© Revista de Matemática: Teoría y Aplicaciones 2019 **26**(2) : 281–297
cimpa – ucr issn: 1409-2433 (Print), 2215-3373 (Online)
doi: https://doi.org/10.15517/rmta.v26i2.38319

UN NUEVO ENFOQUE A LA CRIPTOGRAFÍA MATEMÁTICA USANDO LA FUNCIÓN DISCRETA DE AMBIGÜEDAD

A NEW APPROACH TO MATHEMATICAL CRYPTOGRAPHY USING THE DISCRETE AMBIGUITY FUNCTION

Juan Pablo Soto–Quirós* Domingo Rodríguez†

Received: 23/Feb/2012; Revised: 7/Jun/2019;
Accepted: 7/Jun/2019

---

*Instituto Tecnológico de Costa Rica, Escuela de Matemáticas, Cartago, Costa Rica. E-Mail: jusoto@tec.ac.cr.
†Universidad de Puerto Rico en Mayagüez, Departamento de Ingeniería Eléctrica y Computadoras, Mayagüez, PR, 00681, USA. E-Mail: domingo@ece.uprm.edu

Resumen

A través de la criptografía, se desea modificar y ocultar cierta información, para que sólo algún grupo determinado de personas pueda interpretarlo por medio de una clave. Al tratar de utilizar diversos campos de la matemática para realizar este proceso, se desarrolla el concepto de criptografía matemática.

La mayoría de métodos criptográficos matemáticos se concentran en teoría de números. También exiten otros métodos criptográficos en el área de física cuántica y geometría algebraica, particularmente elíptica y curvas hyperelípticas definidas sobre cuerpos y campos finitos, finito campos, entre otros. El presente trabajo introduce una nueva modalidad del aspecto de procesamiento de señales al campo de la criptografía matemática, a través de representaciones armónicas bidimensionales como lo es la función discreta de ambigüedad. Este trabajo utiliza dos definiciones equivalentes, en módulo, de la función discreta de ambigüedad.

Este nuevo método criptográfico utiliza el concepto de clave simétrica para efectuar el proceso de cifrar y descifrar el mensaje.

Palabras clave: función discreta de ambigüedad; criptografía; claves simétricas; transformada discreta de Fourier.

Abstract

Through cryptography, be modified and hide certain information, so that only a certain group of people can interpret it through a key. When trying to use various fields of mathematics for this process, the concept of mathematical cryptography is developed.

Most mathematical cryptographic methods focus on number theory. Also, there are other cryptographic methods in the area of quantum physics and algebraic geometry, particularly hyperelliptical curves defined over finite bodies and finite fields. This paper introduces a new method of mathematical cryptography with signal processing techniques, through of a dimensional harmonic representations such as the discrete ambiguity function. This paper uses two equivalent definitions in module discrete ambiguity function.

This new cryptographic method uses the concept of symmetric key to making the process of encrypting and decrypting the message.

Keywords: discrete ambiguity function; cryptography; symmetric keys; discrete Fourier transform.

Mathematics Subject Classification: 94A60, 15A23.

1 Introducción

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. La criptografía se basa en diferentes tipos de aritmética: números enteros y racionales, números complejos en campos finitos, aritmética modular, entre otros [12]. Por ejemplo, en el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números y luego realizar cálculos con estos números para modificarlos y hacerlos incomprensibles; además de asegurarse de que el receptor pueda descifrar tal modificación. El proceso de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El concepto de *criptografía matemática* se refiere a las técnicas criptográficas que utilizan los conceptos matemáticos para su desarrollo. La criptografía matemática se basa en muchas áreas de las matemáticas, incluyendo la teoría de números, geometría algebraica, álgebra abstracta, probabilidad, estadística y teoría de la información [10].

Normalmente, el proceso de cifrar se realiza mediante una clave, denominada *clave para cifrar* y el proceso de descifrar requiere una clave para obtener el mensaje original; dicha clave se denomina *clave para descifrar*. Los métodos criptográficos para descifrar dichas claves se dividen en dos tipos:

- Simétricas: una misma clave es utilizada para cifrar y descifrar.
- Asimétricas: la clave utilizada para cifrar es diferente a la que se utiliza para descifrar.

La mayoría de métodos criptográficos matemáticos se concentran en la teoría de números. Además, otros métodos criptográficos han sido desarrollados en el área de física cuántica y geometría algebraica, particularmente elíptica y curvas hyperelípticas definidas sobre cuerpos y campos finitos, finito campos. El presente trabajo introduce una nueva modalidad del aspecto de procesamiento de señales al campo de la criptografía matemática, a través de representaciones armónicas bidimensionales, utilizando el concepto de la función discreta de ambigüedad (FDA). Este trabajo utiliza dos definiciones equivalentes, en módulo, de la FDA:

$$\mathcal{A}^{\mathbf{1}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n-m\rangle_N]e^{-i\frac{2\pi}{N}nk},$$

y

$$\mathcal{A}^{\mathbf{2}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[\langle n+m\rangle_N]\overline{y}[n]e^{-i\frac{2\pi}{N}nk},$$

las cuales se explican detalladamente en la Sección 2.

