Encriptación cuántica y clásica de imágenes a través de aplicaciones caóticas

Zayda Paola Reyes Quijano

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Física

Bucaramanga

2015

Encriptación cuántica y clásica de imágenes a través de aplicaciones caóticas

Zayda Paola Reyes Quijano

trabajo de grado
para optar al título de física

Director: PhD. Leonardo Augusto Pachón Contreras
Codirector: PhD. Rafael Ángel Torres Amarís

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Física
Bucaramanga
2015

A *mis padres,*

Alfredo Reyes
y Gloria Quijano

Agradecimientos

A mi director el profesor Leonardo A. Pachón y a mi codirector el profesor Rafael A. Torres, por la oportundad de trabajar con ellos en este interesante tema, por su tiempo, paciencia y dedicación.

A los calificadores de mi trabajo, el profesor Arturo Plata y el profesor William Gutiérrez, por su tiempo y colaboración.

A los profesores que se han esforzado durante años para compartir sus conociemientos, en particular, el profesor Ilia Davidovich Mikhailov, el profesor Luis Núñez, el profesor Rafael Cabanzo, el profesor Harold Paredes y el profesor Guillermo González, gracias por contribuir en mi formación como Física.

A mis padres, Alfredo Reyes y Gloria Quijano, y a mi hermano Alfredo Reyes "Jr" por su cariño y confianza durante toda mi vida, quiero expresar mi más profundo agradecimiento por nuestra maravillosa y unida familia, sin su apoyo no hubiese sido posible terminar mi pregrado.

A mis compañeros, Joseph Vergel, Diego Galeano, Oswaldo Nieto, Oscar Forero, y Elkin Santos, gracias por las discusiones académicas, por su compañía y palabras de ánimo cuando más las necesitaba.

Finalmente y de manera especial, a César Pachón por su contribución a este trabajo, por su comprensión y apoyo incondicional, gracias no sólo por las discusiones sobre diversos temas de física, sino también por ser el amigo y novio que me ha acompañado durante cinco años, y con quien he compartido tantas alegrías.

Índice general

Índice de figuras

Resumen

TÍTULO: Encriptación cuántica y clásica de imágenes a través de aplicaciones caóticas. [⋆]

AUTOR: Paola Reyes Q.[†]

PALABRAS CLAVES: Aplicación del panadero, tiempo continuo, encriptación, transformación de Fourier fraccionaria.

DESCRIPCIÓN:

La transformación de Fourier de orden fraccionario α (FrFT) ha sido estudiada recientemente debido a su utilidad en diferentes áreas de la física, como en el procesamiento de señales. Con el objetivo de garantizar la confidencialidad de la información durante su transmisión, en este trabajo se extiende la aplicabilidad de esta transformación al contexto de la encriptación de imágenes, haciendo uso de rotaciones de ángulo arbitratio α para generalizar la versión cuántica de la aplicación del panadero al caso de *tiempo continuo*.

A través de la generalización de la aplicación del panadero se realiza encriptación a nivel cuántico, de imágenes codificadas en un estado físico. La eficacia del proceso de encriptación se establece mediante el análisis del histograma y el cálculo de la calidad de encriptación de las imágenes y se establece que la aplicación de *tiempo continuo* permite obtener mayor control y nivel de la encriptación. El uso de imágenes que pueden ser codificadas en un estado físico permite la posibilidad de realizar una implementación experimental de esta aplicación en un computador cuántico, haciendo uso de compuertas cuánticas para realizar las rotaciones correspondientes a la transformación de Fourier fraccionaria, con la perspectiva de estudiar la dinámica de los sistemas caóticos en *tiempo continuo*.

[⋆] Trabajo de Grado.

[†] Escuela de Física, Facultad de Ciencias, Universidad Industrial de Santander. Director: Prof. Leonardo A. Pachón. Codirector: Prof. Rafael A. Torres.

Abstract

TITLE: Quantum and Classical Images Encryption through Chaotic Maps [*]

AUTHOR: Paola Reyes Q. [†]

KEYWORDS: Baker's map, continuous time, encryption, Fractional Fourier transform.

DESCRIPTION:

Fractional Fourier transform of order α (FrFT) has recently been studied due to its usefulness in different of brands physics, as in signal processing. In order to guarantee the confidentiality of the information throughout its transmission, here we extend the applicability of the FrFT to the context of image encryption, making rotations by an arbitrary angle α to generalize the quantum version of the Baker's map to the case of *continuous time*.

Using the generalized version of the map we encrypt at quantum level, images that can be encoded in a physical state. The efficiency of the encryption process is established by analyzing the histogram and calculating encryption quality of the encypted images.The generalization of the map to the case of *continuous time* allows improving the control and level of encryption, and the use of images that can be encoded in a physical state allows the possibility of an experimental implementation of this map on a quantum computer, making use of quantum gates to realize the rotations corresponding to the fractional Fourier transform, with the perspective of studying the dynamics of chaotic systems in *continuous time*.

[*] Degree work.

[†] Escuela de Física, Facultad de Ciencias, Universidad Industrial de Santander. Director: Prof. Leonardo A. Pachón. Codirector: Prof. Rafael Torres Amarís.

Notación

A,M	Matrices
$\hat{\square}$	Operador en el espacio de Hilbert
$\hat{\rho}$	Operador matriz densidad
$\square_{\mathrm{W}}$	Símbolo de Weyl del operador $\hat{\square}$
$\hat{U}$, U_{W}	Operador unitario de evolción temporal y el asociado al símbolo de Weyl
ρ_{W}	Función de Wigner asociada a $\hat{\rho}$
$G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}', t')$	Propagador de Wigner para $\mathbf{r}'$ en $t = t'$ a $\mathbf{r}''$ en $t = t''$
i, i^*	Unidad imaginaria y su complejo conjugado

Introducción

La importancia y necesidad de transmitir información confidencial de manera rápida y segura ha provocado la creación de una gran variedad de criptosistemas basados en la teoría de los números [13], en algoritmos matemáticos [2] o en términos de aplicaciones dinámicas caóticas (dynamical chaotic maps) [17]. Para entender el concepto de aplicaciones dinámicas, que es un concepto fundamental en este trabajo de grado, es importante notar que, en general, la evolución temporal de estos sistemas se describe mediante ecuaciones diferenciales. Sin embargo, dada su complejidad, se dio la necesidad de simplificar su estudio por medio de aplicaciones dinámicas. Una aplicación describe la transformación general de un sistema, y su iteración corresponde a la evolución del sistema en tiempo discreto.

Las aplicaciones dinámicas han sido utilizadas en la encriptación de imágenes debido a que comparten algunas propiedades con los criptosistemas [17]. En particular, al igual que en los sistemas caóticos, una pequeña variación en las condiciones de encriptación hace que el criptosistema evolucione de manera totalmente distinta. En estos sistemas, cuando se cambia un bit del texto plano o de la clave de cifrado, el texto cifrado se modifica totalmente. Una de estas aplicaciones es la del panadero [17,27]. Esta aplicación expande el espacio de fase (horizontalmente) a lo largo de la posición q y lo contrae (verticalmente) a lo largo de la coordenada de momento p; posteriormente, el espacio de fase se divide verticalmente a la mitad, y la parte derecha se rota un ángulo $\alpha = \pi$. De manera que la parte que rota, se ubica sobre la parte izquierda del rectángulo, conservando así, el área del espacio de fase (ver capítulo 2 para más detalles). En la versión cuántica, la expansión y la contracción se realizan a través de operaciones unitarias que se describen en el capítulo 2, mientras que la rotación se realiza utilizando la transformación de Fourier [7,27]. Este hecho es fundamental en la generalización de este trabajo. Es importante notar que, tanto la versión clásica como la cuántica van más allá del ambito teórico pues se han implementado experimentalmente [9,11,34] y, van más allá del ámbito académico, pues se han utilizado en la encriptación de imágenes [1,17,33].

Aunque los algoritmos diseñados para encriptar imágenes a través de la aplicación del panadero son relativamente eficientes para imagénes pequeñas ($\sim$1024$\times$1024 píxeles) [33], la naturaleza discreta del tiempo hace que para generar una encriptación segura, la aplicación debe aplicarse un número muy grande de veces. Aquí, se generaliza la versión cuántica de la aplicación del panadero al caso de tiempo continuo (rotaciones por un ángulo α arbitrario), que en principio reduciría el número de iteraciones (ver capítulo 3).

Durante la construcción de la aplicación del panadero de tiempo continuo, fue necesario estudiar la función de Wigner y el propagador de la función de Wigner en espacio de fase discreto. En el capítulo 1 se define, en general, el proceso encriptación de información y se justifica el uso de aplicaciones caóticas en dicho proceso, la formulación de la versión clásica y cuántica de la aplicación del panadero en tiempo discreto se presenta en el capítulo 2, así como la definición de la transformación de Fourier finita de orden fraccionario, utilizada en la construcción de la versión cuántica de *tiempo continuo* de la aplicación. Además, allí se discute el uso de la definición no reduntante de la función de Wigner, y su correspondiente propagador, sobre un espacio de fase de simetría toroidal, así mismo se presentan las propiedades más relevantes de estos. En el capítulo 3, se describe el proceso de encriptación de

imágenes y se comparan las imágenes encriptadas obtenidas con las versiones de tiempo discreto y *tiempo continuo*. Además, se verifica la calidad de este proceso a través de dos métodos estándar de certificación de encriptación como el análisis de histograma y el cálculo de la calidad de encriptación. Aunque el operador FrFT forma un semigrupo parametrizado por el ángulo α, se encontró que la aplicación en *tiempo continuo* no forma un semigrupo en α y por tanto, la formulación de *tiempo continuo* es sólo aproximada. En el capítulo 3 también se discute como tomar ventaja de este hecho para incrementar el nivel de encriptación. En el capítulo 4 se propone la implementación de la aplicación utilizando compuertas cuánticas con la perspectiva de realizar experimentos que permitan profundizar en el estudio de la dinámica cuántica de los sistemas clásicamente caóticos. Por último, las conclusiones del trabajo se presentan en el capítulo 5.

CAPÍTULO 1

Encriptación de información con aplicaciones dinámicas

En este capítulo se describe, de forma general, en que consiste la encriptación de información y se justifica el uso de aplicaciones dinámicas en este proceso.

1.1 Encriptación de información

Los avances tecnológicos han permitido extender los límites de la transmisión de información y de las comunicaciones. Sin embargo, la necesidad de mantener cierta información en secreto, como los datos de una transferencia bancaria electrónica, ha producido un aumento en la búsqueda de formas de protección de datos que deben ser guardados o transmitidos de forma confidencial y segura, la criptografía es la ciencia encargada de esto. Las técnicas criptográficas normalmente están basadas en la teoría de números o en algoritmos matemáticos. Cifrar es un procedimiento que consiste en transformar información utilizando un algoritmo con una clave, llamada clave de cifrado, en un mensaje ilegible. Sólo quien posea la clave correspondiente al algoritmo de descifrado puede convertir este mensaje en la información inicial. Si las claves de cifrado y descifrado son iguales, la criptografía es simétrica, de otro modo es llamada asimétrica. Existen muchos tipos de encriptación, pero según la forma en la que operan los algoritmos se clasifican en dos:

- **Encriptación en flujo.** En este tipo el cifrado se realiza bit a bit. Es muy utilizado en las telecomunicaciones donde el cifrado deber ser rápido; por ejemplo, en una conversación telefónica la voz se convierte en un flujo de bits. Su mayor ventaja está en el uso de claves aleatorias muy largas, tanto para cifrar como para descifrar. Estas llaves pueden ser predeterminadas o creadas por un generador pseudoaleatorio que, partiendo de un mismo valor de entrada o clave, genera el mismo flujo de bits de salida.
- **Encriptación por bloques.** Es un tipo de cifrado simétrico que se realiza bloque a bloque. Un bloque es un grupo de bits de longitud fija en que se divide la información original mediante sustituciones (reemplazo de un valor de entrada por otro de los posibles valores de salida) y permutaciones (tipo especial de sustitución, los bits de un bloque de entrada son reordenados para producir el bloque cifrado). En este proceso se conserva el número de unos y ceros del

bloque de entrada que es cifrado. Este tipo de cifrado es más costoso computacionalmente, pero brinda seguridad contra ataques de "fuerza bruta" a pesar de tener claves de 128 o 256 bits, que son cortas en comparación con el cifrado en flujo.

La encriptación cuántica se basa en codificar información usando sistemas cuánticos. Como consecuencia del principio de incertidumbre de Heisenberg, en el momento que una tercera persona intenta leer la información encriptada, ésta es modificada, es decir, la tercera persona perturba el estado del sistema cuántico [18]. De manera que cuando la información llegue a su destino, el receptor sabrá que alguien intentó acceder a su información porque ésta será diferente a la inicial. Por tanto, en teoría, es una forma absolutamente segura de encriptación. En el caso de encriptación en el espacio de fase, el caso abordado en esta tesis, la no-localidad dinámica [22] deberá en principio, potencializar el proceso de encriptación.

