Investigación

Una marca de agua frágil en el dominio de los momentos ortogonales de Krawtchouk

A fragile watermarking on the domain of Krawtchouk's orthogonal moments

Alicia María Centurión Fajardo, Nancy Céspedes Trujillo,

Eduardo Moreno Roque

Revista de Investigación

Volumen XI, Número 1, pp. 017–028, ISSN 2174-0410
Recepción: 8 Jul'20; Aceptación: 8 Sep'20

01 de abril de 2021

Resumen

En esta contribución, proponemos un esquema de marca de agua frágil basada en los momentos ortogonales de Krawtchouk. El algoritmo propuesto inserta la marca de agua generada en los primeros ocho coeficientes de los momentos de Krawtchouk, calculados a partir de la imagen cubierta, con el propósito de garantizar la integridad y autenticidad de la fuente emisora. Además, mediante una clave privada, una clave pública y la función criptográfica Hash - Sha256 se genera una marca de agua frágil que será incrustada en la imagen original. El trabajo experimental sobre la validación del esquema propuesto consiste en el cálculo de la relación señal / ruido pico (PSNR) y en la detección de manipulación de la imagen marcada.

Palabras Clave: Autenticidad, Detección de manipulación, Integridad, Marca de agua frágil, Momentos ortogonales de Krawtchouk

Abstract

In this contribution, we propose a fragile watermarking scheme based on Krawtchouk orthogonal moments. The proposed algorithm inserts the watermarking generated in the first eight coefficients of the Krawtchouk moments, calculated from the covered image, in order to guarantee the integrity and authenticity of the emitter source. Additionally, using a private key, a public key and the Hash-Sha256 cryptographic function, a fragile watermark is generated and will be embedded in the original image. The experimental work on the validation of the proposed scheme consists of calculating the signal-to-noise ratio (PSNR) and detecting manipulation of the watermarked image.

Keywords: Authenticity, Tamper detection, Integrity, fragile watermarking, Krawtchouk orthogonal moments

1. Introducción

Hoy en día, la seguridad de la información es una preocupación constante por todos los usuarios de la red, y los piratas informáticos constituyen una amenaza para dicha seguridad, es por ello que para la transmisión de datos a través de los diferentes canales se necesitan técnicas de encriptación fuertes con el objetivo de garantizar la seguridad deseada [16], la popularización del internet y el uso cada vez más habitual de tecnologías digitales ha provocado que compartir información de diferentes medios digitales, ya sean imágenes, música o video, sea más fácil que nunca y se ha trabajado en proteger las imágenes digitales [14].

Lo anterior llega a ser un asunto de vital importancia, existiendo la necesidad de alcanzar, una protección adecuada de la información, evitando su uso, modificación, grabación o destrucción por usuarios no autorizados, o personas mal intencionadas [18, 19].

En los últimos años han surgido distintos métodos para tratar de proporcionar protección a la información digital y salvaguardar los derechos de sus propietarios, entre los cuales se destaca el uso de marcas de agua digitales, estas son un caso particular de una amplia familia de técnicas destinadas a ocultar información, englobada bajo el epígrafe común de esteganografía [10].

La esteganografía constituye un conjunto de técnicas las cuales permiten ocultar o camuflar cualquier tipo de datos dentro de información considerada como válida [8, 18, 19]. Además, la misma permite burlar la vigilancia electrónica en el Internet, o simplemente que terceras personas no tengan acceso a información no autorizada.

La marca de agua digital es un código de identificación que se inserta directamente en el contenido de un archivo multimedia (imagen, audio, video), de manera que sea difícil de apreciar por el sistema perceptual humano, pero fácil de detectar usando un algoritmo dado y una clave, en un ordenador [13].

Existen múltiples clasificaciones de las marcas de agua, dependiendo del tipo de señal sobre la que se aplica, del método de detección, el dominio con el cual se trabaja y la robustez.

Se pueden clasificar como visibles e invisibles. Las marcas de agua invisibles incrustan una señal aleatoria o una señal relacionada con la imagen, su ubicación es secreta, solo las personas autorizadas extraen la marca de agua durante el proceso de autenticación, y son invisibles al ojo humano [15].