Dicho método criptográfico utiliza el concepto de clave simétrica para efectuar el proceso de cifrar y descifrar los mensajes, a través de la representación matricial de la FDA, llamada matriz FDA, utilizando una fila o una columna de tal matriz como el mensaje encriptado.

Con el fin de probar los teoremas propuestos en este trabajo, se utiliza la definición y algunos resultados sobre: los *productos Kronecker y Hadamard de matrices* [9, 11, 14, 18], la *transformada discreta de Fourier y su representación matricial* [5, 7, 11, 18], *matrices circulantes* [6] y *operadores de permutación y su representación matricial* [1, 7, 11]. En las referencias mencionadas, el lector puede consultar al respecto. Además, cabe mencionar que los teoremas y sus respectivas demostraciones son propuestos y desarrollados por los autores de este artículo.

Este artículo está organizado de la siguiente manera. En la Sección 2 se introduce el concepto de función continua de ambigüedad y la FDA, la representación matricial de la FDA, conocida como matriz FDA, y su cómputo en paralelo. En la Sección 3 se explica el método criptográfico: el proceso para cifrar y descifrar un mensaje, utilizando la matriz FDA. En la Sección 4 se presentan las conclusiones del trabajo.

2 Función discreta de ambigüedad

En 1953, P.M. Woodward define *función de ambigüedad*, la cual trata de un mecanismo formulado para describir el efecto Doppler en los receptores de filtro apareados [19]. Woodward reconoció la influencia de la teoría de la comunicación de Shannon, a partir de 1948, en sus ideas, y explicó la importancia de la “ambigüedad” en el procesamiento de señales de radares, tal vez mejor concebido en términos de una forma del principio de incertidumbre. La función de ambigüedad juega un papel clave en el campo de procesamiento de señales de tiempo-frecuencia, ya que está relacionada con la distribución de Wigner-Ville, a través de la transformada de Fourier de dos dimensiones [4].

Definición 1 (Función de ambigüedad) *Sean* $f, g \in L^2(\mathbb{R})$*, entonces la* función de ambigüedad *de* f *y* g *se define como el mapeo* $\mathcal{A}^{\mathbf{1}}_{f,g} : L^2(\mathbb{R}) \times L^2(\mathbb{R}) \to L^2(\mathbb{R} \times \mathbb{R})$ *tal que*

$$\mathcal{A}^{\mathbf{1}}_{f,g}(t, \theta) = \int_{\mathbb{R}} f(x)\overline{g}(x-t)e^{-2i\pi x\theta}dx, \tag{1}$$

donde $\overline{g}$ *es el conjugado complejo de* y*.*

$\mathcal{A}^{\mathbf{1}}_{f,g}$ recibe el nombre de *función de ambigüedad cruzada* cuando $f \neq g$. En el caso $f = g$ se conoce simplemente como función de ambigüedad. Benedetto y Donatelli [2, 3] definen la función de ambigüedad con ligeras modificaciones a la definida en la ecuación (1):

$$\mathcal{A}^{\mathbf{2}}_{f,g}(t,\theta) = \int_{\mathbb{R}} f(x+t)\overline{g}(x)e^{-2i\pi x\theta}dx. \tag{2}$$

A pesar de las diferencias, estas dos representaciones de la función de ambigüedad mantienen una relación a nivel de módulo: $|\mathcal{A}^{\mathbf{1}}_{f,g}(t,\theta)| = |\mathcal{A}^{\mathbf{2}}_{f,g}(t,\theta)|$. Por lo tanto, las ecuaciones (1) y (2) serán consideradas representaciones equivalentes de la función de ambigüedad. A nivel de implementación, la función de ambigüedad que desarrolló Woodward admite una representación con dominio discreto y finito.

Definición 2 *Sea $x, y \in \mathbb{C}^N$. La función discreta de ambigüedad (FDA) de x, y se define como el mapeo $\mathcal{A}^{\mathbf{1}}_{x,y} : \mathbb{C}^N \times \mathbb{C}^N \to \mathbb{C}^{N\times N}$ tal que*

$$\mathcal{A}^{\mathbf{1}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle m-n\rangle_N]\omega_N^{-nk}, \tag{3}$$

donde $\mathbb{C}^N \times \mathbb{C}^N$ es el espacio de matrices de dimensión $N \times N$, $\overline{y}$ es el conjugado complejo de y, $\langle m-n\rangle_N = m - n \; mod \; N$ y $\omega_N = e^{i\frac{2\pi}{N}}$.

Benedetto y Donatelli [2, 3] también definen una representación con dominio discreto y finito de la ecuación (2):

$$\mathcal{A}^{\mathbf{2}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[\langle m+n\rangle_N]\overline{y}[n]\omega_N^{-nk}. \tag{4}$$

Las dos definiciones de FDA también son equivalentes a nivel de módulo; es decir, $|\mathcal{A}^{\mathbf{1}}_{x,y}[m,k]| = |\mathcal{A}^{\mathbf{2}}_{x,y}[m,k]|$. Al ser la FDA una función de dos dimensiones, entonces se puede expresar en notación matricial. Sea $A^{\mathbf{1}}_{x,y}, A^{\mathbf{2}}_{x,y} \in \mathbb{C}^{N\times N}$, entonces la representación matricial de FDA de las ecuaciones (3) y (4) se define como $(A^{\mathbf{1}}_{x,y})_{m,k} = \mathcal{A}^{\mathbf{1}}_{x,y}[m,k]$ y $(A^{\mathbf{2}}_{x,y})_{m,k} = \mathcal{A}^{\mathbf{2}}_{x,y}[m,k]$. El siguiente teorema explica un modo de expresar y computar la matriz FDA, la cual permite su cómputo en paralelo, al utilizar los productos Kronecker y Hadamard.