1.2 Aplicaciones dinámicas

Como se mencionó arriba, en general, la evolución de los sistemas se da por medio de ecuaciones diferenciales. Estas ecuaciones son muy complejas en el caso de los sistemas cuyo comportamiento es caótico, por esta razón se utilizan aplicaciones dinámicas.

Ya que algunas propiedades de los sistemas caóticos son similares a las de los criptosistemas tradicionales, también existen técnicas basadas en el comportamiento de aplicaciones caóticas. Específicamente, cualquier sistema criptográfico debe:

- Convertir el texto plano (mensaje inicial) en un texto cifrado aleatorio (mensaje cifrado) que no tenga ningún patrón.
- Ser sensible respecto al texto plano, es decir, al cambiar un bit del texto plano, el texto cifrado que se crea es completamente diferente al que se crearía si no se hubiese cambiado el bit.
- Ser sensible respecto a las claves, es decir, al cambiar un bit en la clave crea un texto cifrado completamente diferente.

La encriptación de imágenes a través de aplicaciones caóticas se ha realizado a nivel clásico y cuántico [1,17]. Una de las aplicaciones clásicas utilizadas corresponde a la aplicación del panadero cuya versión clásica es continua en el espacio y discreta en el tiempo, mientras que la versión cuántica es discreta tanto en el espacio como en el tiempo, esta aplicación es discutida en el siguiente capítulo.

CAPÍTULO 2

Aplicación del panadero en el espacio de fase

En este capítulo se presenta la definición clásica y cuántica de esta aplicación y se discute el uso de la transformación de Fourier fraccionaria en la construcción de la versión cuántica de tiempo continuo de la aplicación del panadero.

2.1 Versión clásica de la aplicación del panadero

La aplicación del panadero se define a través de las ecuaciones de transformación

$$(q,p) = \begin{cases} (2q, \frac{1}{2}p), & \text{para} \quad 0 \leq q < \frac{1}{2}, \\ (2q-1, \frac{1}{2}(p+1)), & \text{para} \quad \frac{1}{2} < q \leq 1. \end{cases} \tag{2.1}$$

La aplicación del panadero presenta sensibilidad a las condiciones iniciales debido al estiramiento en la dirección q y posee inmumerables órbitas caóticas [7, 14]. La figura 2.1 ilustra en que consiste la transformación

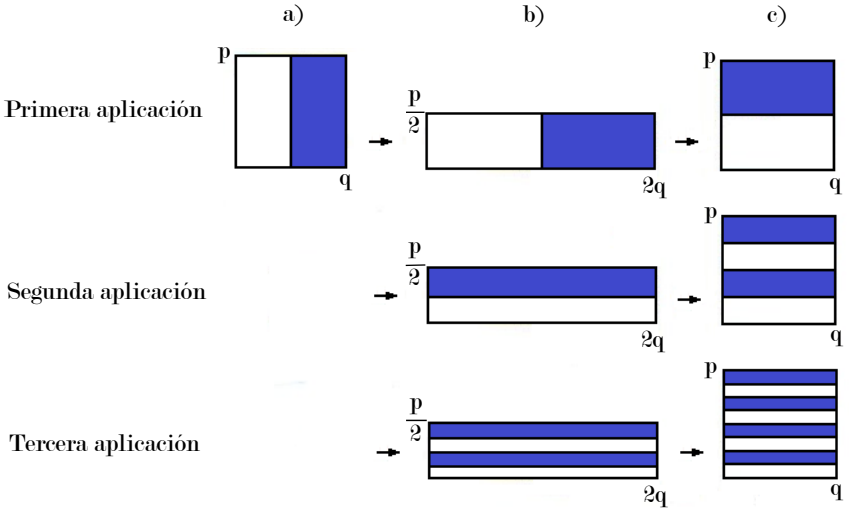


Figura 2.1: Aplicación del panadero para tres iteraciones. El conjunto de imágenes de la primera fila describe la primera aplicación. a) El espacio de fase se estira en la posición y se contrae en el momento, convirtiéndose así en un rectángulo de $2q * \frac{p}{2}$. b) Después, simulando la forma en que un panadero amasa, la aplicación corta el espacio de fase a la mitad y, c) la parte derecha se ubica sobre la parte izquierda.

La relación entre los criptosistemas y los sistemas caóticos ha sido estudiada creando un esquema de encriptación simétrica por bloques y adaptando aplicaciones caóticas invertibles de 2D a aplicaciones sobre un toro o un cuadrado [17]. Una de las aplicaciones utilizadas corresponde a la aplicación del panadero, la cual es generalizada, y posteriormente discretizada en una red cuadrada de puntos (que representan píxeles), resultando un cifrado simple, rápido y seguro [17]. El análisis se ha extendido a versiones 3D de la aplicación [33]. En este trabajo se construye una versión de la aplicación del panadero de *tiempo continuo* con la que se aumenta la calidad de encriptación de imágenes, a través de (i) la adición de un nuevo parámetro de control y (ii) la violación de la ley de composición en el nuevo parámetro.

Para cuantizar la aplicación del panadero, y posteriormente poder realizar una comparación con la versión clásica, es necesario escribir el espacio de Hilbert en términos de funciones definidas sobre el espacio de fase como se establece en la siguiente sección.

2.2 Dinámica cuántica en el espacio de fase discreto

La mecánica cuántica puede ser formulada en el espacio de fase (q, p), posición y momento respectivamente, de manera similar a la mecánica clásica en términos conceptuales y operacionales mediante la construcción de una distribución de cuasi-probabilidad [4, 23]. La distribución más utilizada corresponde a la función de Wigner que permite estudiar en forma natural el límite semiclásico y que por tanto, es necesaria cuando se desea realizar un estudio cuántico de sistemas que son clásicamente caóticos [8, 15, 20]. En esta sección se introduce esta formulación de la dinámica cuántica en el espacio de fase discreto.

2.2.1. Operador densidad

Para estudiar ensambles cuánticos utilizando un formalismo similar al análisis estadístico clásico, es necesario introducir el concepto de probabilidad estadística [10] porque, en general, el estado de un sistema físico es una mezcla no coherente, es decir, que no contiene toda la información del ensamble. De modo que es posible suponer que un sistema tiene una probabilidad P_i de estar en un estado $|\phi_i\rangle$, donde $i = 1, 2, 3, ...$ y los P_i están restringidas por

$$0 \leq P_i \leq 1, \tag{2.2}$$

$$\sum_k P_i = 1, \tag{2.3}$$

es decir, se tiene una mezcla estadística de estados $|\phi_1\rangle$,$|\phi_2\rangle$, etc, con probabilidades P_1,P_2, etc. Entonces el operador densidad $\hat{\rho}$ se define como

$$\hat{\rho} = \sum_i P_i |\phi_i\rangle\langle\phi_i|, \tag{2.4}$$

que describe tanto estados mezclados como puros. Un sistema cuántico estará en un estado puro si $\mathrm{tr}[\hat{\rho}^2] = 1$.

Algunas de las propiedades del operador densidad son:

- Es autoadjunto y acotado.
- Es un operador cuya traza es igual a la unidad $\mathrm{tr}[\hat{\rho}] = 1$. Esto implica que $\sum_i p_i = 1$.
- Es un operador compacto y por tanto sus autovectores forman una base ortonormal, y si $\hat{\rho}|\psi_i\rangle = q_j|\psi_i\rangle$ entonces $q_j \geq 0 \ \forall \ j$.
- El valor medio de un observable $\hat{A}$ del sistema de estados mezclados se define como el promedio estadístico, con pesos p_i, de sus valores medios en los estados puros $|\psi_i\rangle$ con que se construyó el estado mezclado, es decir,

  $$\langle\hat{A}\rangle = \sum_{i=1} p_i \langle\psi_i|\hat{A}|\psi_i\rangle = \mathrm{tr}[A\hat{\rho}]. \tag{2.5}$$

  De manera que se tiene la posibilidad de expresar el valor esperado de un observable en términos de la traza del producto de éste con el operador densidad.

2.2.2. Función de Wigner

En 1932 Wigner asoció [31] el operador densidad definido en la expresión (2.4) con una función de cuasi-probabilidad en el espacio de fase cuántico, que se conoce como función de Wigner, esto con el fin de estudiar correlaciones cuánticas análogamente a la mecánica estadística clásica. A esta función también se le llama distribución de Wigner de cuasi-probabilidad. La función de Wigner está definida como la transformada de Weyl [30] del operador densidad multiplicada por $\frac{1}{2\pi\hbar}$, i.e.,

$$\rho_{\mathrm{W}}(\mathbf{p}, \mathbf{q}) = T_{\mathrm{W}}\left[\frac{\hat{\rho}}{2\pi\hbar}\right], \tag{2.6}$$

donde ρ_{W} representa la función de Wigner.

En la cuantización de la aplicación caótica se establecen condiciones de contorno periódicas para el espacio de fase (ver sección 2.3), que lo convierten en una superficie homogénea (un toro). Por tanto, es necesario utilizar la función de Wigner correspondiente al espacio geométrico con este tipo de geometría.

En representación del momento, la función de Wigner sobre un espacio toroidal toma la forma [4, 5, 16, 23],

$$\rho_{\mathrm{W}}(p_\mu, q_\mu, t) = \sum_{\mu'}^{2N-1} \frac{1+(-1)^{\mu+\mu'}}{2} \left\langle \frac{\mu+\mu'}{2} \middle| \hat{\rho}(t) \middle| \frac{\mu-\mu'}{2} \right\rangle \exp\left[\mathrm{i}\frac{\pi n \mu}{N}\right], \tag{2.7}$$

donde $\mu, n = 0, 1, 2, ..., 2N$. Esta función contiene información adicional que es redundante y que forma patrones de interferencia virtual, los cuales pueden sobrelapar los patrones de interferencia cuánticos [5]. La ecuación (2.7) se conoce como la definición redundante de la función de Wigner [4].

Para el estudio cuántico de sistemas clásicamente caóticos, es necesario que desaparezcan los patrones de interferencia virtual. Por tanto, se utiliza la definición no redundante de la función de Wigner [4, 5, 16, 23].

Para $\hat{\rho}$, en representación de coordenadas, se tiene

$$\bar{\rho}_{\mathrm{W}}(\mu, m) = \frac{1}{2N} \sum_{n'=-N}^{N-1} \frac{1+(-1)^{n+n'}}{2} \left\langle \frac{n+n'}{2} \middle| \hat{\rho} \middle| \frac{n-n'}{2} \right\rangle \exp\left[-2\mathrm{i}\frac{\pi n' \mu}{2N}\right], \tag{2.8}$$

con,

$$\delta_n^m = \begin{cases} 1, & \text{si} \quad Par(n) = Par(m), \\ 0, & \text{si} \quad Par(n) \neq Par(m). \end{cases} \tag{2.9}$$

donde $Par(n)$ corresponde a la paridad del número n, de modo que la ecuación (2.8) se puede escribir como

$$\bar{\rho}_{\mathrm{W}}(\mu, n) = \mathcal{F}_{2N}\left[\delta_n^{n'} \rho_{n'/2}^{n/2}\right]. \tag{2.10}$$

A continuación se realiza una transformación de Fourier de la matriz densidad en la dirección n con el fin de separar espacialmente la información necesaria de los patrones de interferencia virtual

$$\begin{aligned} \bar{\rho}_{n'\lambda} &= \mathcal{F}_{2N}\left[\delta_n^{n'} \rho_{n/2}^{-n'/2}\right] \\ &= \frac{1}{2N} \sum_{n=-N}^{N-1} \frac{1+(-1)^{n+n'}}{2} \left\langle \frac{n+n'}{2} \middle| \hat{\rho}(t) \middle| \frac{n-n'}{2} \right\rangle \exp\left[-2\mathrm{i}\pi \frac{n\mu'}{2N}\right]. \end{aligned} \tag{2.11}$$

Luego se extrae la información de interés de la parte central de este espacio y finalmente se realiza una transfomación de Fourier doble

$$\begin{aligned} \rho_{\mu m} = \frac{1}{N^2} \sum_{n'} \sum_{\mu'} \sum_{n}^{2N} & \frac{1+(-1)^{n+n'}}{2} \left\langle \frac{n+n'}{2} \middle| \hat{\rho}(t) \middle| \frac{n-n'}{2} \right\rangle \\ & \times \exp\left[-2\mathrm{i}\pi \frac{n\mu'}{2N}\right] \exp\left[2\mathrm{i}\pi \frac{m\mu'}{N}\right] \exp\left[-2\mathrm{i}\pi \frac{n'\mu}{N}\right], \end{aligned} \tag{2.12}$$

de manera que

$$\rho_{\mathrm{W}}(p_\mu, q_n, t) = \frac{1}{N} \sum_{n'} \sum_{n}^{2N} \delta_n^{n'} \left\langle \frac{n+n'}{2} \middle| \hat{\rho}(t) \middle| \frac{n-n'}{2} \right\rangle \widetilde{\delta}(2m-n) \exp\left[-2\mathrm{i}\pi \frac{n'\mu}{N}\right], \tag{2.13}$$

donde

$$\tilde{\delta}(k) = \frac{1}{N}\frac{\sin(\pi k/2)}{\sin(\pi k/2N)}, \tag{2.14}$$

y $\widetilde{\delta}(2k) = \delta(k)$. ρ_{W} corresponde a la función de Wigner sobre un espacio toroidal discreto sin información redundante.