En [15 y 21], se clasifican según su reacción ante los ataques en robustas, frágiles y semifrágiles

- robustas deben resistir todo tipo de ataques, detectándoselas incluso después de producidos los mismos. Sirven para proteger los derechos de autor.
- semifrágiles sobreviven a cierto tipo de alteraciones, como compresión sin pérdidas, pero deben destruirse ante cambios importantes, no reversibles.

- frágiles son aquellas que quedan eliminadas o modificadas y dejan de cumplir su función en caso de ataque. La incapacidad de recuperarlas, revela que se produjo algún cambio y ese es el objetivo buscado. No toleran ninguna transformación, ni siquiera las más comunes en procesamiento de datos. Se utilizan fundamentalmente para asegurar integridad ya que a través de ellas se conoce si el objeto fue alterado.

Las marcas de agua frágiles que son las que nos interesan en este trabajo deben cumplir dos requisitos: imperceptibilidad y capacidad [21]. La imperceptibilidad de la marca tiene como base el comportamiento del sistema perceptual humano. Una marca de agua es imperceptible, si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar [13] y la capacidad permite incorporar datos sin inconvenientes [4, 7].

Se han elaborado y son muy utilizados los algoritmos de marcas de agua frágiles, ya que su característica principal es que pueden detectar (idealmente) la alteración de un bit en el medio marcado [14].

La estructura de este documento es la siguiente: en la Sección 2 describimos el esquema de marca de agua propuesto. Finalmente, en la Sección 3, mostramos los resultados experimentales, vinculados al nivel de imperceptibilidad y a la detección de manipulación.

2. Descripción del Algoritmo

2.1 Función criptográfica Hash - Sha256

Una función hash es un proceso que transforma cualquier conjunto arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente del tamaño de los datos de entrada. En general, funciona de la siguiente forma [1]:

- El mensaje de entrada se divide en bloques.
- Un formula calcula el hash, un valor con un tamaño fijo, para el primer bloque.
- Se calcula el hash del siguiente bloque y suma al resultado anterior.
- Se realiza el mismo proceso sucesivamente hasta que se recorren todos los bloques.

[3] refiere que se llaman funciones hash criptográficas a las funciones hash que cumplen los requisitos de seguridad para ser empleadas en criptografía. Este tipo de funciones se caracterizan por presentar propiedades adicionales que las hacen resistentes frente a los ataques que intentan romper la seguridad de los sistemas informáticos.

2.2 Momentos ortogonales de Krawtchouk

Los momentos ortogonales definidos en términos de un conjunto de base ortogonal son una de las herramientas más importantes en el análisis de imagen debido a su potencialidad para representar imágenes digitales con la cantidad mínima de redundancia en la información [11]. Además, en los últimos años los polinomios de Krawtchouk han sido ampliamente

utilizados en el desarrollo de marcas de agua [5, 17, 20, 22] y en la creación de algoritmos esteganográficos para la protección y seguridad de la información confidencial [17].

Los polinomios discretos de Krawtchouk de orden n, $K_n^{p,N}(x)$, con $0 < p < 1$ [23], son aquellos polinomios que satisfacen la condición de ortogonalidad [11]

$$\sum_{0\le x\le N} K_m^{p,N}(x)\, K_n^{p,N}(x)\, \omega(x;p,N) = \rho(n;p,N)\delta_{m,n},$$

los cuales están dados explícitamente mediante

$$K_n^{p,N}(x) = {}_2F_1\left(\begin{matrix}-n,-x\\-N\end{matrix}\middle| p^{-1}\right), \qquad (1)$$

donde la función peso $\omega(x;p,N)$ está dada por

$$\omega(x;p,N) = \binom{N}{x} p^x (1-p)^{N-x},$$

mientras que el cuadrado de la norma $\rho(n;p,N)$ está dado mediante

$$\rho(n;p,N) = (-1)^n \left(\frac{1-p}{p}\right)^n \frac{n!}{(-N)_n}.$$

Aquí, ${}_rF_s$ denota la serie hiper-geométrica ordinaria definida por

$${}_rF_s\left(\begin{matrix}a_1,\dots,\ a_r\\ b_1,\dots,\ b_s\end{matrix}\middle| x\right) = \sum_{k\ge 0} \frac{(a_1,\dots,a_r)_k x^k}{(b_1,\dots,b_s)_k k!},$$

donde

$$(a_1,\dots,a_r)_k := \prod_{1\le i\le r} (a_i)_k,$$

y $(\cdot)_n$ denota el símbolo de Pochhammer [9], también se le denomina factorial desviado, definido por

$$(x)_n = \prod_{0\le j\le n-1} (x+j), \qquad n \ge 1, \qquad (x)_0 = 1.$$

Ciertamente, $\{a_i\}_{i=1}^r$ y $\{b_j\}_{j=1}^s$ son números complejos que cumplen la condición $b_j \neq -n$ con $n \in \mathbb{N} \setminus \{0\}$ para $j = 1, 2, \dots, s$.

