NFCIP-1). ECMA International. Diponible: http://www.ecma-international.org/publications/standards/Ecma-340.htm. (Consultado 5-9-2018).

Haselsteiner, E. & Breitfub, K. (2016). Security in Near Field Communication (NFC). Philips Semiconductors.

Kavya, S., Pavithra, K., Rajaram, S., Vahini, M. & Harini, N. (2014). Vulnerability Analysis and Security System For NFC-Enabled Mobile Phones. International Journal of Scientific and Technology Research.

Kim, H. (2016). A study on the Cryptographic Algorithm for NFC. Indian Journal of Science and Technology. 1-5.

Mazurczyk, W. & Caviglione, L. (2014), Steganography in Modern Smartphones and Mitigation Techniques. Polish National Science Center.

Mishra, B. & Tripathi, M. (2015). Information security though digital image Steganography using multilevel and Compression technique. International Research Journal of Computer Science IRJCS. 23-31.

Muke, S., Shinde, S., Mistry, C. & Jawalkar, P. (2015). NFC Hardware Device Based Access Control System using Information Hiding. International Journal of Innovative Research in electrical, electronics, Instrumentation and Control Engineering. 69-72.

Rivest, R., Shamir, A. & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 120–126.

Sankpal, L. J., Mundhe, S., Kotwal M., Machale, P. & Malchikare S. (2017). NFC Based Access Control System Using Image Hiding. International Journal of Innovative Research in Computer and Communication Engineering. 5352-5355.

Schürmann, D., Dechand, S. & Wolf, L. (2017) OpenKeychain: An Architecture for Cryptography with Smart Cards and NFC Ring son Android", ACM Interact Mob. Werable Ubiquiotous Tech. 1-24.

Tian, H., Qin, J., Huang, Y., Chen, Y., Wang, T., Liu, J., & Cai, Y. (2015). Optimal matrix embedding for Voice-over-IP steganography. College of Computer Science and Technology. National Huaqiao University China. 33-43.

Tripathi, D., Singh, Y. K. & Singh, R. (2016). A survey on Image Steganography With its Related Technique and its Types. IJSART. 163-169.

Vaithiyanathan, V., Karthikeyan, B., Anischin Raj, M. M., Reddy, R., Priyanka, S. & Abinaya, K. (2015). An Amalgamated Approach of cryptography and steganography using IWT and Random pixel selection for secure transmission. ARPN Journal of Engineering and Applied Sciences. 2352-2357.

Vernam, G. S. (1926). Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. Journal of the IEEE. 109-115.

Yi, W. J. and Saniie, J. (2013). Smart Mobile System for Body Sensor Network. Estados Unidos. Proceedings of the IEEE International Conference on Electro/Information Technology (EIT). 1-4.

Notas biográficas:

Héctor Caballero recibió el título de Ingeniero en Computación de la Universidad del Estado de México, México en 2011, y es estudiante de doctorado en Ciencias de la Ingeniería, en la Universidad del Estado de México, México . Sus temas de investigación son la esteganografía y la ciencia basada en lenguaje natural.

Vianney Muñoz es Profesor investigador en procesamiento de imágenes y visión computacional en la Universidad Autónoma del Estado de México. En 2009, recibió su doctorado de la Universidad Paris 13, Francia. Su trabajo de investigación es sobre visión computacional, procesamiento de imágenes, compresión de video, inteligencia artificial, entre otros.

Marco A. Ramos es Profesor investigador en Inteligencia Artificial y Realidad Virtual en la Universidad Autónoma del Estado de México. Obtuvo su doctorado en la Universidad de Toulouse en 2007, Francia. Sus temas de investigación son: Vida artificial, técnicas de animación, sistemas distribuidos, agentes inteligentes, etc.

Marcelo Romero Huertas es Profesor investigador en ciencias de la computación en la Universidad Autónoma del Estado de México. Obtuvo su doctorado en la Universidad de York en el 2010, Reino Unido. Sus temas de investigación son: tratamiento de imágenes, reconocimiento de patrones, puntos antropométricos, etc.

Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.5 México.