Propiedades de la función de Wigner

Las propiedades más relevantes de la función de Wigner sobre un espacio de fase toroidal se presentan a continuación.

- La función de Wigner es real.

  Para comprobar esta propiedad, se calcula el complejo conjugado de la función de Wigner. Haciendo uso de la hermiticidad de $\hat{\rho}$, la ecuación (2.13) puede ser escrita como

$$\rho_{\mathrm{W}}(\mu, m) = \frac{1}{N}\sum_{n'=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta^{n}_{n'}\left\langle\frac{n+n'}{2}\middle|\hat{\rho}\middle|\frac{n-n'}{2}\right\rangle\exp\left[-2\mathrm{i}\pi\frac{n'\mu}{N}\right]\tilde{\delta}(2m-n), \tag{2.15}$$

  cuyo complejo conjugado es

$$\begin{aligned}
\rho^{*}_{\mathrm{W}} =& \frac{1}{N}\sum_{n'=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta^{n}_{n'}\left\langle\frac{n-n'}{2}\middle|\hat{\rho}\middle|\frac{n+n'}{2}\right\rangle\exp\left[2\mathrm{i}\pi\frac{n'\mu}{N}\right]\tilde{\delta}(2m-n)\\
&(n''=-n')\\
=&\frac{1}{N}\sum_{n''=-\frac{N}{2}+1}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta^{n}_{-n''}\left\langle\frac{n+n''}{2}\middle|\hat{\rho}\middle|\frac{n-n''}{2}\right\rangle\exp\left[-2\mathrm{i}\pi\frac{n''\mu}{N}\right]\tilde{\delta}(2m-n)\\
+&\frac{1}{N}\sum_{n=-N}^{N-1}\delta^{n}_{\frac{N}{2}}\left\langle\frac{n+\frac{N}{2}}{2}-2N\middle|\hat{\rho}\middle|\frac{n-\frac{N}{2}}{2}+2N\right\rangle\exp\left[-2\mathrm{i}\pi\frac{\frac{N}{2}\mu}{N}\right]\tilde{\delta}(2m-n)\\
=&\frac{1}{N}\sum_{n''=-\frac{N}{2}+1}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta^{n}_{-n''}\left\langle\frac{n+n''}{2}\middle|\hat{\rho}\middle|\frac{n-n''}{2}\right\rangle\exp\left[-2\mathrm{i}\pi\frac{n''\mu}{N}\right]\tilde{\delta}(2m-n)\\
+&\frac{1}{N}\sum_{n=-N}^{N-1}\delta^{n}_{-\frac{N}{2}}\left\langle\frac{n-\frac{N}{2}}{2}\middle|\hat{\rho}\middle|\frac{n+\frac{N}{2}}{2}\right\rangle(-1)^{\mu}\tilde{\delta}(2m-n)
\end{aligned} \tag{2.16}$$

  El término $n'' = \frac{n}{2}$ ha sido separado de la suma. En la última expresión es posible ver que este término coincide con uno para el cual $n'' = -\frac{N}{2}$. Luego de añadir un término $-\frac{N}{2}$ a la suma sobre n'' y de eliminar el término $\frac{N}{2}$ se obtiene que $\rho^{*}_{\mathrm{W}}(\mu, m) = \rho_{\mathrm{W}}(\mu, m)$. Por tanto, la función de Wigner es real.

- Provee las probabilidades marginales correctamente. La distribución marginal en la posición (momento) se obtiene al realizar una sumatoria sobre el momento (posición).

A partir de la definición (2.15), y haciendo uso de las funciones $\delta(k)$ y $\tilde{\delta}(k)$

$$\begin{aligned}\sum_{\mu=-\frac{N}{2}}^{\frac{N}{2}-1}\rho_{\mathrm{W}}(\mu,m) &= \sum_{n'=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta_n^{n'}\left\langle\frac{n+n'}{2}\right|\hat{\rho}\left|\frac{n-n'}{2}\right\rangle\tilde{\delta}(2m-n)\frac{1}{N}\sum_{\mu=-\frac{N}{2}}^{\frac{N}{2}-1}\exp\left[-2\mathrm{i}\pi\frac{n'\mu}{N}\right]\\ &= \sum_{n=-N}^{N-1}\delta_0^n\left\langle\frac{n}{2}\right|\hat{\rho}\left|\frac{n}{2}\right\rangle\tilde{\delta}(2m-n)\\ &\quad (n=2k)\\ &= \sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1}\langle k|\,\hat{\rho}\,|k\rangle\,\delta(m-k) = \langle m\,|\hat{\rho}|\,m\rangle\,.\end{aligned} \tag{2.17}$$

Por otro lado, para la probabilidad marginal en μ, escribiendo explícitamente $\tilde{\delta}(2m-n)$ se tiene

$$\begin{aligned}\sum_{m=-\frac{N}{2}}^{\frac{N}{2}-1}\rho_{\mathrm{W}}(\mu,m) =& \frac{1}{N}\sum_{n'=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\sum_{\mu'=-\frac{N}{2}}^{\frac{N}{2}-1}\delta_{n'}^{n}\left\langle\frac{n+n'}{2}\right|\hat{\rho}\left|\frac{n-n'}{2}\right\rangle\exp\left[-2\mathrm{i}\pi\frac{n'\mu}{N}\right]\exp\left[-2\mathrm{i}\pi\frac{\mu' n}{2N}\right]\\ &\times\frac{1}{N}\sum_{m=-\frac{N}{2}}^{\frac{N}{2}-1}\exp\left[2\mathrm{i}\pi\frac{\mu' m}{N}\right]\\ =& \frac{1}{N}\sum_{n'=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-N}^{N-1}\delta_n^{n'}\left\langle\frac{n+n'}{2}\right|\hat{\rho}\left|\frac{n-n'}{2}\right\rangle\exp\left[-2\mathrm{i}\pi\frac{n'\mu}{N}\right],\end{aligned} \tag{2.18}$$

finalmente se obtiene $\sum_{m=-\frac{N}{2}}^{\frac{N}{2}-1}\rho_{\mathrm{W}}(\mu,m) = \langle\mu|\,\hat{\rho}\,|\mu\rangle\,.$

2.2.3. Propagador de la función de Wigner

A continuación, se introduce el formalismo que determina la evolución de la función de Wigner y su relación con la transformación de Weyl.

La evolución temporal de un sistema bajo la acción de un hamiltoniano $\hat{H}$ está dada por la ecuación de Landau-von Newmann $\mathrm{i}\frac{\mathrm{d}\hat{\rho}}{\mathrm{d}t} = \left[\hat{H},\hat{\rho}\right]$, donde $\hat{\rho}$ corresponde a la matriz densidad del sistema, la solución de esta ecuación se puede escribir como

$$\rho_W(p_{\mu'},q_{m'},t') = \sum_{\mu=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{\mu=-\frac{N}{2}}^{\frac{N}{2}-1}G_W(p_{\mu',q_{m'},t';p_\mu q_{m'},t})\rho_W(p_\mu,q_m,t), \tag{2.19}$$

donde G_W es el propagador de la función de Wigner. El operador evolución $\hat{U}(t',t)$ se escribe como

$$\hat{U}(t',t) = \sum_a \exp\left[-\frac{\mathrm{i}}{h}E_a(t'-t)\right]|\phi_a\rangle\langle\phi_a|. \tag{2.20}$$

Al aplicar la transformación de Weyl al operador evolución se obtiene

$$U_W(p_\mu,q_m,t',t) = \sum_a \exp\left[-\frac{\mathrm{i}}{h}E_a(t'-t)\right]\Phi_{aa}(p_\mu,q_m), \tag{2.21}$$

que corresponde al **propagador de Weyl**. Partiendo de la expresión (2.20)

$$\hat{\rho}(t') = \hat{U}(t',t)\hat{\rho}(t)\hat{U}^{\dagger}(t',t), \tag{2.22}$$

y utilizando la expresión (2.21), $\hat{\rho}(t')$ se puede escribir como

$$\hat{\rho}(t') = \sum_{a=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{b=-\frac{N}{2}}^{\frac{N}{2}-1} \exp\left[-\frac{\mathrm{i}}{h}(E_a - E_b)(t'-t)\right] \langle\phi_a|\hat{\rho}(t)|\phi_b\rangle|\phi_a\rangle\langle\phi_b|, \tag{2.23}$$

aplicando la transformación de Weyl a la ecuación anterior, se obtiene

$$\rho_W(p_{\mu'}, q_{m'}, t') = \frac{1}{N}\sum_{a=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{b=-\frac{N}{2}}^{\frac{N}{2}-1} \exp\left[-\frac{\mathrm{i}}{h}(E_a - E_b)(t'-t)\right] \langle\phi_a|\hat{\rho}(t)|\phi_b\rangle\Phi_{ab}(p_{\mu'}, q_{m'}), \tag{2.24}$$

que es la función de Wigner en el tiempo t'. Teniendo en cuenta que al aplicar la transformada de Weyl a un operador $\hat{A} = \sum_{ab} A_{ab}|\phi_{ab}\rangle\langle\phi_b|$ se tiene

$$A_W(p_\mu, q_m) = \sum_{ab} A_{ab} T_W\left[|\phi_a\rangle\langle\phi_b|\right] = \sum_{ab} A_{ab}\Phi_{ab}(p_\mu, q_m), \tag{2.25}$$

donde es claro que $\Phi_{ab} = T_W\left[|\phi_a\rangle\langle\phi_b|\right]$, entonces el elemento matricial

$$A_{ab} = \frac{1}{N}\sum_{\mu=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{n=-\frac{N}{2}}^{\frac{N}{2}-1} A_W(p_\mu, q_m)\Phi^*_{ab}(p_\mu, q_m), \tag{2.26}$$

es la proyección de la función de espacio de fase A_W sobre la función base Φ_{ab}. Reemplazando en la ecuación (2.24) se obtiene

$$G_W(p_{\mu'}, q_{m'}, t'; p_\mu, q_m, t) = \frac{1}{N}\sum_{a=-\frac{N}{2}}^{\frac{N}{2}-1}\sum_{b=-\frac{N}{2}}^{\frac{N}{2}-1} \exp\left[-\frac{\mathrm{i}}{h}(E_a - E_b)(t'-t)\right] \Phi^*_{ab}(p_\mu, q_m)\Phi_{ab}(p_{\mu'}, q_{m'}), \tag{2.27}$$

que corresponde a la expresión para el propagador de la función de Wigner. Ya que la encriptación en el caso cuántico se realiza a través de operaciones unitarias, en el espacio de fase la encriptación se realiza en términos del propagador de la función de Wigner.

Propiedades del propagador de la función de Wigner

El análisis desarollado en el texto lleva de una manera muy clara a la forma de construir el propagador discreto de la función de Wigner. Sin embargo, de la misma manera que la funcion de Wigner cumple ciertas propiedades heredadas de la version continua, el propagador debe cumplir ciertas propiedades como lo hace su contraparte continua.

- Propagador de la función de Wigner para $t' = t$.

Denotando $(\mu, m) := \mathbf{r}$, el propagador de la función de Wigner para $(t' = t)$ es

$$\begin{aligned} G_{\mathrm{w}}(\mathbf{r}', t; \mathbf{r}, t) =& \frac{1}{N} \sum_{ab} \Phi^*_{ab}(\mathbf{r}) \Phi_{ab}(\mathbf{r}') \\ =& \frac{1}{N} \sum_{ab} \sum_{n'l'} \sum_{nl}^{2N} \delta_n^{n'} \delta_l^{l'} \left\langle \frac{n+n'}{2} | a \right\rangle \left\langle a | \frac{l-l'}{2} \right\rangle \left\langle \frac{l+l'}{2} | b \right\rangle \left\langle b | \frac{n-n'}{2} \right\rangle \\ \times& \tilde{\delta}(2m' - n) \tilde{\delta}(2m - l) \exp\left[-2\mathrm{i}\pi \frac{n'\mu'}{N}\right] \exp\left[-2\mathrm{i}\pi \frac{l'\mu}{N}\right] \\ =& \frac{1}{N} \sum_{n'} \sum_{n}^{2N} \delta_{n'}^{n} \tilde{\delta}(2m' - n) \tilde{\delta}(2m - n) \exp\left[-2\mathrm{i}\pi \frac{n'}{N}(\mu' - \mu)\right], \end{aligned} \tag{2.28}$$

Donde se ha hecho uso que $\hat{I} = \sum_a |a\rangle\langle a|$ y que $\langle k|k\rangle = \delta(k - k')$ analizando los casos n' par e impar. Se calcula la suma sobre n, teniendo ahora que

$$\begin{aligned} G_{\mathrm{W}}(\mathbf{r}', t; \mathbf{r}, t) =& \frac{1}{N} \delta(m' - m) \sum_{n'} \exp\left[-2\mathrm{i}\pi \frac{n'}{N}(\mu' - \mu)\right] \\ =& \delta(m' - m) \delta(\mu' - \mu) \end{aligned} \tag{2.29}$$

- Propiedades de grupo del propagador.

