Sistema de Comunicación OFDM Óptico-Criptográfico

C. Ferrin and J. Léon

***Abstract*— This paper presents conception and software implementation of an Encrypted Optical OFDM System. A Fourier Encryption Optical technique is conceived for data security, and adequate encoding of complex information is realized to couple with OFDM transmitter and receiver. The simulations suggest that optical encryption blocks into an Optical OFDM communication system decrease intensity values of images when transmitted, under Additive White Gaussian Noise assumption for optical links.**

***Keywords*— Optical Encryption, OFDM (Orthogonal Frequency-Division Multiplexing), Digital Communication.**

I. INTRODUCCION

El usuario de las tecnologías de información y comunicación (TIC's) cada día demanda mayor velocidad en transferencia de datos (principalmente multimedia) y a su vez la seguridad suficiente para proteger su contenido. En estos dos contextos Colombia ha tomado dos grandes decisiones que marcarán el futuro de la sociedad: por un lado, en 2008, la Comisión Nacional de Televisión (CNTV) seleccionó la norma de origen Europeo DVB-T [1], [2] como el estándar de la Televisión Digital Terrestre (TDT) que se emitirá en el país. Y por otro lado, en 2011, establece una política de ciberseguridad y ciberdefensa detallada en el CONPES 3701 [3] que vigilará y protegerá la actividad de los usuarios en esta era de la información.

La tecnología DVB-T basa su principio de operación en la Multiplexación por División de Frecuencias Ortogonales (OFDM – siglas en inglés) [4], [5], el cual es un esquema de comunicación multiportadora, desarrollado desde 1966, que resuelve dos grandes problemas: la interferencia intersimbólica (ISI - siglas en inglés) [6], [7]y la interferencia interportadora [ICI - siglas en inglés] [6], [7]. Para lograr lo anterior, combina portadoras con bajas tasas de transferencia para construir un sistema compuesto de comunicación de altas tasas de transferencia. La ortogonalidad permite que las portadoras puedan estar cercanamente espaciadas, inclusive ligeramente traslapadas, evitando así la ISI. Las bajas tasas de transferencia de las portadoras implican largos periodos en los símbolos, y esto disminuye significativamente la ICI. La generación y detección de este tipo de portadoras se logra mediante operaciones en tiempo discreto, utilizando la Transformada Discreta de Fourier inversa (IDFT), y directa (DFT) [7].

C. Ferrin, Universidad del Valle, carlos.ferrin@correounivalle.edu.co
J. León, Universidad Autónoma de Bucaramanga, jleon544@unab.edu.co

De igual manera, desde hace algunas décadas, y hoy en día la comunidad de científicos en comunicaciones ópticas ha incrementado su interés por la investigación en el OFDM Óptico [8], [9]. Se han realizado una serie de demostraciones experimentales de transferencia de datos hasta 1Tb s^{-1} [8], junto con un avance rápido en demostraciones de tiempo real. En este nuevo enfoque el principio de operación del OFDM [4], [5], [6] se conserva en la etapa codificación-decodificación de los datos de entrada y salida, ver figura 1; el canal de comunicación está constituido ahora por enlaces ópticos (principalmente fibra óptica), y las etapas de modulación RF (Radio Frecuencia) se han reemplazado por moduladores ópticos, a la entrada y salida del receptor y transmisor OFDM, respectivamente.

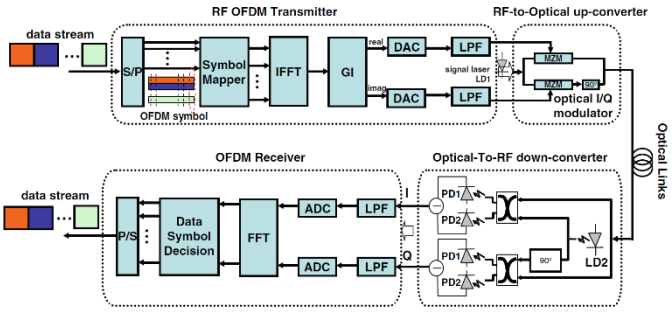

Figura 1. Diagrama de bloques conceptual de un sistema comunicación OFDM. Tomado de [8].