Teorema 1 *Sea $x, y \in \mathbb{C}^N$. Entonces*

$$A^{\mathbf{1}}_{x,y} = \mathcal{R}_{N,N}\{L_N^{N^2}\left[I_N \otimes F_N\right]\left[(\boldsymbol{1}_N \otimes \overline{x}) \odot \overline{Y}\right]\}, \tag{5}$$

$$A^{\mathbf{2}}_{x,y} = \mathcal{R}_{N,N}\{L_N^{N^2}\left[I_N \otimes F_N\right]\left[X \odot (\boldsymbol{1}_N \otimes \overline{y})\right]\}, \tag{6}$$

donde $\mathcal{R}_{N,N}$ es el operador re-shape[1]*; $\otimes$ y $\odot$ son los productos Kronecker y Hadamard de matrices, respectivamente; $I_N \in \mathbb{C}^{N\times N}$ es la matriz identidad de orden N; $F_N \in \mathbb{C}^{N\times N}$ es la matriz de la transformada discreta de Fourier de orden N; $L_N^{N^2} \in \mathbb{C}^{N^2\times N^2}$ es la matriz de permutación de paso N y orden N^2; $\boldsymbol{1}_N \in \mathbb{C}^N$ es el vector tal que todas sus entradas son iguales a 1 y $X, Y \in \mathbb{C}^{N^2}$ son vectores de orden N^2 tal que*

$$Y = \begin{pmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{N-1} \end{pmatrix}, \quad X = \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix},$$

donde $X_m, Y_m \in \mathbb{C}^N$ tal que $X_m[n] = x[\langle m+n\rangle_N]$ y $Y_m[n] = y[\langle m-n\rangle_N]$, para $m, n \in \mathbb{Z}_N$.

Demostración. Se realizará la demostración de la ecuación (5). La demostración de la ecuación (6) se desarrolla de forma similar.

Sea $a_{x,y} = L_N^{N^2}\left[I_N \otimes F_N\right]\left[(\mathbf{1}_N \otimes \overline{y}) \odot \overline{Y}\right]$. Entonces

$$a_{x,y} = L_N^{N^2}\begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N-1} \end{pmatrix}, \quad H_m \in \mathbb{C}^N, \tag{7}$$

tal que $H_m = F_N(x \odot \overline{Y_m})$. Aplicando el operador $\mathcal{R}_{N,N}$ a ambos lados de la ecuación (7) y utilizando la propiedad $\mathcal{R}_{N,N}\left\{L_N^{N^2} v\right\} = \left(\mathcal{R}_{N,N}\left\{v\right\}\right)^T$, para cualquier $v \in \mathbb{C}^{N^2}$, se obtiene

$$\mathcal{R}_{N,N}\{a_{x,y}\} = \mathcal{R}_{N,N}\left\{L_N^{N^2}\begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N-1} \end{pmatrix}\right\} = \left(\mathcal{R}_{N,N}\left\{\begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N-1} \end{pmatrix}\right\}\right)^T.$$

[1] $\mathcal{R}_{N,N} : \mathbb{C}^{N^2} \to \mathbb{C}^{N\times N}$ reordena un vector de orden N^2 en una matriz de orden $N \times N$, dividiendo el vector en N bloques y acomodando cada bloque como una columna. Más detalles en [13].

Sea

$$H = \mathcal{R}_{N,N}\left\{\begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N-1} \end{pmatrix}\right\},$$

es decir, $H = (H_0\ H_1\ ...\ H_{N-1})$, donde $H \in \mathbb{C}^{N\times N}$ y H_m representa la columna m de la matriz H. Entonces,

$$(H_{m,k})^T = H_{k,m} = H_m[k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle m-n\rangle_N]\omega_N^{-nk} = \mathcal{A}^{\mathbf{1}}_{x,y}[m,k].$$

■

Nota: Existen otras formas de realizar el computo de la función discreta de ambiguedad, la cual no involucra productos Kronecker y Hadamard, los cuales no utilizan computo en paralelo [15]. El objetivo de usar las ecuaciones (5) y (6), es realizar un eficiente computo usando procesamiento en paralelo, el cual se puede utilizar en una computadora con varios procesadores [16].

3 Nuevo método criptográfico

En esta sección se desarrolla el nuevo método criptográfico, utilizando la función discreta de ambigüedad. Se explicará el proceso para cifrar un mensaje utilizando una clave simétrica, la cual se puede generar de forma aleatoria. Para este proceso se utiliza la matriz FDA, la cual genera el mensaje cifrado, seleccionando una fila o una columna de dicha matriz. Luego, se explicará el proceso para descifrar el mensaje, el cual depende de la selección de una fila o una columna para el mensaje cifrado, ya que son dos procesos distintos.