  Por simplicidad se implementará la siguiente notación

$$\begin{aligned} \mathbf{r} =& (p_\mu, q_m), \\ \rho' =& \rho_{\mathrm{w}}(p'_\mu, q'_m, t'). \end{aligned} \tag{2.30}$$

  La evolución de una distribución en el espacio de fase se hace por medio del propagador de manera que

$$\rho' = \sum_r G_{\mathrm{W}}(\mathbf{r}', t'; \mathbf{r}, t) \rho. \tag{2.31}$$

  Aplicando una segunda propagación se tendría que

$$\begin{aligned} \rho'' =& \sum_{r'} G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}', t') \rho' \\ =& \sum_{r'} G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}', t') \sum_r G_{\mathrm{W}}(\mathbf{r}', t'; \mathbf{r}, t) \rho \\ =& \sum_r G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}, t). \end{aligned} \tag{2.32}$$

  Por tanto, un propagador se puede escribir como el producto de dos propagadores mediante

$$G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}, t) = G_{\mathrm{W}}(\mathbf{r}'', t''; \mathbf{r}', t') G_{\mathrm{W}}(\mathbf{r}', t'; \mathbf{r}, t). \tag{2.33}$$

2.3 Versión cuántica de la aplicación del panadero

La versión cuántica de esta aplicación permite el estudio de la relación entre la mecánica clásica y la mecánica cuántica en el límite semiclásico para sistemas caóticos [29]. Existen diferentes formas de cuantizar la aplicación. Sin embargo, la aplicación cuántica obtenida debe ser unitaria, conservar las simetrías y establecer las condiciones de contorno adecuadas [26]. La cuantización más conocida es la realizada por Balazs, Voros y Saraceno [7, 27]. A continuación, se describe en términos generales la formulación cuántica de la aplicación. En esta versión es importante especificar el espacio de Hilbert de

los estados cuánticos. Por tanto, se realiza una precuantización en la que se establecen las condiciones de contorno cuasi-periódicas en la posición y en el momento de manera tal que el espacio de fase se convierte en un toro, análogo al cuadrado unitario de la versión clásica.

Cuando se usa la aplicación sobre una función de onda ψ se obtiene

$$\psi(q+1) = e^{2\pi \mathrm{i}\chi_q}\psi(q), \tag{2.34}$$

$$\tilde{\psi}(p+1) = e^{-2\pi \mathrm{i}\chi_p}\tilde{\psi}(p), \tag{2.35}$$

donde $\psi(q)$ y $\tilde{\psi}(p)$ representan la función de onda en la representación de la posición y del momento, respectivamente. Las soluciones de (2.34) y (2.35) existen sólo si $2\pi N\hbar = 1$. Entonces, los autovectores de posición y momento son

$$|q_n\rangle = \left|\frac{n+\chi_p}{N}\right\rangle, n = 1, 2, ..., N-1, \tag{2.36}$$

$$|p_m\rangle = \left|\frac{m+\chi_q}{N}\right\rangle, m = 1, 2, ..., N-1, \tag{2.37}$$

donde N corresponde a la dimensión del espacio de Hilbert, y $|q_n\rangle$ y $|p_m\rangle$ son discretos.

El núcleo de la transformación corresponde al núcleo de la transformación de Fourier discreta

$$\langle p_m|q_n\rangle = \frac{1}{\sqrt{N}}e^{-2i\pi(n+\chi_p)(m+\chi_q)/N} = (F_N^{\chi_q,\chi_p})_{m,n}, \tag{2.38}$$

en donde los parámetros χ_q, χ_p caracterizan la cuantización. El procedimiento para cuantizar la aplicación consiste en discretizar la función generadora de la representación mixta. Posterior a esto, se deben establecer en ceros los elementos matriciales prohíbidos y, finalmente, aplicar la transformación de Fourier inversa a la representación de coordenadas. La versión cuántica de la aplicación del panadero que se obtiene es [27]

$$\hat{B} = \left[F_N^{\chi_q,\chi_p}\right]^{-1}\begin{bmatrix} F_{N/2}^{\chi_q,\chi_p} & 0 \\ 0 & F_{N/2}^{\chi_q,\chi_p}\end{bmatrix}. \tag{2.39}$$

Esta aplicación cuántica tiene el comportamiento de la aplicación del panadero clásica cuando $\hbar \to 0$ [14, 27]. En la ecuación (2.39), $\hat{B}$ corresponde a un operador unitario que actúa sobre el espacio de Hilbert de dimensión N.

La versión cuántica de la aplicación del panadero en la que la noción de tiempo es continua, se construye mediante la transformación de Fourier de orden fraccionario [12] que se discute en la siguiente sección. Con esta versión es posible realizar un número irracional de "iteraciones", obteniendo así mayor poder de encriptación.

Para obtener la aplicación del panadero de tiempo continuo, en esta tesis se propone reemplazar las transformaciones de Fourier discretas de la ecuación (2.39) por transfomaciones de Fourier *discreta* de orden fraccionario,

$$\hat{B}_\alpha = \left[F_N^{\chi_q,\chi_p}\right]^{-\alpha}\begin{bmatrix} F_{N/2}^{\chi_q,\chi_p\,\alpha} & 0 \\ 0 & F_{N/2}^{\chi_q,\chi_p\,\alpha}\end{bmatrix}, \tag{2.40}$$

donde F_N^a corresponden a la transformación de Fourier finita de orden fraccionario [12].

2.3.1. Transformación de Fourier finita de orden fraccionario

Para encriptar imágenes en este trabajo se utiliza la versión cuántica de tiempo continuo de la aplicación del panadero. En esta versión, se realizan transformaciones de Fourier fraccionarias [21].

La transformación de Fourier fraccionaria continua (FrFT) sobre una función $f(x)$, acotada en el espacio L^2, es definida en [12] como

$$\mathcal{F}^{\alpha}\left[f\right]\left(t_{\alpha}\right)=\int_{-\infty}^{\infty}\mathrm{d}tK_{\alpha}(t_{\alpha},t)f(t), \tag{2.41}$$

donde $K_{\alpha}(t_{\alpha},t)$ corresponde al núcleo de la FrFT, el cual está definido por

$$K_{\alpha}(t_{\alpha},t)=K_{\phi}e^{\mathrm{i}\pi(t_{\alpha}^{2}\cot\phi-2t_{\alpha}t\csc\phi+t^{2}\cot\phi)}, \tag{2.42}$$

con $K_{\phi}=e^{[-\mathrm{i}(\pi\mathrm{sng}(\phi)/4-\phi/2)]}/\left|\sin(\phi)\right|^{1/2}$ y $\phi=\frac{\alpha\pi}{2}$, donde $\alpha\in\mathbb{R}$, $0\leq|\alpha|\leq 2$.

A diferencia de la transformación de Fourier ordinaria que corresponde a rotaciones de 90 grados, la transformación fraccionaria corresponde a rotaciones continuas en el espacio de fase, y es por esta razón que es necesaria en la construcción de la versión de tiempo continuo de la aplicación del panadero(ver Apéndice A). Como se mencionó antes, la aplicación del panadero actúa sobre el espacio de fase discreto, de modo que la FrFT utilizada debe ser *discreta* [12].

Dado el carácter finito del espacio de Hilbert de las compuertas cuánticas utilizadas para implementar la aplicación del panadero, es necesario considerar este hecho en la formulación del espacio de fase donde actua la aplicación. Por esta razón, es necesario hacer uso de la transformación de Fourier fraccionaria discreta (DFrFT) [21]. Esta transformación discreta debe cumplir ciertas condiciones [12]: *i*) ser unitaria y de índices aditivos, propiedades de la transformación continua, *ii*) ser una generalizacón consistente de la Transformación de Fourier Discreta (DTF) ordinaria, es decir, la DFrTF debe reducirse a DTF cuando su orden es igual a la unidad y, *iii*) es necesario que sea una aproximación de la transformación fraccionaria de Fourier continua. La transformación fraccionaria de Fourier discreta se describe en detalle en el capítulo 6 de la Ref [19], y se define como

$$\mathcal{F}_{N}^{\alpha}[m,n]=\sum_{k=0,k=(N-1+(N)_{2})}^{N}u_{k}[m]e^{-\mathrm{i}\frac{\pi}{2}k\alpha}u_{k}[n], \tag{2.43}$$

donde u_k es un conjunto de autovectores único y ortogonal que corresponde a la $k-$ésima función discreta de Hermite-Gauss.

2.3.2. Aplicación del panadero de tiempo continuo en el espacio de fase

Como se discutió en la sección 2.2.2, la definición de la función de Wigner puede adaptarse al espacio de Hilbert discreto con el fin de eliminar la información redundante y ser utilizada en el estudio cuántico de sistemas clásicamente caóticos.

En la figura 2.2 se presenta la acción de la aplicación del panadero para el caso cuántico sobre la distribución dada por la expresión

$$\widetilde{\psi}(p_{\lambda})=\frac{1}{N}\sum_{l=-\infty}^{\infty}\exp\left[-2\pi^{2}\sqrt{60}\frac{l^{2}}{N^{2}}+2\mathrm{i}\pi\frac{\lambda l}{N}\right], \tag{2.44}$$

que define una función gaussiana de periodo N. Se utiliza la ecuación (2.19) para calcular la evolución temporal de la función.

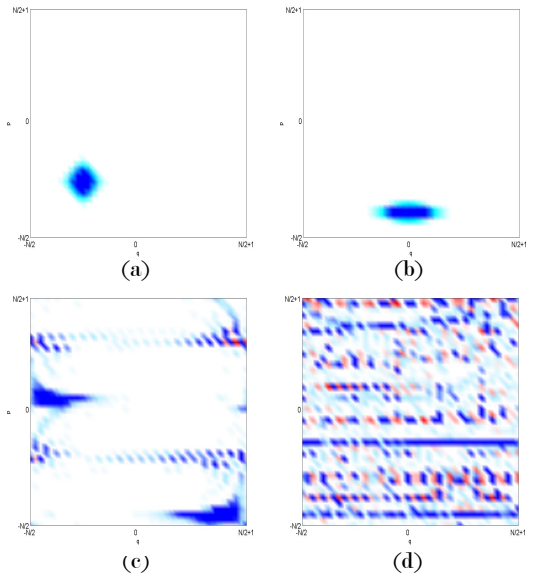


Figura 2.2: Acción de la aplicación del panadero sobre una distribución inicial. El conjunto de imágenes corresponde a la aplicación de *tiempo continuo* para $\alpha = 1$. (a) Distribución inicial, (b) $t = 1$, (c) $t = 2$, y (d) $t = 5$.

Las gráficas de la figura 2.2 presentan la acción de la aplicación del panadero de *tiempo continuo* sobre una distribución inicial en el espacio de fase.

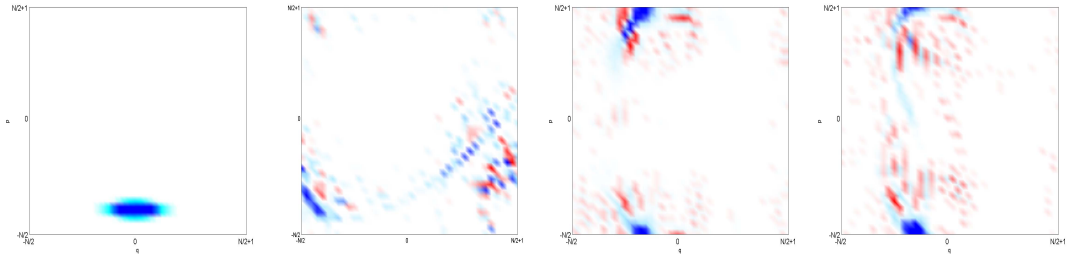


Figura 2.3: Acción de la aplicación del panadero sobre una distribución inicial realizando composición. El estado inicial coincide con la figura 2.2a. a) Distribución cuasiprobabilidad para $\alpha = 1$ y $t = 1$, b) Distribución de cuasiprobabilidad para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2$ y $t = 1$, c) Distribución cuasiprobabilidad para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}3$ y $t = 1$ y d) Distribución cuasiprobabilidad para la secuencia $\alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3$ y $t = 1$.

En las gráficas de la figura 2.3 se compara la acción de la aplicación del panadero de *tiempo continuo* sobre la distribución gaussiana de la expresin (2.44) para $\alpha = 1$ con la acción de la aplicación al realizar diferentes secuencias de α, se observa que en el caso de la composición de α, la distribución en 2.3b), 2.3c) y 2.3d) es diferente a la obtenida para $\alpha = 1$. Se observa que en el caso de la versión cuántica de *tiempo continuo* la distribución toma valores negativos (zonas rojas), estos valores se deben al carácter no local de la dinámica cuántica. En el caso clásico no es posible que los valores positivos se conviertan

en negativos [22], de modo que al incluir este fenómeno de no-localidad, en principio, se mejora el proceso de encriptación.