Generalmente, antes que los datos entren al transmisor OFDM, estos son cifrados para proteger su contenido. En este campo del cifrado se ha desarrollado un sinnúmero de técnicas digitales, y en la práctica dependiendo de la aplicación se decide entre utilizar técnicas convencionales a técnicas avanzadas [10]. Sin embargo cada vez que se desarrolla una técnica de cifrado, también se investiga la forma para atacarla y poderla descifrar. En esta misma línea de investigación la comunidad de científicos ópticos han propuesto esquemas para cifrar la información [11] demostrando alta invulnerabilidad frente a las propuestas digitales.

Las técnicas de cifrado óptico han sido investigadas y evaluadas [11], [12], [13], [14], convirtiéndose en una alternativa novedosa en un mundo de computación basado en tecnología óptica. Algunas de estas basan su principio de funcionamiento en la transformada de Fourier (la lente es un elemento transformante en el plano de Fourier de la misma) y la ubicación de máscaras aleatorias de fase (la llave) dentro del proceso. Otros investigadores [11], [12] han propuesto el uso de la transformada wavelet [14] y la propuesta de esquemas ópticos para lograrlo, e inclusive las versionas

fraccionales de estas últimas [13], [14], donde el orden fraccional constituye la llave, y su posibilidad de implementación fuera de la región paraxial a nivel óptico [15], [16]. En esta oportunidad se centrará la atención en el esquema de cifrado basado en Fourier que utiliza máscara de fase aleatoria como llave de cifrado. En este enfoque se utiliza un esquema 4f de lentes cóncavas como modelo físico propuesto en [11] (ver figura 2), y en la figura 3 se puede ver el modelo matemático en diagrama de bloques.

Para una descripción más amplia se puede consultar la descripción matemática detallada en [12] de este proceso de cifrado óptico.

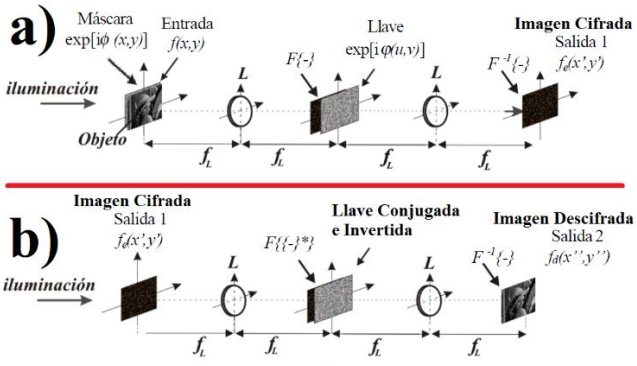

Figura 2. Modelo físico del proceso a) cifrado de la imagen, b) descifrado de la imagen. ***L*** es una lente cóncava y f_L su distancia focal. Tomado de [11].

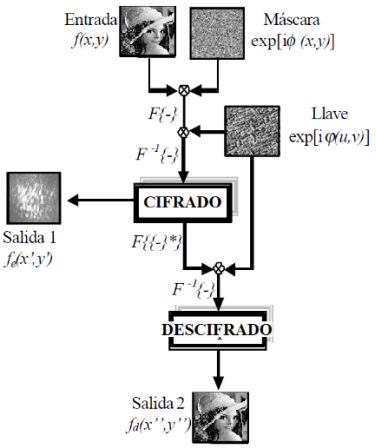

Figura 3. Flujograma del proceso de Cifrado-Descifrado mediante la Transformada de Fourier. $\boldsymbol{F}\{\ \}$ y $\boldsymbol{F^{-1}}\{\ \}$ indican Transformad Directa e Inversa de Fourier, respectivamente. × indica multiplicación compleja punto a punto, y { }* indica complejo conjugado. Tomado de [12].

Lo que se plantea ahora es desarrollar un esquema de comunicación OFDM Óptico que incluya etapas de cifrado-descifrado óptico, y evaluar el efecto que tiene en el primero el último. Para ello se propone un método de simple codificación de la imagen cifrada antes de entrar al transmisor OFDM, y se utilizan métricas de evaluación como la relación señal a ruido entre la imagen de entrada y la imagen de salida y el error medio cuadrático entre las mismas.

I. METODOLOGÍA

En la figura 4 muestra el diagrama de bloques para la propuesta del sistema de comunicación OFDM Óptico Criptográfico.