Además, estos polinomios satisfacen la siguiente ecuación en diferencias de segundo orden (ecuación de tipo hiper–geométrica)

$$(1-p)x \triangle \nabla K_n^{p,N}(x) + \left(N_p - x\right)\Delta K_n^{p,N}(x) + nK_n^{p,N}(x) = 0,$$

así como la relación de recurrencia de tres términos

$$-xK_n^{p,N}(x) = p(N-n)K_{n+1}^{p,N}(x) - [p(N-p) + n(1-p)]K_n^{p,N}(x) + n(1-p)K_{n-1}^{p,N}(x), \qquad n \ge 1,$$

con las condiciones iniciales $K_0^{p,N}(x) = 1$ y $K_1^{p,N}(x) = (Np - x)(Np)^{-1}$. Este resultado es usado para calcular los polinomios de Krawtchouk de orden superior. Aquí, Δ y ∇ denotan los

operadores en diferencias progresivas y regresivas definidos por $\Delta f(x) = f(x+1) - f(x)$ y $\nabla f(x) = f(x) - f(x-1)$, respectivamente.

Según algunos autores [6, 24] el cálculo de los polinomios ortogonales de Krawtchouk usando (1) conduce a fluctuaciones numéricas y por tanto se hace necesario usar una versión más estable de estos, los así llamados polinomios normalizados de Krawtchouk, dados mediante,

$$\overline{K}_n^{p,N}(x) = K_n^{p,N}(x)\sqrt{\frac{\omega(x;p,N)}{\rho(n;p,N)}},$$

los cuales satisfacen la siguiente relación de recurrencia de tres términos [12]

$\alpha_n(Np - 2np + n - x)\overline{K}_n^{p,N}(x) = p(n-N)\overline{K}_{n+1}^{p,N}(x) + \beta_n n(1-p)\overline{K}_{n-1}^{p,N}(x), \quad n \geq 1,$

con las condiciones iniciales

$$\overline{K}_0^{p,N}(x) = \sqrt{\omega(x;p,N)p^{-1}}\,,$$

y

$$\overline{K}_1^{p,N}(x) = (Np - x)(Np)^{-1}\sqrt{\omega(x;p,N)(1-p)(Np)^{-1}}\,,$$

donde

$$\alpha_n = \sqrt{\frac{(1-p)(n+1)}{p(N-n)}},$$

y

$$\beta_n = \sqrt{\frac{(1-p)^2(n+1)n}{p^2(N-n)_2}}.$$

Los momentos directos de Krawtchouk de orden (n + m) en términos de los polinomios normalizados de Krawtchouk para una imagen con función de intensidad, f(x, y), están definidos como sigue:

$$Q_{nm} = \sum_{0\leq x\leq N-1}\sum_{0\leq y\leq N-1} \overline{K}_n^{p,N-1}(x)\,\overline{K}_m^{p,N-1}(y)f(x,y), \quad 0 \leq m,n \leq N-1,$$

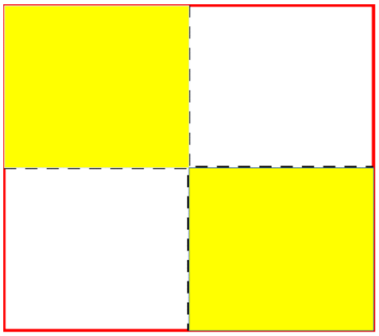
y los inversos mediante,

$$f(x,y) = \sum_{0\leq x\leq N-1}\sum_{0\leq y\leq N-1} Q_{nm}\overline{K}_n^{p,N-1}(x)\,\overline{K}_m^{p,N-1}(y), \quad 0 \leq x,y \leq N-1.$$

2.3 Algoritmo de inserción de la marca de agua frágil

A continuación se describirá detalladamente el esquema de inserción de la marca de agua frágil. Aquí se asume, que tanto el emisor como el receptor poseen el mismo sistema de claves privadas.