Del análisis de estos resultados se encuentra que aunque el operador FrFT forma un semigrupo parametrizado por el ángulo α, en la versión de la aplicación del panadero diseñada en este trabajo, no es posible realizar composición del ángulo α, es decir, para el caso de tiempo continuo el operador FrFT no forma un semigrupo en α. En el siguiente capítulo se discute como tomar ventaja de este hecho para incrementar el nivel de encriptación.

2.4 Análisis de variedades clásicas

Un sistema caótico se caracteriza por un conjunto de puntos pertenecientes a órbitas periódicas. Una órbita periódica es aquella que no cambia cuando se realizan iteraciones de la aplicación caótica. Las funciones de Wigner de los estados propios de una aplicación caótica presentan *cicatrices* de este comportamiento clásico [16]. En el caso de la aplicación del panadero, los puntos periódicos se calculan fácilmente a partir de las ecuaciones de transformación (2.1).

Existe una manera de encontrar estos rasgos clásicos en la dinámica cuántica utilizando la expresión (2.27). El propagador de la función de Wigner en un punto final (p_μ, q_m) para una condición inicial (p_μ, q_m) determinada, establece la densidad de probabilidad de regresar al mismo punto (p_μ, q_m), los puntos que tienen mayor probabilidad de regresar corresponden a puntos periódicos.

Las órbitas periódicas clásicas coinciden con los máximos de las funciones de Wigner asociadas a los estados propios de la versión cuántica de tiempo discreto de la aplicación del panadero [5, 23].

La figura 2.4 muestra la comparación de órbitas periódicas clásicas y el propagador diagonal $G_W(p_\mu, q_m; p_\mu, q_m)$ de la función de Wigner de los estados propios de la aplicación del panadero de *tiempo continuo*.

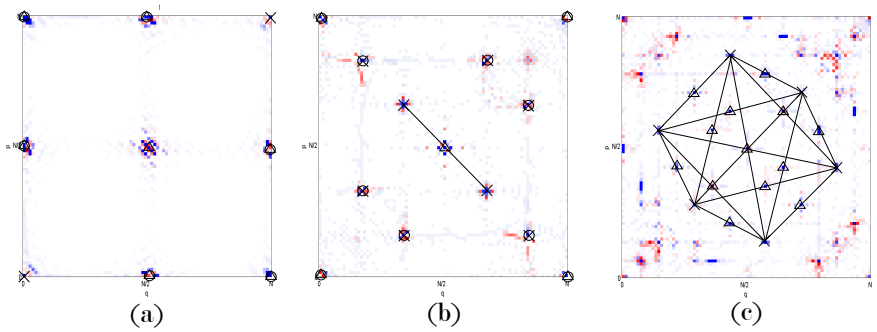


Figura 2.4: Propagador diagonal de Wigner de la aplicación del panadero de *tiempo continuo* para $\alpha = 1$. Cada gráfica corresponde a una iteración de la aplicación (a) $t = 1$, (b) $t = 2$ y, (c) $t = 3$. Los símbolos $\times$ y $\triangle$ corresponden a los puntos periódicos de la aplicación y sus puntos medios respectivamente. Espacio de Hilbert de dimensión $N = 84$.

Es posible observar que al utilizar la versión de *tiempo continuo* de la aplicación para el caso en el que $\alpha = 1$ se obtienen los resultados esperados, es decir, las órbitas periódicas coinciden con las que se obtendrían al utilizar la aplicación del panadero de tiempo discreto. Con esto se comprueba que la

aplicación del panadero de *tiempo continuo* cuando el ángulo $\alpha = 1$ corresponde a la versión de tiempo discreto de la aplicación, entonces se puede concluir que en el algoritmo utilizado, la transformación de Fourier fraccionaria se reduce a la transformación de Fourier discreta cuando $\alpha = 1$.

En la aplicación de *tiempo continuo* propuesta en este trabajo es posible realizar rotaciones de ángulo α arbitrario debido al uso de la transformación de Fourier discreta de orden fraccionario. Por tanto, es posible observar y estudiar la evolución de un punto en *tiempo continuo* como se muestra en la siguiente figura.

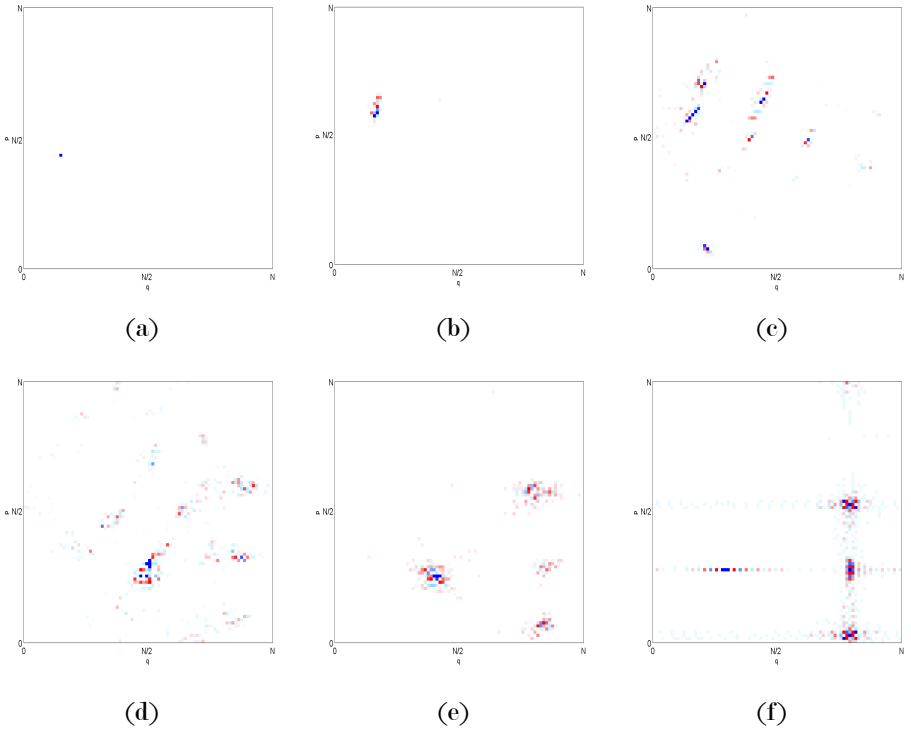


Figura 2.5: Propagador diagonal de Wigner para una condición inicial determinada. (a) Condición inicial (37,13), (b) $\alpha = 0{,}2$ y, (c) $\alpha = 0{,}4$, d) $\alpha = 0{,}6$, (e) $\alpha = 0{,}8$, y (f) $\alpha = 1$. Espacio de Hilbert de dimensión $N = 84$ y $t = 1$. Propagador de Wigner.

En la figura 2.5 se presenta la evolución temporal del punto (37,13) del espacio de fase, cambiando el ángulo α en pasos de 0,2, dado que $\alpha \in \mathbb{R}$ (ver sección 2.3.1), el punto en el espacio de fase puede ser seguido en pasos tan pequeos como se desee. Esto permite profundizar en el estudio del comportamiento cuántico de los sistemas clásicamente caóticos.

CAPÍTULO 3

Encriptación de imágenes a través de la aplicación del panadero

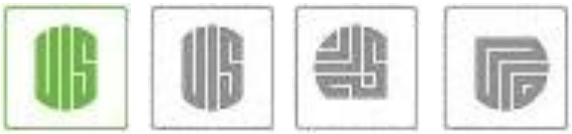
En este capítulo se presenta una descripción del proceso de encriptación de imágenes a través de la aplicación del panadero y se verifica la calidad de este proceso utilizando dos métodos estándar de certificación de encriptación.

3.1 Encriptación de imágenes

Los componentes más pequeños de una imágen digital se llaman pixeles, una imagen digital puede ser representada de manera bidimensional como una matriz, cada elemento de la matriz corresponde a un pixel de la imagen, una imagen RGB (Red, Green, Blue) requiere una matriz tridimensional, donde se representen las intensidades de rojo, verde y azul, el color de cada pixel está dado por la combinación de las tres intensidades, a diferencia de una imagen de intensidad, por ejemplo, en escala de grises, que requiere una sola matriz. Esto permite que trabajar con imágenes sea similar a trabajar con cualquier tipo de matriz.

Aquí no se utilizan las imágenes estándar encontradas en la literatura, porque la principal motivación para el desarrollo de este trabajo es implementar experimentalmente la aplicación del pandero de *tiempo continuo* para estudiar la dinámica de los sistemas caóticos en *tiempo continuo*. De modo que las imágenes deben estar codificadas en un estado físico. A continuación se describe el tratamiento que se le da a la imagen para satisfacer esta condición.

En este trabajo se utilizan imágenes en escala de grises, la siguiente figura muestra la imagen de prueba elegida.



(a) (b) (c) (d)

Figura 3.1: Imagen de prueba. (a) Imagen RGB, (b) escala de grises, (c)parte superior reflejada y (d) parte inferior reflejada . Imagen de 42×42 pixeles

Antes de comenzar con el proceso de encriptación, la imágen de prueba se convierte a una imagen de intensidad, en este caso, una imagen en escala de grises. La matriz de la imagen A contiene toda la información de ésta, de igual manera en que la matriz densidad $\hat{\rho}$ contiene toda la información de un sistema cuántico, como se estableció en la sección 2.2. El operador $\hat{\rho}$ debe ser hermítico, es decir, $\hat{\rho} = \hat{\rho}\dagger$, por esta razón se debe construir una imagen simétrica, entonces la traza de la matriz de la imagen debe ser igual a la unidad $[\mathrm{tr}(\mathsf{A}) = 1]$. Para lograr que la suma de los elementos de la diagonal de la matriz asociada a la imagen sea 1 se toma la matriz triangular superior de A y se refleja, esto también se hace para la matriz triangular inferior, como se puede ver en *c*) y *d*) de la figura 3.1.

De modo que ahora se tienen dos imágenes (dos matrices), al aplicar el proceso de encriptación se obtienen dos imágenes encriptadas, que finalmente se combinan en una sola. Es importante mencionar que la condición de simetría mencionada anteriormente es la única que deben cumplir las imágenes que se desean encriptar, y que el tratamiento inicial que se le aplica a A puede ser reproducido en cualquier imagen. Para el proceso de encriptación se utiliza la aplicación del panadero de *tiempo continuo* para calcular las funciones Φ_{ab} y Φ^*_{ab} de la ecuación (2.27), de modo que se obtiene el propagador, y mediante la ecuación (2.19) se obtiene la evolución temporal de la imagen A.

A continuación se presentan las imágenes encriptadas.

(a) (b) (c) (d)

Figura 3.2: Imágenes encriptadas a través de la aplicación de *tiempo continuo*. (a) Imagen de prueba, (b) imagen encriptada para $t = 10^2$, c) imagen encriptada para $t = 10^3$ y (d) imagen encriptada para $t = 10^4$. Imagen de 42×42 pixeles. Ángulo $\alpha = 0{,}5$.

Para el proceso de desencriptación se calcula el transpuesto complejo conjugado de la expresión para la aplicación del panadero de *tiempo continuo* (2.40), con el cual se calculan las funciones Φ_{ab} y Φ^*_{ab} de la ecuación (2.27). De modo que se obtiene el propagador inverso, que se utiliza de igual forma que en el proceso de encriptación.

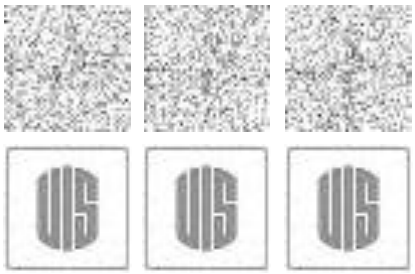


Figura 3.3: Imagen desencriptada a través de la aplicación de *tiempo continuo*. (a) Imágenes encriptada y desencriptada para $t = 50$, (b) imágenes encriptada y desencriptada para $t = 5\times^2$ y (c) imágenes encriptada y desencriptada para $t = 5\times^3$. Imagen de 42×42 pixeles. Ángulo $\alpha = 1$.

Como se mencionó en el capítulo anterior, en el caso de *tiempo continuo* no es posible realizar composición en α, en las siguientes figuras se ve claramente este hecho.

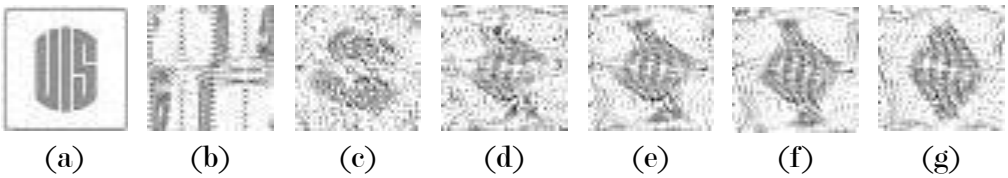


Figura 3.4: Imágenes encriptadas realizando composición. (a) Imagen de prueba, (b) imagen encriptada para $\alpha = 1$, (c) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2$, (d) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}3$, (e) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3$, (f) imagen encriptada para la secuencia $\alpha = 0{,}1, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}1$, y (g) imagen encriptada para la secuencia $\alpha = 0{,}3, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}1, \alpha = 0{,}1$. Para $t = 1$. Imagen de 42×42 pixeles.