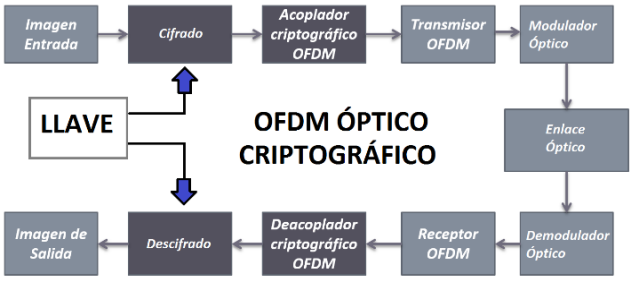

Figura 4. Diagrama de bloques del sistema de comunicación OFDM Óptico Criptográfico.

La **imagen de entrada**, I_e, (de 1 canal y 8 bit) es cifrada utilizando **llave** (matriz aleatoria de números complejos de magnitud unitaria e igual tamaño de la imagen de entrada) y el método propuesto en [11], [12], el cual fue ilustrado en las figuras 2 y 3. A la salida del bloque de cifrado se tiene una matriz de valores complejos de igual tamaño a la imagen de entrada la cual es codificada (en el **Acoplador Criptográfico OFDM**) como una matriz del doble de ancho de la imagen de entrada y en cada mitad se guarda la parte real e imaginaria. Esta última matriz se convierte en una trama de datos y se envían al **Transmisor OFDM** que se encarga de codificar la información que posteriormente se **modula ópticamente** para ser enviado a través del **enlace óptico**, el cual en esta oportunidad se modela como un canal de comunicación que únicamente agrega Ruido Blanco Gaussiano Aditivo (AWGN – siglas en inglés) [7] a la señal que viaja a través del enlace. Los bloques siguientes al enlace óptico se encargan de realizar los procesos inversos a los de la etapa de transmisión y así obtener la **imagen de salida**, I_s.

Con base en el sistema de comunicación OFDM propuesto en [6] se establecen los siguientes parámetros que definen la arquitectura final del sistema de comunicación digital:

1. Tamaño de la IDFT (T_IDFT).
2. Número de Portadoras (NP).
3. Amplitud de Corte a la llegada de las portadoras (AC).
4. El SNR_C (Signal to Noise Ratio) del enlace.
5. Tipo Modulación (BPSK, QPSK 16PSK y 256PSK) [6], [7].

En este caso existe una relación entre el tamaño de la IDFT y el Número de Portadoras que debe respetarse:

$$NP \leq \frac{T\_IDFT}{2} - 2 \qquad (1)$$

Para evaluar el desempeño del sistema se utilizan el Error Medio Cuadrático (MSE) [7] y la relación señal a ruido (SNR)

[7] entre la imagen de entrada y la de salida, las cuales se establecen a continuación.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[I_e(x,y) - I_s(x,y)]^2 \qquad (2)$$

$$SNR(dB) = 10log\left(\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[I_e(x,y)]^2}{(MN)*(MSE)}\right) \qquad (3)$$

Donde M y N son el alto y ancho de la imagen de entrada respectivamente.

II. I MPLEMENTACIÓN

Para la generación de llaves se desarrolla una GUI en Matlab 2012b, la cual se puede descargar de [17], ver figura 5.

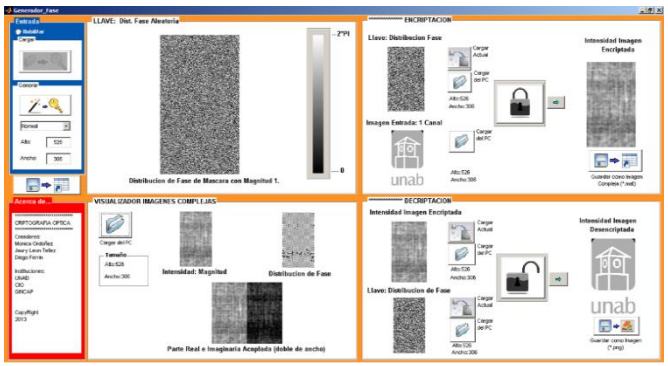

Figura 5. GUI para generación de Llaves para cifrado óptico.

La interfaz permite realizar procesos de cifrado y descifrado, así como guardar los diferentes resultados en archivos **.mat*.