1.- El emisor solicita al receptor una clave pública de 128 bits.
2.- El emisor aplica la función Hash-Sha256 tanto a la clave pública como a la privada para generar de esta manera las secuencias binarias Key1Sha256 y Key2Sha256, respectivamente.
3.- Dividir la imagen en bloques no solapados de 32×32 bytes.
4.- Dividir cada bloque de 32×32 bytes en 4 bloques de 16×16 bytes.



5.- Crear una copia de cada bloque descrito en el paso 4.
6.- Sustituir los bloques de 16×16 bytes de la copia descrita en el paso 5, representados mediante el color amarillo, por Key1Sha256 y Key2Sha256, respectivamente.
7.- Aplicar la función Hash-Sha256 al bloque resultante del paso anterior para generar la secuencia binaria blockSha256.
8.- Crear la marca de agua frágil WaterMark = Unión de los primeros y últimos 32 bits de la secuencia binaria blockSha256.
9.- Dividir los bloques de 16×16 bytes, representados por el color amarillo, en 8 bloques de 8×8 bytes.
10.- Aplicar los momentos directos de Krawtchouk a cada uno de los bloques de 8×8 bytes.
11.- Insertar la WaterMark en los bits menos significativos de los primeros 8 coeficientes de los momentos directos de Krawtchouk.
12.- Aplicar los momentos inversos de Krawtchouk a cada uno de los bloques de 8×8 bytes resultantes del paso 10, para así conseguir la imagen marcada.

2.4 Algoritmo de autenticidad y detección de manipulación

1.- El receptor aplica la función Hash-Sha256 tanto a la clave pública como a la privada para generar las secuencias binarias Key1Sha256 y Key2Sha256, respectivamente.

2.- Dividir la imagen en bloques no solapados de 32 × 32 bytes.
3.- Dividir cada bloque de 32 × 32 bytes en 4 bloques de 16 × 16 bytes.
4.- Crear una copia de cada bloque descrito en el paso 4.
5.- Sustituir los bloques de 16 × 16 bytes de la copia descrita en el paso 5, representados mediante el color amarillo, por Key1Sha256 y Key2Sha256, respectivamente.
6.- Aplicar la función Hash-Sha256 al bloque resultante del paso anterior para generar la secuencia binaria blockSha256.
7.- Crear la marca de agua frágil WaterMark = Unión de los primeros y últimos 32 bits de la secuencia binaria blockSha256.
8.- Dividir los bloques de 16 × 16 bytes, representados por el color amarillo, en 8 bloques de 8 × 8 bytes.
9.- Aplicar los momentos directos de Krawtchouk a cada uno de los bloques de 8 × 8 bytes.
10.- Extraer los bits menos significativos de los primeros 8 coeficientes de los momentos directos de Krawtchouk y representar la secuencia binaria resultante mediante extractedLSB.
11.- Comparar la secuencia binaria extractedLSB con WaterMark,
- ✓ Si coinciden, la fuente emisora de la imagen marcada es auténtica.
- ✓ En caso contrario, la fuente emisora de la imagen marcada no es auténtica y se señalan los bloques modificados.

3. Análisis experimental

3.1 Prueba de imperceptibilidad

En esta sección se presentan los resultados vinculados a nivel de imperceptibilidad y a la detección de manipulación de la imagen marcada.

Una medida para determinar el nivel de imperceptibilidad es la conocida PSNR (Relación Señal a Ruido Pico). El PSNR está dado en unidades llamadas decibelios (dB) y se escribe de la siguiente forma

$$\text{PSNR}=10\log_{10}\left(\frac{256^2}{\text{MSE}}\right),$$

donde MSE está dado por el error cuadrático medio

$$\text{MSE}=\frac{1}{3mn}\sum_{1\le i\le m}\sum_{1\le j\le n}\sum_{1\le k\le 3}|I(i,j,k)-E(i,j,k)|^2\,,$$

siendo I la imagen original y E el esteganograma.

Para el primer experimento se calcularon los valores de PSNR para las imágenes de la base de datos [2] , consiguiéndose valores que se encuentran alrededor de $51.71557353931331\approx 51.72$

dB, lo cual indica que no existen diferencias significativas entre las imágenes marcadas y las imágenes originales, alcanzándose así un elevado nivel de imperceptibilidad.