Es de esperar que al realizar la aplicación cinco veces para $\alpha = 0{,}2$ se obtenga el mismo resultado que realizar la aplicación una vez para $\alpha = 1$. Sin embargo, como se puede observar en la figura 3.4, las imágenes encriptadas utilizando estas condiciones y otras secuencias como en 3.4d) y 3.4e) son diferentes. En la siguiente figura se muestra nuevamente que no es posible realizar composición en α

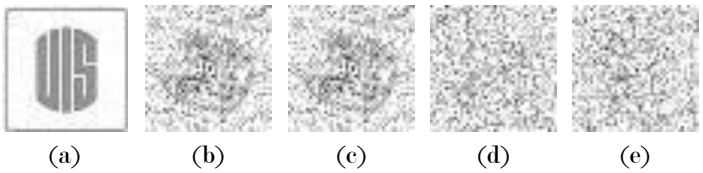


Figura 3.5: Imágenes encriptadas realizando composición en t y en α. (a) Imagen de prueba, (b) imagen encriptada para $\alpha = 0{,}2$ y $t = 10^2$, (c) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2$ y $t = 20$ (composición en t), (d) imagen encriptada para la secuencia $\alpha = 0{,}1, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}1$ y $t = 20$ (composición en α), y (e) imagen encriptada para la secuencia $\alpha = 0{,}3, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}1, \alpha = 0{,}1$ y $t = 20$ (composición en α). Imagen de 42×42 pixeles.

En la figura 3.5 se observa que las imágenes b) y c) en las que se utiliza el mismo valor de α y diferente t son iguales, es decir, realizar 10^2 iteraciones para $\alpha = 0{,}2$ corresponde a realizar 5 veces, 20 iteraciones para $\alpha = 0{,}2$. Sin embargo, cuando se realizan 20 iteraciones de diferentes α como en d), la imagen obtenida no es igual, por tanto, es claro que para el caso de *tiempo continuo* de la aplicacioón del panadero, no es posible realizar composición en α.

Se establece entonces que, el nivel de encriptación de las imágenes utilizando la versión de *tiempo continuo* de la aplicación es mayor, dado que no es posible realizar composición en el ángulo α, este hecho hace necesario establecer los valores de α y el orden en que se utilizaron en el proceso de encriptación para obtener la imagen original. Es importante recalcar que $\alpha \in \mathbb{R}$ y que en la encriptación por bloques es posible dividir la imagen en grupos de pixeles (bloques), y aplicar diferentes secuencias de α a cada bloque. Este hecho hará aún más segura la encriptación.

Con el fin de certificar la calidad del proceso de encriptación presentado en este trabajo se utilizan dos métodos estándar, el análisis del histograma de las imágenes y el cálculo del valor de la calidad de encriptación.

3.1.1. Análisis de histograma

Una gráfica de histograma muestra la distribución de los pixeles en una imagen, en el caso de una imagen en escala de grises, el histograma indica el número de pixeles en cada nivel de gris. El término nivel de gris, en general, hace referencia a la intensidad de un pixel en particular en una imagen, en una imagen en escala de grises cada pixel se encuentra en un rango de $(0 - 255)$ de nivel de gris.

El histograma de una imagen encriptada debe ser uniforme, de modo que no revele información que permita realizar ataques estadísticos a las imágenes.

A continuación se presentan los histogramas correspondientes a la imágen original y a las imágenes encriptadas a través de la aplicación del panadero de *tiempo continuo*, y a través de la versión de tiempo discreto.

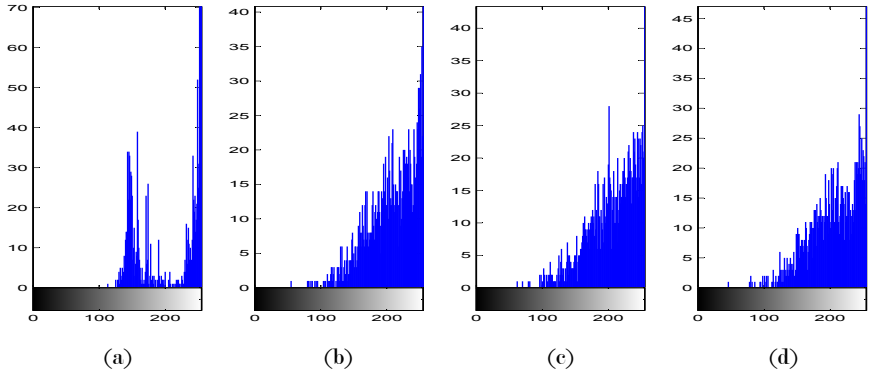


Figura 3.6: Histograma de imágenes encriptadas a través de la aplicación de *tiempo continuo*. (a) Imagen de prueba, (b) imagen encriptada para $t = 10^2$, (c) imagen encriptada para $t = 10^3$ y (d) imagen encriptada para $t = 10^4$. Imagen de 42×42 pixeles. Ángulo $\alpha = 0{,}5$.

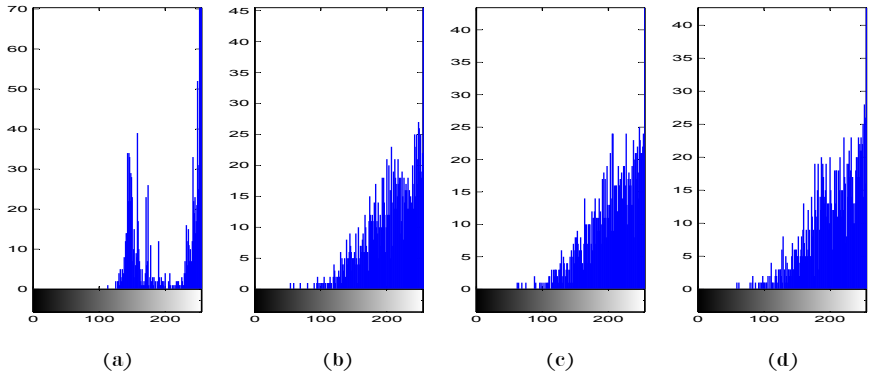


Figura 3.7: Histograma de imágenes encriptadas a través de la aplicación de *tiempo continuo*. (a) Imagen de prueba, (b) imagen encriptada para $t = 50$, (c) imagen encriptada para $t = 5 \times 10^2$ (d) imagen encriptada para $t = 5 \times 10^3$. Imagen de 42×42 pixeles. Ángulo $\alpha = 1$.

Es necesario aclarar que en las figuras 3.6 y 3.7 los histogramas correspondientes a las imágenes encriptadas a través de la aplicación del panadero de *tiempo continuo* no tienen una distribución uniforme debido a que la mayoría de los pixeles de la imagen de prueba están ubicados en niveles de gris más claros, como se puede ver en el histograma 3.6a) de la imagen de prueba.

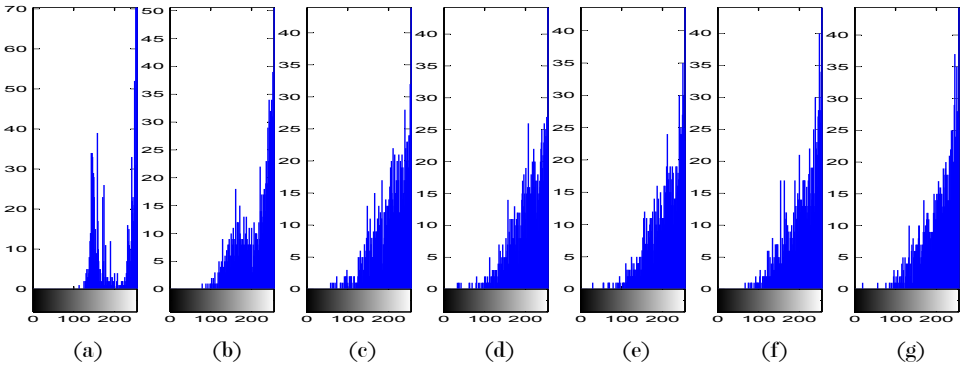


Figura 3.8: Histograma de imágenes encriptadas encriptadas realizando composición. (a) Imagen de prueba, (b) imagen encriptada para $\alpha = 1$, (c) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2$, (d) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}3$, (e) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3$, (f) imagen encriptada para la secuencia $\alpha = 0{,}1, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}1$, y (g) imagen encriptada para la secuencia $\alpha = 0{,}3, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}1, \alpha = 0{,}1$. Para $t = 1$ Imagen de 42×42 pixeles.

En la figura 3.8 es posible observar para el caso de *tiempo continuo* las imágenes encriptadas tienden a llenar más rápido los demás niveles, es decir, que las imágenes encriptadas con la aplicación de *tiempo continuo* son más homogéneas que las imágenes encriptadas con la aplicación de tiempo discreto, haciendo más difícil obtener información estadística de la imagen original, al no poder realizar composición del ángulo α.

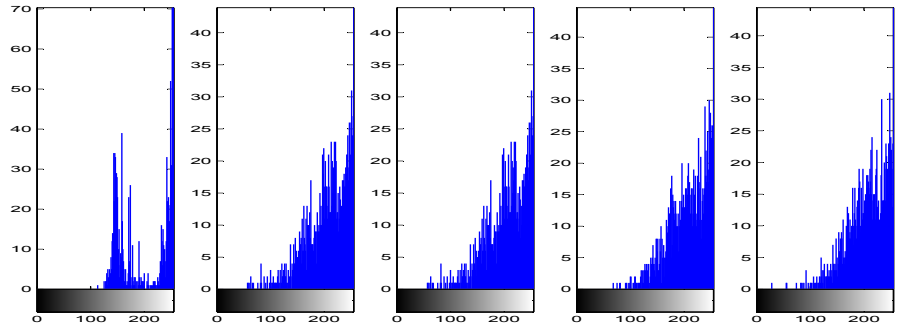


Figura 3.9: Histograma de imágenes encriptadas encriptadas realizando composición en t y en α. (a) Imagen de prueba, (b) imagen encriptada para $\alpha = 0{,}2$ y $t = 10^2$, (c) imagen encriptada para la secuencia $\alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2, \alpha = 0{,}2$ y $t = 20$, y (d) imagen encriptada para la secuencia $\alpha = 0{,}1, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}3, \alpha = 0{,}1$ y $t = 20$, y (e) imagen encriptada para la secuencia $\alpha = 0{,}3, \alpha = 0{,}3, \alpha = 0{,}2, \alpha = 0{,}1, \alpha = 0{,}1$ y $t = 20$ (composición en α). Imagen de 42×42 pixeles.

En las figuras 3.8 y 3.9, los histogramas correspondientes a las imágenes encriptadas utilizando diferentes secuencias de α, reiteran que en el caso de la aplicación de tiempo continuo la transformación de Fourier fraccionaria no forma un semigrupo en α.

La llave de la encriptación en este caso corresponde a las secuencias de α utilizadas en el proceso de encriptación. Esta llave puede encriptarse usando otros métodos y transferirse. Este hecho hace atractiva la propuesta presentada en este trabajo de grado.

3.1.2. Medida de la calidad de encriptación

Cuando se lleva a cabo un proceso de encriptación sobre una imagen, en la imagen encriptada se produce un cambio en el valor de los pixeles comparado con el valor de los pixeles de la imagen original, cuanto mayor sea el cambio, mayor será la eficacia del proceso y de la calidad de la encriptación. La calidad de encriptación es una medida que utiliza los datos del histograma de una imagen encriptada y su imagen original para establecer la calidad de la encriptación.

Siendo OI la imagen plana (imagen original) de dimensiones $M \times N$ pixeles con K niveles de gris y EI la imagen encriptada con las mismas características. Entonces $OI(x, y)$, $OE(x, y)\epsilon 0, ..., K - 1$ corresponden a los niveles de gris de las imágenes OI y EI en la posición (x, y) donde $(0 \leq x \leq M - 1, 0 \leq y \leq N - 1)$. Se define $H_K(OI)$ como número de veces que ocurre cada nivel de gris en la imagen original OI, y $H_K(EI)$ como número de veces que ocurre cada nivel de gris en la imagen encriptada EI, entonces

$$EQ = \frac{\sum_K^{255} |H_K(EI) - H_K(OI)|}{256}, \tag{3.1}$$

se conoce como calidad de encriptación, que representa el número promedio de cambios de cada nivel de gris.

En las siguientes tablas se indica el valor de la calidad de encriptación para las imágenes presentadas

en la sección 3.1.

Tabla 3.1: Medida de la calidad de encriptación.

Imagen	α	t	Calidad de encriptación
Figura 3.6b	0.5	10^2	6.8516
Figura 3.6c	0.5	10^3	7.0469
Figura 3.6d	0.5	10^4	6.7031
Figura 3.7b	1	50	6.5938
Figura 3.7c	1	5×10^2	6.9375
Figura 3.7d	1	5×10^3	6.9375

Los valores de la tabla 3.1 muestran que la calidad de la encriptación es similar para las imágenes para diferente t y con α fijo. Al realizar un gran número de iteraciones para $\alpha = 1$ (figuras 3.7c y 3.7d) el valor de la calidad de encriptación es el mismo, este resultado puede estar asociado a la saturación de estructuras, en los sistemas caóticos se generan estructuras en el espacio de fase [35], pero esta generación de estructuras se satura luego de un determinado tiempo t y ya no se generan más, en este caso cuando la aplicación del pandero no genera más estructuras el valor de la calidad de encriptacińn no cambia.