Y en la figura 6 se puede ver la GUI desarrollada también en Matlab 2012b para el Sistema de Comunicación OFDM Óptico Criptográfico.

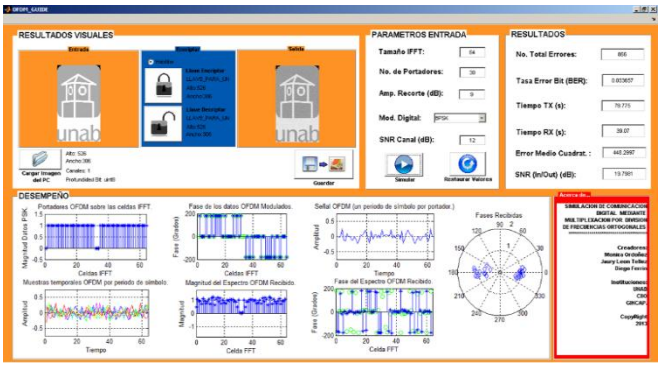

Figura 6. GUI para el Sistema de Comunicación OFDM Óptico Criptográfico.

En él se puede realizar simulación del proceso de transmisión de imágenes con y sin cifrado, pudiendo variar los parámetros que definen la arquitectura OFDM (mencionados en la sección anterior). La plataforma de simulación permite visualizar las diferentes métricas de desempeño en forma gráfica y numérica.

III. RESULTADOS Y DISCUSIÓN

Aun cuando es posible seleccionar diferentes configuraciones para realizar simulaciones, a continuación se mostrarán resultados obtenidos bajo la configuración presentada en la tabla 1.

TABLA I. VALORES DE LOS PARÁMETROS PARA DEFINIR UNA ARQUITECTURA OFDM DE EXPERIMENTACIÓN.

PARÁMETRO	VALOR
T_IDFT	2048
NP	1009
AC	9dB
Tipo Modulación	BPSK
Imagen (Ver fig. 7)	1 Canal, 8 bits, 300x300.

En la figura 7 se puede ver la imagen de prueba y la distribución de fase de la llave sintetizada con la GUI de la figura 5. Puede notarse en la tabla 1 que NP respeta la restricción impuesta en la ecuación 1.

Figura 7. Imagen de Entrada, Izq. Llave para cifrado óptico, Der.

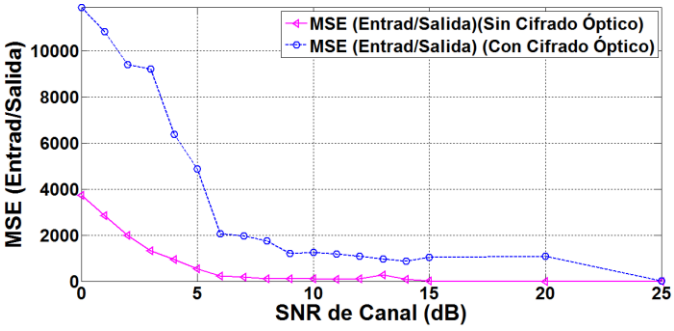

Figura 8. Curvas del comportamiento del MSE (Entrada/Salida) con y sin cifrado óptico utilizando modulación BPSK sobre un enlace óptico modelado como AWGN.

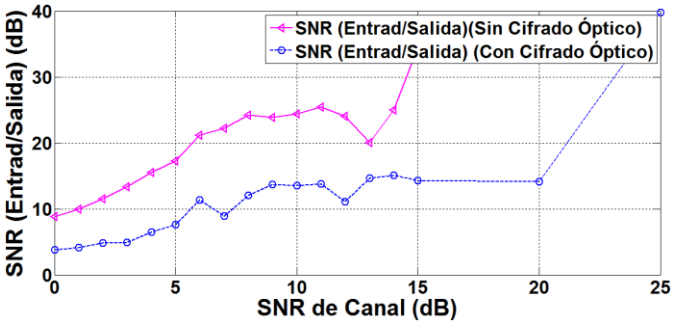

Figura 9. Curvas del comportamiento del SNR (Entrada/Salida) con y sin cifrado óptico utilizando modulación BPSK sobre un enlace óptico modelado como AWGN.