3.2 Prueba de detección de manipulación

Figura 1. A la izquierda se muestran las imágenes originales y a la derecha las marcadas.

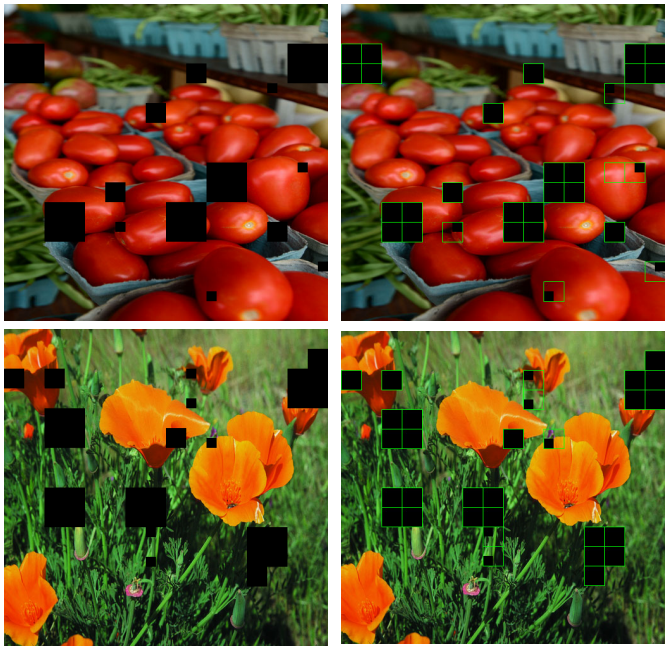


Figura 2. Aplicación y detección del ruido cropping.

Figura 3. Aplicación y detección del ruido gaussiano.

En la Figura 1 se muestran dos imágenes originales tomadas de la base de datos [2] y sus correspondientes imágenes marcadas; mientras que en las Figuras 2 y 3 se aprecia la aplicación de los ruidos cropping y gaussiano, así como su detección por parte del algoritmo propuesto.

4. Conclusiones

En este trabajo se ha presentado un esquema de marca de agua frágil que utiliza una clave privada y una clave pública de 128 bits, así como los momentos ortogonales de Krawtchouk para generar la imagen marcada. De acuerdo con los análisis de los valores de PSNR se mostró que no existen anomalías detectables a simple vista, entre la imagen original y la marcada, alcanzándose un elevado nivel de imperceptibilidad. Además el algoritmo propuesto es capaz de detectar cualquier tipo de manipulación a la imagen marcada, clasificando la fuente emisora en auténtica o no.

Referencias

[1] AEPD. *Introducción al Hash como técnica de seudonimización de datos personales*, European Data Protection Supervisor; Octubre 2019.

[2] ALJARRAH. *RGB-BMP Steganalysis Dataset*. Mendeley Data, v1, http://dx.doi.org/10.17632/sp4g8h7v8k.1, 2018

[3] ANDRADE, A.L. *Características y aplicaciones de las funciones resumen criptográficas en la gestión* DE *contraseñas.* Universidad de Alicante, Tesis de Grado Científico, Doctor en

Ciencias Computacionales, pp. 118, Instituto Universitario de Investigación en Informática, Universidad de Alicante, 2019.

[4] ARTZ, D. *Digital Steganography: Hiding Data within Data,* IEEE Internet Computing Journal, June 2001.

[5] AVILA, E., SORIA**,** A. *Watermarking Based on Krawtchouk Moments for Handwritten*, Progress in Artificial Intelligence and Pattern Recognition, pp.122-129, 2018. DOI https://doi.org/10.1007/978-3-030-01132-1_14.

[6] BARMAK, S. A. Y JAN, F. *Fast computation of Krawtchouk moments*, Inform. Sci, 288, pp. 73-86, 2014

[7] BISWAJITA DATTA, UPASANA MUKHERJEE, KUMAR BANDYOPADHYAY, Samir. *LSB Layer Independent Robust Steganography using Binary Addition*, Procedia Computer Science, 85, pp. 425 – 432, 2016.

[8] BISWASA, D., BISWASB, S., MAJUMDERA, A., SARKARA, D., SINHAA, D., CHOWDHURYA, A., DASA, S. K. *Digital Image Steganography using Dithering Technique*, Procedia Technology, 4, pp. 251–255, 2012.