Tabla 3.2: Medida de la calidad de encriptación para la composición de α.

Imagen	α	t	Calidad de encriptación
Figura 3.8b	1	1	5.6484
Figura 3.8c	0.2, 0.2, 0.2, 0.2, 0.2	1	6.6172
Figura 3.8d	0.2, 0.2, 0.3, 0.3	1	6.8516
Figura 3.8e	0.2, 0.3, 0.2, 0.3	1	6.7266
Figura 3.8f	0.1, 0.3, 0.2, 0.3, 0.1	1	6.5859
Figura 3.8g	0.3, 0.3, 0.2, 0.1, 0.1	1	6.5703
Figura 3.9b	0.2	10^2	6.8750
Figura 3.9c	0.2, 0.2, 0.2, 0.2, 0.2	20	6.8750
Figura 3.9d	0.1, 0.3, 0.2, 0.3, 0.1	20	6.8828
Figura 3.9e	0.3, 0.3, 0.2, 0.1, 0.1	20	6.8984

En el caso de las imágenes encriptadas realizando diferentes secuencias para la composición de ángulo α (figuras 3.8b, 3.8c, 3.8d, 3.8e, y 3.8f) el valor de la calidad de encriptación es mayor que la de la imagen encriptada con la aplicación de *tiempo continuo* para $\alpha = 1$ (figura 3.8a).

En la tabla 3.2 se puede obsevar que el valor de la calidad de encritación para el caso en que se realiza composición de tiempo (figura 3.9c) es igual al valor para la figura 3.9b, ya que realizar 5 veces 20 iteraciones para $\alpha = 0{,}2$ equivale a realizar 10^2 iteraciones para $\alpha = 0{,}2$. Sin embargo, cuando se realiza composición del parámetro α, como en el caso de las figuras 3.9d y 3.9e la calidad de la encriptación es mayor.

Los resultados mostrados aquí comprueban que al utilizar la aplicación del panadero de *tiempo continuo* propuesta en este trabajo para encriptar imágenes se obtiene un mayor nivel y control de encriptación

que al utilizar la versión de tiempo discreto de la aplicación. Se espera que con el uso de imágenes de prueba más complejas y con mayor estructura las ventajas de la encriptacón con la versión continua se hagan más claras.

CAPÍTULO 4

Implementación física de la versión cuántica de tiempo continuo

En este capítulo se propone una implementación de la aplicación del panadero de *tiempo continuo* en un computador cuántico de RMN utilizando compuertas cuánticas para realizar las rotaciones de la transformación de Fourier de orden fraccionario.

4.1 Compuertas cuánticas

El progreso de la ciencia y los avances tecnológicos han permitido idear la creación de computadores cuánticos con los que se obtendrían mejores capacidades de cómputo y nuevas formas de procesamiento y de transmisión de información.

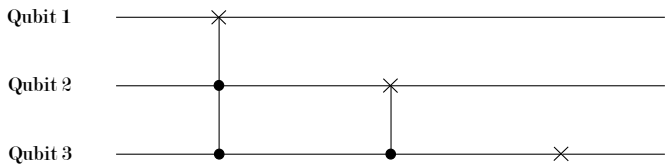
En los computadores cuánticos la información se procesa a través de la manipulación controlada de qubits (bits cuánticos) y se utilizan las compuertas lógicas para el diseño y la construcción de hardware. Una compuerta lógica cuántica es una función que realiza un operador unitario en un conjunto de qubits seleccionados durante un determinado tiempo [32]. Las compuertas cuánticas son reversibles, es decir, es posible calcular la entrada de una compuerta si se conoce la salida ya que cada salida se relaciona con una única entrada. Esta característica es contraria al caso de las compuertas lógicas clásicas, por ejemplo, la compuerta AND tiene dos líneas de entrada y sólo una de salida. Los sistemas de cómputo irreversible operan con procesos de pérdida de energía, esto no ocurre cuando se utilizan compuertas cuánticas. Por tanto, ofrecen una alta velocidad de procesamiento y un mínimo de consumo de energía, es decir, son más eficientes.

Generalmente, las compuertas cuánticas son representadas como matrices y el número de qubits de la entrada es igual al de la salida. La función que realiza una compuerta está dada por la multiplicación de la matriz que representa la compuerta con el vector que representa el estado cuántico. Entre las compuertas cuánticas más usadas se encuentran: NOT, CNOT, SWAP, TOFFOLI y FREDKIN (ver apéndice A).

Estas compuertas cuánticas han sido utilizadas para estudiar el caos cúantico [6, 28]. En particular,

se demostró que el mapa del panadero cuántico puede ser investigado experimentalmente mediante una simulación eficiente en un computador cuántico de 3 qubits, es decir, que sería posible el estudio experimental del caos cuántico [28]. También se han propuesto y analizado dos experimentos de caos cuántico [9, 34]. En estos experimentos se utiliza un computador cuántico de resonancia magnética nuclear de 3 qubits que mide la sensibilidad de la aplicación cuántica del panadero con respecto a perturbaciones controladas. La versión cuántica de 3 qubits de la aplicación del panadero se representa en [34] se realizó con tres compuertas lógicas NOT CNOT y TOFOLLI.

Figura 4.1: Versión cuántica de la aplicación del panadero de tiempo discreto de tres qubits.



La figura 4.1 corresponde a la secuencia de compuertas cuánticas utilizadas para desarrollar el algoritmo de simulación de la aplicación cuántica del panadero. La primera es una compuerta TOFFOLI, la segunda compuerta es una CNOT y la tercera compuerta es una NOT, las cuales actúan sobre el primero, segundo y tercer qubit, respectivamente.

Las implementaciones experimentales de la aplicación cuántica del panadero, mencionadas arriba, permiten avanzar en el estudio de los sistemas cuyo comportamiento es caótico [11, 24]. En particular, ya que los sistemas físicos evolucionan en tiempo continuo y no en tiempo discreto, la construcción de la versión cuántica de *tiempo continuo* de la aplicación, permite avanzar en la comprensión de la dinámica de las compuertas y procesadores cuánticos, en un trabajo posterior.

Para escribir la aplicación del panadero de *tiempo continuo* en términos de compuertas cuánticas, es necesario escribir las rotaciones realizadas con la FrFT en términos de compuertas cuánticas, como se realiza para la transformación de Fourier ordinaria en la versión de tiempo discreto de la aplicación [9]. En la descripción del proceso de encriptación en la sección 3.1 se establece que la imagen utilizada debe cumplir con la condición de estar codificada en un estado físico. Esta condición toma importancia en la implementación experimental de la aplicación del panadero de *tiempo continuo* donde la imagen se codifica en el estado de los qubits, se propone enviar una secuencia de pulsos con técnicas de resonancia magnética nuclear (RMN) como en [9] donde para $\frac{\tau}{2}$ se realiza una rotación de ángulo π, en el caso particular de la versión de *tiempo continuo*, las rotaciones de la aplicación son se ángulo arbitrario α, por tanto las mediciones experimentales se realizarían cada $\frac{\tau\alpha}{2\pi}$, donde τ y α corresponden al periodo de los pulsos y al parámetro de la transformación fraccionaria de Fourier.

CAPÍTULO 5

Conclusiones

En este trabajo se expuso un nuevo proceso de encriptación de información, con el cual se extiende la aplicabilidad de la transformación de Fourier de orden fraccionario (FrFT) que recientemente se ha convertido en un elemento principal en el procesamiento de señales. Se generalizó la versión cuántica de la aplicación del panadero al caso de *tiempo continuo* mediante el uso de la FrFT con el fin de realizar rotaciones de ángulo arbitrario α, y con esta nueva versión de la aplicación se encriptaron imágenes.

A partir del cálculo del propagador de Wigner diagonal de la aplicación del panadero de *tiempo continuo* para el caso en que $\alpha = 1$, se comprobó que los máximos del propagador diagonal asociado a los estados propios de esta versión propuesta coinciden con las órbitas periódicas clásicas de la aplicación de tiempo discreto; debido al uso de la FrFT en la construcción de esta versión de la aplicación fue posible observar la evolución en *tiempo continuo* de una determinada condiciónn inicial del espacio de fase, este hecho es fundamental en el estudio de la dinámica cuántica de los sistemas que clásicamente presentan comportamiento caótico.

Finalmente, se realizó la encriptación cuántica de imágenes a través de la versión de *tiempo continuo* de la aplicación del panadero. Estas imágenes se evaluaron utilizando dos métodos estándar de certificación de encriptación: el análisis de histograma y el cálculo de la calidad de encriptación de cada imagen, es importante recalcar que el proceso de encriptación diseñado fue probado inicialmente sobre una distribución gaussiana y se encontró que en el caso de *tiempo continuo* la transformación de Fourier fraccionaria no forma un semigrupo en α pese a que el operador FrFT forma un semigrupo parametrizado por el ángulo α, este comportamiento permite que al realizar diferentes secuecias equivalentes de α se obtengan imágenes encriptadas diferentes, lo que no sólo aumenta el nivel de encriptación sino que también representa una ventaja en la seguridad de la encriptación de imágenes ya que hace más complejo intentar establecer los valores de α en un ataque de fuerza bruta, e intentar obtener información estadística del histograma de la imagen encriptada.

Con el análisis y la comparación de los resultados obtenidos se comprobó que para el caso de *tiempo continuo*, el nivel y el control de encriptación de las imágenes es mayor, indicando la utilidad de la versión de la aplicación desarrollada en este trabajo. Se espera que estos resultados no sólo influyan en el mejoramiento de la calidad de encriptación clásica cuando se construya la versión clásica de *tiempo continuo* de la aplicación en un trabajo posterior, si no que permitan ahondar en la comprensión del comportamiento de los sistemas caóticos en tiempo continuo con la implementación experimental de la versión de *tiempo continuo* de la aplicación del panadero.

Bibliografía

[1] A. Akhavan S-C Lim A. Akhshani, S. Behnia and Z. Hassan. An image encryption approach using quantum chaotic map. 2013.

[2] P. Van Oorschot A. Menezes and S. Vanstone. Handbook of applied cryptography. 2001.

[3] L. B. Almeida. The fractional Fourier transform and time-frequency representations. *IEEE Transactions on signal processing*, 42(11):3084–3091, Nov 1994.

[4] A. Argüelles. Construcción de la función de Wigner para espacio de fase discretos. Master's thesis, 2004.

[5] A. Argüelles and T. Dittrich. Wigner function for discrete phase space: Exorcising ghost images. *Physica A.*, 356:72–77, 2005.

[6] B. Georgeot B. Lévi and D. L. Shepelyansky. Quantum computing of quantum chaos in the kicked rotator model. *Phys. Rev. Lett*, 67:046220, 2003.

[7] N. L. Balazs and A. Voros. The quantized baker's transformation. *Europhys. Lett*, 1987.

[8] M. V. Berry. Semi-classical mechanics in phase space: a study of Wigner's function. *Phil. Trans. R. Soc. A.*, 1977.

[9] T. A. Brun and R. Schack. Realizing the quantum baker's map on a NMR quantum computer. *Phys. Rev. Lett*, 1998.

[10] B. Diu C. Cohen-Tannoudji and F. Laloe. *Quantum Mechanics*. John Wiley and Sons. Inc., 1977.

[11] P. Carriére. On a three-dimensional implementation of the baker's transformation. *Physics of fluids*, 2007.

[12] M. A. Kutay Ç. Candan and H. M. Ozaktas. The discrete fractional Fourier transform. *IEEE Transactions on signal processing*, 48, 2000.

[13] S. C. Coutinho. *The Mathematics of Ciphers: Number Theory and RSA Cryptography*. A. K Peters Ltd, 1999.

[14] A. M. Osorio de Almeida and M. Saraceno. Periodic orbit theory for the quantized baker's map. *Annals of physics.*, 1991.

[15] A. M. Ozorio de Almeida. The Weyl representation in classical and quantum mechanics. *Phys. Rep.*, 295, 1998.

[16] T. Dittrich and L. A. Pachón. Time-domain scars: Resolving the spectral form factor in phase space. *Phys. Rev. Lett.*, 102:150401, Apr 2009.

[17] J. Fridrich. Symetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 8, 1997.

[18] J. Lomonaco Jr. A talk on quantum cryptography, or how alice outwits eve. *ArXiv e-prints*, 2001.

[19] M. A. Kutay and Z. Zalevsky. *The Fractional Fourier Transform: With Applications in Optics and Signal Processing*. Wiley, 2001.

[20] A. Voros M. J. Giannoni and J. Zinn-Justin. Chaos and quantum physics. *Les Houches Lectures LII.*, 1992.

[21] H. M. Ozaktas and A. Kutay. Introduction to the fractional Fourier transform and its applications. *Phys. Rev. Lett.*, 104:180501, 2010.