3.1 Proceso para cifrar el mensaje

Este proceso necesita computar la matriz FDA. El proceso es independiente de cuál definición de la función discreta de ambigüedad se utilice; ya sea la definición original (ecuación (3)) o la definición modificada (ecuación (4)). Para eso se utilizará el símbolo de $\mathcal{A}_{x,y}$, la cual representará a las dos definiciones de la FDA.

Sea $y \in \mathbb{C}^N$ el mensaje a encriptar y sea $x \in \mathbb{C}^N$ parte de la clave simétrica, que se puede generar de forma aleatoria. El mensaje y es cifrado, calculando la matriz FDA de x, y, utilizando una fila o una columna de la matriz FDA de x, y. Para esto, se generan dos números enteros, c_0, c_1, de forma aleatoria:

- $c_0 \in \mathbb{Z}_2$ representa la selección de una fila o una columna de la matriz FDA. En este caso, si $c_0 = 0$, entonces se escoge una fila, y si $c_0 = 1$ se escoge una columna.
- $c_1 \in \mathbb{Z}_N$ representa el número de fila o columna a seleccionar.

Posteriormente, se genera el vector $z \in \mathbb{C}^N$ que contiene el mensaje cifrado[2]: si $c_0 = 0$, entonces $z = \mathcal{A}_{x,y}[c_1, :]^T$; si $c_0 = 1$, entonces $z = \mathcal{A}_{x,y}[:, c_1]$. Finalmente, se genera la clave simétrica, $w \in \mathbb{C}^{N+2}$ tal que $w[0] = c_0$, $w[1] = c_1$ y $w[n] = x[n-2]$ para $n = 2, 3, \ldots, N+1$. El vector w será la información disponible al público (clave pública). El Algoritmo 1 muestra el pseudo-código de lo explicado anteriormente.

Algoritmo 1 Proceso para cifrar el mensaje y.

Entrada: $y \in \mathbb{C}^N$ (mensaje original).
Salida: $w \in \mathbb{C}^{N+2}$ (clave), $z \in \mathbb{C}^N$ (mensaje cifrado).

1: $x \leftarrow \text{Rand}(\mathbb{C}^N)$
2: $A \leftarrow \mathcal{A}_{x,y}$
3: $c_0 \leftarrow \text{Rand}(\mathbb{Z}_2)$, $c_1 \leftarrow \text{Rand}(\mathbb{Z}_N)$
4: **si** $c_0 = 0$ **entonces**
5: $\quad z \leftarrow \mathcal{A}[c_1, :]^T$
6: **si no**
7: $\quad z \leftarrow \mathcal{A}[:, c_1]$
8: **fin si**
9: $w[0] \leftarrow c_0$, $w[1] \leftarrow c_1$, $w[2 : N+1] \leftarrow x$

3.2 Proceso para descifrar el mensaje

El proceso para descifrar el mensaje $z \in \mathbb{C}^N$ depende de si el vector z representa una fila o una columna de la matriz FDA. A continuación se explicarán los métodos para recuperar el mensaje original. En el caso de que el mensaje cifrado representa una *fila* de la matriz FDA, se explicará el procedimiento utilizando la definición original de la función discreta de ambigüedad, es decir, la ecuación (3). Para el caso cuando el mensaje cifrado representa una *columna* de la matriz FDA, se explicará el procedimiento utilizando la definición modificada de la función discreta de ambigüedad propuesta por Benedetto y Donatelli en [2, 3],

[2]Dado una matriz A, la notación $A[m, :]$ y $A[:, n]$ representan la fila m y la columna n de la matriz A, respectivamente.

es decir, la ecuación (4). La decisión de utilizar una definición u otra de la FDA para explicar los métodos de recuperación del mensaje original ha sido arbitraria y no influye en el resultado final.

3.2.1 Caso 1: El mensaje cifrado representa una fila de la matriz FDA

Sin pérdida de generalidad, el siguiente procedimiento se explicará utilizando la definición original de la función discreta de ambigüedad, es decir, la ecuación (3). Para la ecuación (4), propuesta por Benedetto y Donatelli, se prosigue de forma similar y el resultado se presenta al final.

Sea $w \in \mathbb{C}^{N+2}$ la clave simétrica y $z \in \mathbb{C}^N$ el mensaje cifrado. Considere el caso $w[0] = 0$, es decir, el vector z contiene una fila de la matriz FDA y el número de fila que representa está dado por $w[1]=m$; entonces $w=\mathcal{A}^{\mathbf{1}}_{x,y}[m,:]^T$, para $m \in \mathbb{Z}_N$. Por lo tanto, para m fijo,

$$\mathcal{A}^{\mathbf{1}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n-m\rangle_N]\omega_N^{-nk}, \qquad k \in \mathbb{Z}_N. \tag{8}$$

Usando la ecuación (8), considere los siguientes pasos:

Paso 1: Aplicar la inversa de la transformada discreta de Fourier:

$$\mathcal{F}^{-1}\{\mathcal{A}^{\mathbf{1}}_{x,y}\}[n] = x[n]\overline{y}[\langle n-m\rangle_N].$$