[9] CHONG, C. Y RAVEENDRAN, P. *On the computational aspects of Zernike moments*. Image and Vision Computing, 25, pp. 967-980, 2007.

[10] ESPAÑA BOQUERA, María Carmen. *Aplicaciones y Servicios de Comunicaciones,* 2003, Disponible en: http://www.google libros/. [Consulta: 6 de junio de 2020].

[11] GUIBERT, Y., CENTURIÓN, A.M., SORIA, A. *Los momentos de krawtchouk y tchebichef y sus aplicaciones en el procesamiento de imágenes digitales*, ROCA, Revista científico- educacional de la provincia Granma, 14(2), pp. 128-136, 2018.

[12] HU, B. Y LIAO, S. *Local Feature Extraction Property of Krawtchouk Moment*, Lecture Notes on Software Engineering, 1, pp. 356-359, 2013.

[13] ORÚE LÓPEZ, Amalia Beatriz*. Marcas de agua en el mundo real,* 2002. Disponible en: https://digital.csic.es/ bitstream/ 10261/8864/ 1/ Marcas_de_agua_en_el_mundo_real.pdf, [Consulta: 6 de junio de 2020].

[14] PÉREZ, Valdemar. *Marca de Agua asimétrica para Imágenes con Propiedades de Traitor Tracing,* Tesis de Grado Científico, Master en Ciencias Computacionales, pp. 97, INAOE, México, 2015.

[15] RAMÍREZ GUTIÉRREZ, Kelsey Alejandra. *Esquemas de Seguridad para Imágenes Digitales*, Cátedra CONACyT- INAOE, 2018, https://ccc.inaoep.mx/~kramirez/Esquemas%20de% 20Seguridad %20para %20 Imagenes%20Digitales.pdf/.

[16] SENA REDDY, M.I., SIVA KUMAR, A.P. *Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm*, Procedia Computer Science, 85, pp. 62 – 69, 2016.

[17] SORIA, A., BERRES, S., AVILA, E. *Hiding data inside images using orthogonal moments*, arXiv:1910.07383v1 [cs.MM] 16 Oct 2019, https://arxiv.org/pdf/1910.07383.pdf.

[18] SORIA, A Y BERRES, S. *A secure steganographic algorithm based on frequency domain for the transmission of hidden information*, Security and Communication Networks, 2017.

[19] SORIA, A., MECÍAS, R., PÉREZ, A. A. & RODRÍGUEZ, D. *Algoritmo esteganográfico pseudo-asimétrico*, Lecturas Matemáticas, 35 (2), pp. 183–196, 2014.

[20] TENGFEI, Y., JIANFENG, M., YINBIN, M., XIMENG, L., XUAN, W., BIN, X., QIAN, M. *Privacy-Preserving Krawtchouk Moment feature extraction over encrypted image data*, Information Sciences, 536, pp. 244-262, 2020, https://doi.org/10.1016/j.ins.2020.05.093.

[21] VARGAS, Laura M., VERA, Elizabeth, DI GIONANTONIO, Alejandra. *Marcas de agua: una contribución a la seguridad de archivos digitales,* Revista Facultad de Ciencias Exactas, Físicas y Naturales, 3(1), pp. 49-54, 2016.

[22] VENKATARAMANA, A., ANANTH, P. *Image Watermarking Using Krawtchouk Moments*, IEEE, 2007, DOI: 10.1109/ICCTA.2007.72.

[23] WANG, G. B. Y WANG, S. G. *Recursive computation of Tchebichef moment and its inverse transform*, Pattern Recognition, 39, pp. 47-56, 2007.

[24] YAP, P., PARAMESRAN, R. Y ONG, S. H. *Image Analysis by Krawtchouk Moments*, IEEE Trans, Image Process, 12, pp. 1367-1377, 2003.

Sobre el/los autor/es:

Nombre: Alicia María Centurión Fajardo
Correo Electrónico: acenturionf@udg.co.cu
Institución: Universidad de Granma, Cuba.

Nombre: Nancy Céspedes Trujillo
Correo Electrónico: nancyct@ult.edu.co.cu
Institución: Universidad de Las Tunas, Cuba.

Nombre: Eduardo Moreno Roque
Correo Electrónico: emorenor@udg.co.cu
Institución: Universidad de Granma, Cuba.