Se varía el SNR_C desde 0dB hasta 15 dB en incrementos de 1B, y de 15 dB hasta 25dB en incrementos de 5dB. En las figuras 8, 9 se puede ver el comportamiento del MSE del SNR de la imagen de entrada con respecto a la imagen de salida, en función del SNR_C, respectivamente.

Las figuras 8 y 9 muestran claramente que con un ruido de canal hasta de 20dB la calidad de la imagen de salida es más afectada para el caso en el que se utiliza cifrado óptico que en el caso que no se utiliza cifrado. En las pruebas realizadas se pudo observar también que el MSE (Entrada/Salida) llegaba a ser cero y el SNR (Entrada/Salida) tendía a infinito (fidelidad total en la imagen transmitida) cuando los valores de SNR_C eran mayores a 25dB para ambos casos (con y sin cifrado). El la figura 10 se puede observar la imagen de salida para algunos valores de SNR_C.

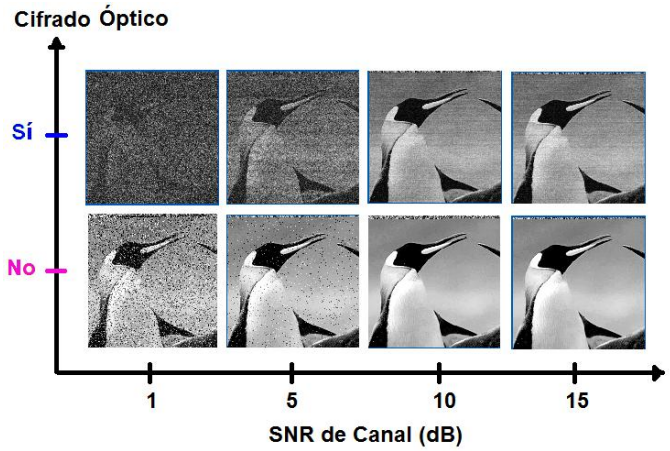

Figura 10. Imágenes de Salida obtenidas con y sin cifrado para 4 valores de SNR_C.

Igualmente, en la figura 11, se muestra el comportamiento de la Tasa de Error de Bit (BER – siglas en inglés) [7] en función del ruido del canal. El BER es similar para las dos situaciones planteadas hasta 5dB, entre 5dB y 15dB el BER es mayor para el caso sin cifrado. Es importante anotar que la cantidad de información a transmitir es mayor para el caso con cifrado óptico. De todas formas al igual que en el caso anterior a partir de 20dB el BER es nulo

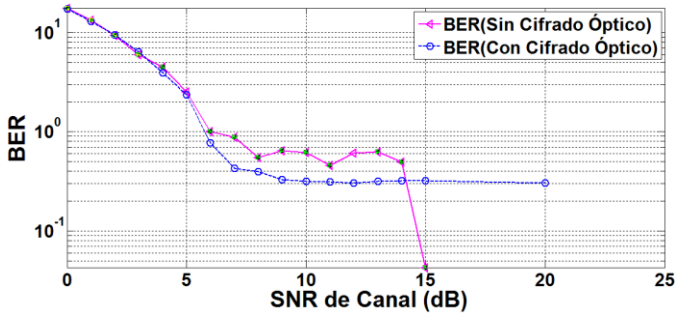

Figura 11. BER en función del ruido de canal con y sin cifrado óptico.

En términos generales, la inclusión del bloque de cifrado óptico tiene un efecto más de oscurecer la imagen que afectar el cifrado como tal, como puede verse en la figura 10. Esto puede mejorarse con técnicas de manipulación del histograma de la imagen, algo que podría incluirse como un bloque adicional dentro del proceso de descifrado óptico.

Experiencias similares se realizaron con otros tipos de modulación como QPSK, 16PSK y 256PSK llegando resultados similares evidenciando únicamente las diferencias propias de cada tipo de modulación [4], [5], [6], [7].

IV. CONCLUSIONES

En este trabajo se ha presentado la implementación software de un sistema de comunicación digital OFDM Óptico Criptográfico. La herramienta desarrollada provee una completa plataforma de simulación de este tipo de sistemas pudiendo configurar parámetros que definen la arquitectura final del sistema de comunicación.