[22] C. E. Pachón and L. A. Pachón. The origin of the dynamical quantum non-locality. *ArXiv e-prints*, July 2013.

[23] L. A. Pachón. *Coherence and Decoherence in the Semiclassical propagation of the Wigner function*. PhD thesis, 2010.

[24] B. E. Anderson-S. Ghose S. Chudhury, A. Smith and P. S. Jessen. *Quantum signatures of chaos in a kicked top*. PhD thesis, 2009.

[25] B. Santhanam and J. H. McClellan. The discrete rotational Fourier transform. *IEEE Transactions on signal processing*, 44(4):994–998, Apr 1996.

[26] M. Saraceno and R. O. Vallejos. The quantized D transformation. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 6:193–199, 1996.

[27] M. Saraceno and A. Voros. Towards a semiclassical theory of the quantum baker's map. *Physica D.*, 1994.

[28] R. Schack. Using a quantum computer to investigate quantum chaos. *Phys. Rev. Lett*, 57, 1998.

[29] G. Tanner. Periodic orbit action correlations in the baker map. *J. Phys. A: Math*, 1999.

[30] H. Weyl. *Gruppentheorie und Quantenmechanik*. Hirzel, Leipzig, 1928.

[31] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev. Lett.*, 40:749–759, 1932.

[32] C. P. Williams. Explorations in quantum computing. 2011.

[33] S. Lian Y. Mao, G. Chen. A novel fast image encryption scheme based on 3d chaotic baker maps. *International Journal of Bifurcation and Chaos,*, 14, 2004.

[34] J. Emerson Y. S. Weinstein, S. Lloyd and D. G. Cory. Experimental implemetation of the quantum baker's map. *Phys. Rev. Lett*, 89, 2002.

[35] W. H. Zurek. Sub-planck structure in phase space and its relevance for quantum decoherence. *Nature Lett.*, 412:712–717, 2001.

APÉNDICE A

Transformación de Fourier como una rotación en el espacio de fase

La transformación de Fourier ordinaria se define en [25] como

$$X(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}q x(t) \exp\left[(-\mathrm{i}\omega t)\right], \tag{A.1}$$

donde se transforma una función $x(t)$ en $L^2(\mathbb{R})$ en una función $X(p)$ en $L^2(\mathbb{R})$.

Aplicando la transformación de Fourier $\mathcal{F}$ dos, tres y cuatro veces, sobre $x(t)$ se tiene

$$\begin{aligned} \mathcal{F}^2[x](t) &= x(-t), \\ \mathcal{F}^3[x](t) &= X(-\omega), \\ \mathcal{F}^4[x](t) &= x(t), \end{aligned}$$

donde se observa que $\mathcal{F}^2$, $\mathcal{F}^3$ y $\mathcal{F}^4$ corresponden a rotaciones de 180, 270 y 360 grados en el espacio de fase (p, q), respectivamente. Entonces, la transformación de Fourier ordinaria representa rotaciones de 90 grados.

Para demostrar que la transformación de Fourier fraccionaria corresponde a rotaciones continuas en el espacio de fase, se utiliza la distribución de Wigner, definida en [3] como

$$\overline{W}(t, \omega) = \int_{-\infty}^{\infty} \mathrm{d}\tau f\left(t + \frac{\tau}{2}\right) f^*\left(t - \frac{\tau}{2}\right) \exp\left[-\mathrm{i}\omega\tau\right], \tag{A.2}$$

que puede reescribirse como

$$\overline{W}(t, \omega) = 2 \exp\left[2i\omega t\right] \int_{-\infty}^{\infty} \mathrm{d}\tau f(\tau) f^*(2t - \tau) \exp\left[-2\mathrm{i}\omega\tau\right]. \tag{A.3}$$

La función $f^*(2t - \tau)$ se expresa en [3] como

$$f^*(2t - \tau) = \int_{-\infty}^{\infty} \mathrm{d}z \mathcal{F}_\alpha^*(-z + 2t\cos\alpha) \times \exp\left[-2\mathrm{i}t^2 \sin\alpha\cos\alpha + 2\mathrm{i}zt\sin\alpha\right] K_\alpha(\tau, z), \tag{A.4}$$

donde $\mathcal{F}_\alpha(z)$ denota la transformación de Fourier fraccionaria de orden α de $f(t)$.

Reemplazando (A.4) en (A.3) se obtiene que

$$\begin{aligned}\overline{W}(t,\omega) &= 2\exp\left[2\mathrm{i}\omega t\right]\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}\tau\mathrm{d}z f(\tau)\mathcal{F}_{\alpha}^{*}(-z+2t\cos\alpha)\exp\left[-2\mathrm{i}t^{2}\sin\alpha\cos\alpha+2\mathrm{i}zt\sin\alpha\right]\\ &\times K_{\alpha}(\tau,z)e^{-2\mathrm{i}\omega\tau},\\ &= 2\exp\left[2\mathrm{i}\omega t\right]\int_{-\infty}^{\infty}\mathrm{d}z\mathcal{F}_{\alpha}^{*}(-z+2t\cos\alpha)\exp\left[-2\mathrm{i}t^{2}\sin\alpha\cos\alpha+2\mathrm{i}zt\sin\alpha\right]\\ &\times\int_{-\infty}^{\infty}\mathrm{d}\tau f(\tau)\exp\left[-2\mathrm{i}\omega\tau\right]K_{\alpha}(\tau,z).\end{aligned} \tag{A.5}$$

Utilizando el hecho que $f(t)\exp\left[\mathrm{i}vt\right]$ se expresa en términos de la transformación de Fourier de orden fraccionario como $\mathcal{F}(u-v\sin\alpha)\exp\left[\mathrm{i}\frac{\tau^{2}}{2}\sin\alpha\cos\alpha+\mathrm{i}uv\cos\alpha\right]$, se tiene que

$$\begin{aligned}\overline{W}(t,\omega) = 2\exp\left[2\mathrm{i}\omega t\right]&\int_{-\infty}^{\infty}\mathrm{d}z\mathcal{F}_{\alpha}(-z+2\omega\sin\alpha)\mathcal{F}_{\alpha}^{*}(-z+2t\cos\alpha)\\ &\times\exp\left[-2\mathrm{i}(t^{2}+\omega^{2})(\sin\alpha\cos\alpha+2\mathrm{i}zt\sin\alpha-2\mathrm{i}z\omega\cos\alpha)\right],\end{aligned} \tag{A.6}$$

realizando el cambio de variable $\varepsilon = z+2\omega\sin\alpha$ y reescribiendo la ecuación anterior

$$\begin{aligned}\overline{W}(t,\omega) = 2\exp\left[2\mathrm{i}\omega t\right]&\int_{-\infty}^{\infty}\mathrm{d}\varepsilon\mathcal{F}_{\alpha}\mathcal{F}_{\alpha}^{*}(-\varepsilon+2t\cos\alpha+2\omega\sin\alpha)\\ &\times\exp\left[2\mathrm{i}(\omega^{2}-t^{2})\sin\alpha\cos\alpha+\mathrm{i}\varepsilon(t\sin\alpha-\omega\cos\alpha-4\mathrm{i}\omega t\sin^{2}\alpha)\right].\end{aligned} \tag{A.7}$$

Realizando el cambio de variables

$$\begin{aligned}u &= t\cos\alpha+\omega\sin\alpha,\\ v &= -t\sin\alpha+\omega\cos\alpha,\end{aligned}$$

se rotan los ejes t y ω por un ángulo α. Simplificando la expresión (A.7) se obtiene

$$\overline{W}(t,\omega) = 2\exp\left[2\mathrm{i}uv\right]\int_{-\infty}^{\infty}\mathrm{d}\varepsilon\mathcal{F}_{\alpha}(\varepsilon)\mathcal{F}_{\alpha}^{*}(2u-\varepsilon)\exp\left[2\mathrm{i}v\varepsilon\right]. \tag{A.8}$$

Comparando las ecuaciones (A.3) y (A.8) se observa que la distribución de Wigner de f coincide con la distribución de Wigner de $\mathcal{F}_{\alpha}$, pero ésta última ha rotado un ángulo $-\alpha$, que corresponde al cambio de ejes (t,ω) por (u,v), es decir, la transformación de Fourier fraccionaria induce una rotación en la distribución de Wigner.

APÉNDICE B

Compuertas cuánticas

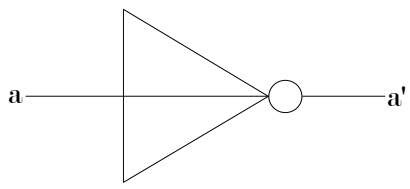
Una compuerta lógica transforma sus bits de entrada en uno o más bits de salida de acuerdo su definición. A continuación se presenta una descripción de las compuertas cuánticas. Todos los detalles presentados aquí, símbolos y tablas de verdad de las compuertas, pueden encontrarsen en el capítulo 2 de la Ref. [32].

- **Compuerta NOT:** Es la compuerta lógica reversible más sencilla, posee una entrada y una salida, su tabla de verdad y representación en un circuito se muestra a continuación.

Tabla B.1: Tabla de verdad para la compuerta NOT.

a	a′
0	1
1	0

Figura B.1: Esquema del circuito para la compuerta NOT.



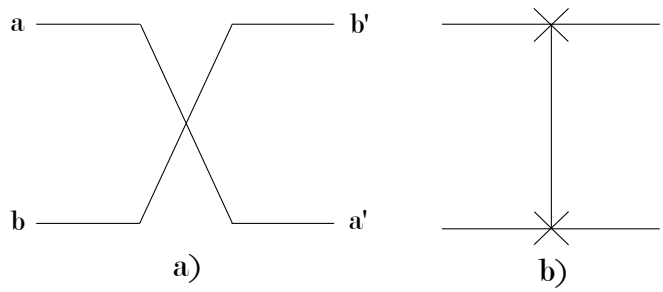
Esta es una compuerta que opera sobre 1 qubit y como se puede observar en la figura, NOT tiene como función invertir dicho qubit.

- **Compuerta SWAP:** Es una compuerta de 2 qubits, que como lo indica su nombre, intercambia los qubits de entrada.

Tabla B.2: Tabla de verdad para la compuerta SWAP.

a	b	a′	b′
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Figura B.2: a) Esquema de la compuerta SWAP, b) esquema más usado en los circuitos.



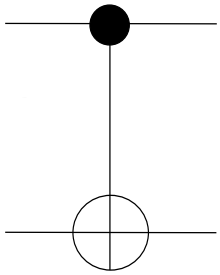
Su correspondiente tabla de verdad e ícono se muestran en la figura anterior.

- **Compuerta CNOT:** ControlledNot (CNOT), es una compuerta NOT controlada de dos qubits. Su función es verificar el valor del primer qubit, si éste es 1, entonces invierte el valor del segundo qubit, es decir, el valor del primer qubit controla la aplicación del NOT en el segundo qubit.

Tabla B.3: Tabla de verdad para la compuerta CNOT.

a	b	a′	b′
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Figura B.3: Esquema del circuito de la compuerta CNOT.



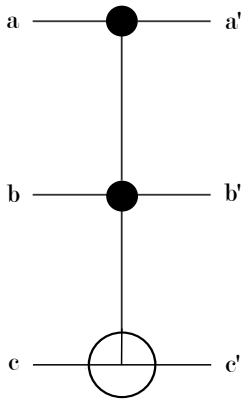
La tabla y la figura anteriores corresponden a la tabla de verdad y el icono que representa la compuerta CNOT respectivamente.

- **Compuerta TOFFOLI:** Es una compuerta cuántica universal, corresponde a una compuerta CNOT controlada que opera sobre 3 qubits. En la tabla y figura se observan la tabla de verdad y el ícono utilizado en los circuitos.

Tabla B.4: Tabla de verdad para la compuerta TOFFOLI.

a	b	c	a′	b′	c′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Figura B.4: Esquema del circuito de la compuerta TOFFOLI.



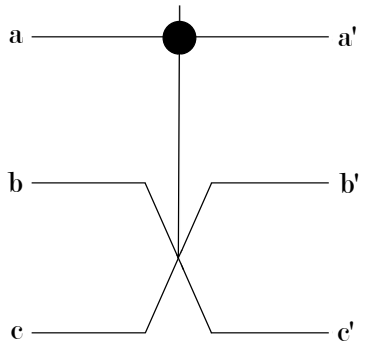
La aplicación del NOT sobre el tercer qubit esta controlada por los dos primeros qubits, es decir, si el valor de los dos primeros es 1 entonces se invierte el valor del tercero.

- **Compuerta FREDKIN:** Al igual que la compuerta anterior, FREDKIN es una compuerta cuántica universal que opera sobre 3 qubits, pero esta corresponde a una compuerta SWAP controlada. A continuación se muestran la tabla de verdad y el ícono utilizado en los circuitos.

Tabla B.5: Tabla de verdad para la compuerta FREDKIN.

a	b	c	a′	b′	c′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Figura B.5: Esquema del circuito de la compuerta FREDKIN.



Si el valor del primer qubit es 1 entonces se cambian el segundo y tercer qubit.