Paso 2: Dividir por $x[n]$, asumiendo que $x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$:

$$\frac{\mathcal{F}^{-1}\{\mathcal{A}^{\mathbf{1}}_{x,y}\}[n]}{x[n]} = \overline{y}[\langle n-m\rangle_N].$$

Paso 3: Aplicar operador de traslación $\mathcal{S}_{-m}$[3]:

$$\mathcal{S}_{-m}\left\{\frac{\mathcal{F}^{-1}\{\mathcal{A}^{\mathbf{1}}_{x,y}\}[n]}{x[n]}\right\} = \overline{y}[n], \text{ para todo } n \in \mathbb{Z}_N.$$

Paso 4: Aplicar el conjugado complejo:

$$\overline{\left\{\mathcal{S}_{-m}\left\{\frac{\mathcal{F}^{-1}\{\mathcal{A}^{\mathbf{1}}_{x,y}\}[n]}{x[n]}\right\}\right\}} = y[n].$$

[3]El operador de traslación se define como el mapeo $\mathcal{S}_m : \mathbb{C}^N \to \mathbb{C}^N$ tal que $\mathcal{S}_m\{x\}[n] = x[\langle n-m\rangle_N]$. Ver [1] para más detalles.

En el **Paso 2**, es necesario que $x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$. Por lo tanto, para recuperar el mensaje original, una condición necesaria es que la clave, representada por el vector x, no posea entradas nulas. Lo anterior prueba el siguiente teorema:

Teorema 2 *Sea $x, y \in \mathbb{C}^N$, tal que $x[n] \neq 0$, para $n \in \mathbb{Z}_N$, y $A^{\mathbf{1}}_{x,y} \in \mathbb{C}^{N\times N}$ la matriz FDA (ecuación (5)). Entonces,*

$$y = \frac{1}{N} S_{-m} \overline{D} F_N \overline{b_m}, \tag{9}$$

donde

- *$F_N \in \mathbb{C}^{N\times N}$ es la matriz de la transformada discreta de Fourier de orden N.*
- *$S_{-m} \in \mathbb{C}^{N\times N}$ es la representación matricial del operador de traslación $\mathcal{S}_{-m}$.*
- *$D \in \mathbb{C}^{N\times N}$ tal que $D = diag\left(\frac{1}{x[0]}, \frac{1}{x[1]}, \ldots, \frac{1}{x[N-1]}\right)$.*
- *$b_m \in \mathbb{C}^N$ tal que $b_m[k] = (A^{\mathbf{1}}_{x,y})_{m,k}$, para $k \in \mathbb{Z}_N$.*

El Algoritmo 2 muestra la implementación del método explicado anteriormente.

Algoritmo 2 Proceso para descifrar el mensaje z.

Entrada: $w \in \mathbb{C}^{N+2}$ (clave), $z \in \mathbb{C}^N$ (mensaje cifrado).
Salida: $y \in \mathbb{C}^N$ (mensaje original).

1: $v_0 \leftarrow \overline{z}$
2: $v_1 \leftarrow \mathcal{F}\{v_0\}$ (transformada discreta de Fourier)
3: $v_2 \leftarrow w[2 : N+1]$
4: $v_3 \leftarrow v_1 \odot v_4$, donde $v_4[n] = \frac{1}{\overline{v_2[n]}}$
5: $m \leftarrow w[1]$
6: $y \leftarrow \frac{1}{N}\mathcal{S}_{-m}\{v_3\}$

Para la matriz FDA que se genera a partir de la ecuación (4), se obtiene un resultado equivalente con un procedimiento similar, el cual se expresa en el teorema 3.

Teorema 3 *Sea $x, y \in \mathbb{C}^N$, tal que $x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$, y $A^{\mathbf{2}}_{x,y} \in \mathbb{C}^{N\times N}$ representa a la matriz FDA (ecuación (6)). Entonces,*

$$y = \frac{1}{N} S_{-m} \overline{D} S_m F_N \overline{b_m}, \tag{10}$$

donde

- *$F_N \in \mathbb{C}^{N\times N}$ es la matriz de la transformada discreta de Fourier de orden N.*
- *$S_m, S_{-m} \in \mathbb{C}^{N\times N}$ son las representaciones matriciales de los operadores de traslación $\mathcal{S}_m$ y $\mathcal{S}_{-m}$, respectivamente.*
- *$D \in \mathbb{C}^{N\times N}$ tal que $D = diag\left(\frac{1}{x[0]}, \frac{1}{x[1]}, \ldots, \frac{1}{x[N-1]}\right)$.*
- *$b_m \in \mathbb{C}^N$ tal que $b_m[k] = \left(A^{\mathbf{2}}_{x,y}\right)_{m,k}$, para $k \in \mathbb{Z}_N$.*

3.2.2 Caso 2: El mensaje cifrado representa una columna de la matriz FDA

Sin pérdida de generalidad, el siguiente procedimiento se explicará utilizando la definición de la función discreta de ambigüedad propuesta por Benedetto y Donatelli, es decir, la ecuación (4). Para la ecuación (3), la definición original, prosigue de forma similar, y el resultado se presenta al final.