Las pruebas realizadas bajo la configuración de los parámetros de la tabla 1, permite concluir que el efecto del bloque de cifrado dentro del sistema de comunicación es el de disminuir la intensidad de los niveles de gris de la imagen de entrada para valores del SNR_C hasta 20 dB, a partir de este valor la diferencia entre utilizar o no cifrado es prácticamente nula.

En trabajos futuros se sugiere utilizar modelos más realísticos del canal de comunicación óptico (modelos no lineales, dispersivos), así como considerar modulaciones no solamente en fase, sino también en amplitud.

AGRADECIMIENTOS

A la Dirección de Investigaciones y al Centro de Investigación en Ingeniería y Organizaciones, CIIO, por el apoyo brindado en marco del proyecto titulado: ***Desarrollo de una plataforma software criptográfica de transmisión y recepción de imágenes utilizando técnicas ópticas de compresión y encriptación modernas para aplicación en ciberseguridad.***

REFERENCIAS

[1] U. Ladebusch and C. Liss, “Terrestrial DVB (DVB-T): A Broadcast Technology for Stationary Portable and Mobile Use,” in *Proceedings of IEEE*, 2006, vol. 94, no. 1, pp. 183–193.

[2] A. Delgado, *TRANSMISIÓN DE SEÑALES DE TV DIGITAL EN EL ESTÁNDAR TERRENO DVB-T*. 2002, p. 38.

[3] MINTIC, MINDEFENSA, and MININTERIOR, “Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa,” 2011.
[4] W. Kabir, “Orthogonal Frequency Division Multiplexing (OFDM),” in *2008 China-Japan Joint Microwave Conference*, 2008, pp. 178–184.
[5] X. Wang, “OFDM and its application to 4G,” in *14th Annual International Conference on Wireless and Optical Communications, 2005. WOCC 2005*.
[6] P. G. Lin, “OFDM SIMULATION in MATLAB,” California Polytechnic State University, 2010.
[7] B. Sklar, *Digital communications fundamentals and applications*, 1st ed. Los Ángeles, California, 2005, p. 500.
[8] S. Kumar, Ed., *Impact of Nonlinearities on Fiber Optic Communications*. New York, NY: Springer New York, 2011.
[9] O. González, *Estudio de la aplicación de técnicas de modulación OFDM para comunicaciones ópticas guiadas en el canal infrarrojo*. 2004, p. 166.
[10] M. R. Doomun and K. M. S. Soyjaudah, “Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security,” *International Journal of Network Security*, vol. 9, no. July 2009, pp. 82–94, 2009.
[11] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.
[12] J. Rueda, A. Romero, and L. Castro, “CRIPTOGRAFÍA DIGITAL BASADA EN TECNOLOGÍA ÓPTICA,” *BISTUA*, vol. 3, pp. 19–25, 2005.
[13] J. M. Vilardy, C. O. Torres, and L. Mattos, “Digital Images Encryption Via Discrete Fractional Fourier Transform And Jigsaw Transform,” *Revista Colombiana de Fisica*, vol. 43, pp. 523–527, 2011.
[14] J. M. Vilardy, J. Useche, C. O. Torres, and L. Mattos, “Cifrado De Imágenes Utilizando La Transformada Wavelet Fraccional,” *Revista Colombiana de Fisica*, vol. 43, 2011.
[15] M. Born and E. Wolf, *Principles of Optics Electromagnetic Theory of Propagation, Interference and Diffraction of Light*, 7th ed. 1999, p. 985.
[16] E. Hecht, *Óptica*, 3rd ed. 2001, p. 722.
[17] C. Ferrin, J. León, and M. Ordoñez, “crypto-simulator-optical-based.” Bucaramanga, p. 1, 2013.

Carlos Ferrin recibió su título de Ingeniero Físico en 2010 de la Universidad del Cauca (Colombia). Actualmente es candidato a Magister en Ingeniería Electrónica de la Universidad del Valle. Sus áreas actuales de interés son el procesamiento de señales e imágenes y los sistemas de comunicación digital.

Jauri León recibió su título de Licenciado en Física en 1977 y Magister en Física en 1980 ambos en la Universidad Industrial de Santander (Colombia). Actualmente trabaja en la Universidad Autónoma de Bucaramanga. Su campo de interés es la Óptica Aplicada en Ciencia e Ingeniería y Biomédica.