Sea $w \in \mathbb{C}^{N+2}$ la clave simétrica y $z \in \mathbb{C}^N$ el mensaje cifrado. Considere el caso $w[0] = 1$, es decir, el vector z contiene una columna de la matriz FDA y el número de columna que representa está dado por $w[1] = k$; entonces $z[2 : N+1] = \mathcal{A}^{\mathbf{2}}_{x,y}[:, k]$, para $k \in \mathbb{Z}_N$. Por lo tanto, para k fijo,

$$\mathcal{A}^{\mathbf{2}}_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[\langle n+m\rangle_N]\overline{y}[n]\omega_N^{-nk}, \qquad m \in \mathbb{Z}_N. \tag{11}$$

Ahora, considere el sistema de N ecuaciones, generado de la ecuación (11), variando el valor de la primera entrada (m):

$$\begin{cases} x[0]\overline{y}[0] & + \cdots + & x[N-1]\overline{y}[N-1]\omega_N^{-(N-1)k} & = \mathcal{A}^{\mathbf{2}}_{x,y}[0,k], \\ x[1]\overline{y}[0] & + \cdots + & x[0]\overline{y}[N-1]\omega_N^{-(N-1)k} & = \mathcal{A}^{\mathbf{2}}_{x,y}[1,k], \\ & \vdots & & \vdots \\ x[N-1]\overline{y}[0] & + \cdots + & x[N-2]\overline{y}[N-1]\omega_N^{-(N-1)k} & = \mathcal{A}^{\mathbf{2}}_{x,y}[N-1,k]. \end{cases}$$

La representación matricial del sistema de ecuaciones anterior es

$$\underbrace{\begin{pmatrix} x[0] & x[1]\omega_N^{-k} & \cdots & x[N-1]\omega_N^{-(N-1)k} \\ x[1] & x[2]\omega_N^{-k} & \cdots & x[0]\omega_N^{-(N-1)k} \\ \vdots & \vdots & \ddots & \vdots \\ x[N-1] & x[0]\omega_N^{-k} & \cdots & x[N-2]\omega_N^{-(N-1)k} \end{pmatrix}}_{Z} \begin{pmatrix} \overline{y}[0] \\ \overline{y}[1] \\ \vdots \\ \overline{y}[N-1] \end{pmatrix} = \begin{pmatrix} \mathcal{A}^{\mathbf{2}}_{x,y}[0,k] \\ \mathcal{A}^{\mathbf{2}}_{x,y}[1,k] \\ \vdots \\ \mathcal{A}^{\mathbf{2}}_{x,y}[N-1,k] \end{pmatrix}.$$

Ahora, sea $W \in \mathbb{C}^{N\times N}$ tal que $W = diag(1, \omega_N^{-k}, ..., \omega_N^{-(N-1)k})$, entonces

$$\begin{aligned} Z &= ZW^{-1}W \qquad (12) \\ &= \underbrace{\begin{pmatrix} x[0] & x[1] & \cdots & x[N-1] \\ x[1] & x[2] & \cdots & x[0] \\ \vdots & \vdots & \ddots & \vdots \\ x[N-1] & x[0] & \cdots & x[N-2] \end{pmatrix}}_{G=ZW^{-1}} \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega_N^{-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_N^{-(N-1)k} \end{pmatrix}}_{W}. \end{aligned}$$

Por lo tanto, de la ecuación (12), se obtiene

$$\underbrace{\begin{pmatrix} x[0] & x[1] & \cdots & x[N-1] \\ x[1] & x[2] & \cdots & x[0] \\ \vdots & \vdots & \ddots & \vdots \\ x[N-1] & x[0] & \cdots & x[N-2] \end{pmatrix}}_{G} \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega_N^{-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_N^{-(N-1)k} \end{pmatrix}}_{W} \underbrace{\begin{pmatrix} \overline{y}[0] \\ \overline{y}[1] \\ \vdots \\ \overline{y}[N-1] \end{pmatrix}}_{\overline{y}} = \underbrace{\begin{pmatrix} \mathcal{A}^{\mathbf{2}}_{x,y}[0,k] \\ \mathcal{A}^{\mathbf{2}}_{x,y}[1,k] \\ \vdots \\ \mathcal{A}^{\mathbf{2}}_{x,y}[N-1,k] \end{pmatrix}}_{b_k},$$

por lo tanto

$$GW\overline{y} = b_k. \qquad (13)$$

Ahora, sea $R_N \in \mathbb{C}^{N\times N}$ una matriz de reflexión. Para este caso, una propiedad de una matriz de reflexión es $R_N G = C_x$, donde C_x es una matriz circulante con respecto al vector x. Entonces, de la ecuación (13) se obtiene

$$R_N G W \overline{y} = R_N b_k \Rightarrow C_x W \overline{y} = R_N b_k. \tag{14}$$

Asumiendo que $\mathcal{F}_x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$, entonces C_x es invertible [8], y su inversa se representa por $C_x^{-1} = \frac{1}{N} F_N D \overline{F_N}$, donde $D \in \mathbb{C}^{N\times N}$ es una matriz diagonal tal que

$$D = \left(\frac{1}{\mathcal{F}_x[0]}, \frac{1}{\mathcal{F}_x[1]}, \ldots, \frac{1}{\mathcal{F}_x[N-1]} \right).$$

Por lo tanto

$$\begin{aligned} C_x W \overline{y} = R_N b_k \quad &\Rightarrow \quad y = \overline{W^{-1} C_x^{-1} R_N b_k} \\ &\Rightarrow \quad y = \tfrac{1}{N} W \overline{F_N}\, \overline{D} F_N R_N \overline{b_k}. \end{aligned}$$

Lo anterior prueba el siguiente resultado:

Teorema 4 *Sea $x, y \in \mathbb{C}^N$ tal que $\mathcal{F}_x[k] \neq 0$, para todo $k \in \mathbb{Z}_N$ y $A^{\mathbf{2}}_{x,y} \in \mathbb{C}^{N\times N}$ representa a la matriz FDA (ecuación 6). Entonces*

$$y = \frac{1}{N} W \overline{F_N}\, \overline{D} F_N R_N \overline{b_k}, \tag{15}$$

donde

- $W \in \mathbb{C}^{N\times N}$ *tal que* $W = diag\left(1, \omega_N^{-k}, \ldots, \omega_N^{-(N-1)k}\right)$.
- $D \in \mathbb{C}^{N\times N}$ *tal que* $D = \left(\frac{1}{\mathcal{F}_x[0]}, \frac{1}{\mathcal{F}_x[1]}, \ldots, \frac{1}{\mathcal{F}_x[N-1]} \right)$.
- $R_N \in \mathbb{C}^{N\times N}$ *es la matriz de reflexión de orden* N.
- $b_k \in \mathbb{C}^N$ *tal que* $b_k[m] = \left(A^{\mathbf{2}}_{x,y}\right)_{m,k}$.

El Algoritmo 3 muestra la implementación del método explicado anteriormente.

Algoritmo 3 Proceso para descifrar el mensaje z.

Entrada: $w \in \mathbb{C}^{N+2}$ (clave), $z \in \mathbb{C}^N$ (mensaje cifrado).

Salida: $y \in \mathbb{C}^N$ (mensaje original).

1: $v_0 \leftarrow \overline{z}$
2: $v_1 \leftarrow \mathcal{R}\{v_0\}$ (Operador de reflexión)
3: $v_2 \leftarrow \mathcal{F}\{v_1\}$
4: $v_3 \leftarrow w[2 : N+1]$
5: $v_4 \leftarrow \mathcal{F}_{v_3}$
6: $v_6 \leftarrow v_2 \odot v_5$, donde $v_5[n] = \frac{1}{v_4[n]}$
7: $v_7 \leftarrow \mathcal{F}^{-1}\{v_6\}$
8: $k \leftarrow w[1]$
9: $y \leftarrow v_7 \odot v_8$, donde $v_8[n] = \omega_N^{-nk}$

Para la matriz FDA que se genera a partir de la ecuación (3), se obtiene un resultado equivalente con un procedimiento similar, el cual se expresa en el siguiente teorema.

Teorema 5 *Sea $x, y \in \mathbb{C}^N$ tal que $\mathcal{F}_x[k] \neq 0$, para todo $k \in \mathbb{Z}_N$ y $A^{\mathbf{1}}_{x,y} \in \mathbb{C}^{N\times N}$ representa a la matriz FDA (ecuación (5)). Entonces*

$$y = \frac{1}{N}\overline{F_N}\, S_{-k}\overline{D}S_k F_N R_N \overline{b_k}, \tag{16}$$

donde

- *$F_N \in \mathbb{C}^{N\times N}$ es la matriz de la transformada discreta de Fourier de orden N.*
- *$S_k, S_{-k} \in \mathbb{C}^{N\times N}$ son la representación matricial de los operadores de traslación $\mathcal{S}_k$ y $\mathcal{S}_{-k}$ respectivamente.*
- *$D \in \mathbb{C}^{N\times N}$ tal que $D = \left(\frac{1}{\mathcal{F}_x[0]}, \frac{1}{\mathcal{F}_x[1]}, \dots, \frac{1}{\mathcal{F}_x[N-1]}\right)$.*
- *$R_N \in \mathbb{C}^{N\times N}$ es la matriz de reflexión de orden N.*
- *$b_k \in \mathbb{C}^N$ tal que $b_k[m] = \left(A^{\mathbf{1}}_{x,y}\right)_{m,k}$.*

4 Conclusiones

Este trabajo ha presentado un nuevo procedimiento de codificación criptográfica a través del diseño de algoritmos para cifrar y descifrar mensajes utilizando técnicas de Procesamiento Computacional de Señales. En particular, se ha presentado un nuevo método criptográfico basado en representaciones armónicas bidimensionales como entes codificadores de mensajes. La finalidad del procedimiento de codificación tiene como objetivo fundamental el intercambio de mensajes desde un punto a otro en espacio-tiempo, de tal manera que la información contenida en estos mensajes no pueda ser extraída por usuarios no autorizados.

El trabajo presentado se ha contextualizado bajo el esquema de Teoría de Información la cual estudia técnicas de codificación que permitan la transmisión y recepción de mensajes desde un punto a otro en espacio-tiempo. Bajo este contexto, el procedimiento de cifrar un mensaje se puede presentar como el envío de este mensaje a través de un canal de comunicación el que tendrá como entrada al mensaje no cifrado y el cual procederá a cifrar dicho mensaje. La salida del canal se convertirá, entonces, en el mensaje cifrado. Esta modalidad permitirá en el futuro combinar el uso de herramientas del área de Teoría de Información, tales como entropía no aditiva y funcionales de mínima divergencia, con herramientas del área de Procesamiento Computacional de Señales, tales como álgebra tensorial de señales y campos aleatorios generalizados, para abordar problemas relacionados con el uso de este nuevo método criptográfico en la comunicación sobre canales de dispersión en tiempo-frecuencia de múltiples entradas y múltiples salidas.

Una ventaja de este enfoque es que se puede utilizar una implementación en paralelo, y así, reducir el tiempo de computo [17, 16]. Además, la implementación del computo de la transformada discreta de Fourier, los productos Kronecker y Hadamard pueden realizarse de una forma eficiente, ver por ejemplo [8]. Por lo tanto, el computo matricial de todos resultados obtenidos en los teoremas presentados anteriormente, pueden ser calculados de una manera eficiente.

Finalmente destacar que el nuevo procedimiento criptográfico presentado en este trabajo podría abarcar aplicaciones en el área que actualmente se conoce como Criptografía Visual y la cual consiste en el intercambio de mensajes en donde cada mensaje está conformado por una imagen compuesta por píxeles negros y blancos.

Agradecimientos

Este artículo fue financiado por el Instituto Tecnológico de Costa Rica, a través de la Vicerrectoría de Investigación y Extensión.

Referencias

[1] M. An, A. K. Brodzik, R. Tolimieri, *Ideal Sequence Design in Time-Frequency Space: Applications to Radar, Sonar, and Communication Systems*, Applied and Numerical Harmonic Analysis, Birkhäuser, 2008.

[2] J. J. Benedetto, J. J. Donatelli, *Frames and a vector-valued ambiguity function*, 42nd Asilomar Conference on Signals, Systems and Computers, 2008, pp. 8–12.

[3] J. J. Benedetto, I. Konstantinidis and M. Rangaswamy, *Phase-coded waveforms and their design*, IEEE Signal Processing Magazine **26** (2009), no. 1, 22–31.

[4] B. Boashash, *Time Frequency Signal Analysis and Processing: A Comprehensive Reference*, Elsevier, 2003.

[5] J. W. Cooley, J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series*, Mathematics of Computation **19** (1965), no. 90, 297–301.

[6] P. J. Davis, *Circulant Matrices (Pure & Applied Mathematics)*, Chelsea Publishing Series, Chelsea, 1994.

[7] F. Franchetti, M. Puschel, Y. Voronenko, S. Chellappa, J. M. F. Moura, *Discrete fourier transform on multicore*, IEEE Signal Processing Magazine **26** (2009), no. 6, 90–102.

[8] G. H. Golub, C. F. Van Loan, *Matrix Computations*, Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, 1996.

[9] A. Graham, *Kronecker products and matrix calculus with applications*, Ellis Horwood series in mathematics and its applications, Horwood, 1981.

[10] J. Hoffstein, J. Piphe, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Undergraduate texts in mathematics, Springer, New York, 2008.

[11] J. R. Johnson, R. W. Johnson, D. Rodriguez, R. Tolimieri, *A methodology for designing, modifying, and implementing Fourier transform algorithms on various architectures*, Circuits, Systems, and Signal Processing **9** (1990), no.4, 449–500.

[12] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, Discrete Mathematics and Its Applications, CRC Press, 1996.

[13] C. D. Moravitz, C. F. Van Loan, *A jacobi-type method for computing orthogonal tensor decompositions*, SIAM J. Matrix Anal. Appl. **30** (2008), no. 3, 1219–1232.

[14] P. A. Regalia and S. K. Mitra, *Kronecker products, unitary matrices, and signal processing applications*, SIAM Rev. **31** (1989), no. 4, 586–613.

[15] M. S. Richman, T. W. Parks, R. G. Shenoy, *Discrete-time, discrete-frequency, time-frequency analysis*, IEEE Transactions on Signal Processing **46** (1998), no. 6, 1517–1527.

[16] P. Soto-Quirós, *A mathematical framework for parallel computing of discrete-time discrete-frequency transforms in multi-core processors*, Applied Mathematics & Information Sciences **8** (2014), no. 6, 2795–2801.

[17] J. P. Soto-Quirós, D. Rodríguez, *Representación matricial de algoritmos en paralelo de la transformada discreta de Fourier, la función discreta de ambiguedad y la distribución discreta de Cohen*, Gaceta de la Real Sociedad Matematica Española **16** (2013), no. 3, 479–500.

[18] R. Tolimieri, M. An, C. Lu, *Algorithms for Discrete Fourier Transform and Convolution*, Signal Processing and Digital Filtering, Springer, New York, 1997.

[19] P. M. Woodward, *Probability and Information Theory: with Applications to Radar*, McGraw-Hill, New York, 1953.