ALMACENAMIENTO EN LA NUBE CON SEGURIDAD ADICIONAL BASADA EN OCULTACIÓN REVERSIBLE DE DATOS

CLOUD STORAGE WITH ADDITIONAL SECURITY BASED ON REVERSIBLE DATA HIDING

Daniela Elizabeth Barrera Martínez
Instituto Politécnico Nacional, México
dbarreram1902@alumno.ipn.mx

Gina Gallegos García
Instituto Politécnico Nacional, México
ggallegosg@ipn.mx

Manuel Cedillo Hernández
Instituto Politécnico Nacional, México
mcedilloh@ipn.mx

Recepción: 30/octubre/2020 **Aceptación:** 4/diciembre/2020

Resumen

Hoy en día los servicios de almacenamiento en la nube son usados de forma masiva. Con fines de protección de la información, se ofrecen niveles de seguridad basados en protocolos de seguridad informática y de la información respectivamente, para hacer frente a diversos tipos de ataques cibernéticos. Ante este escenario, surge la necesidad de desarrollar herramientas tecnológicas que coadyuven con las ya existentes en lo que concierne a la obtención de una protección adicional. En el contexto de imágenes digitales, una de estas herramientas es la técnica de ocultamiento reversible de datos en dominio cifrado, en este sentido, el presente artículo propone un par de estas técnicas que utilizan el cifrado de flujo AES y RC4 como dominios de inserción, este último combinado con mezcla caótica. Los resultados experimentales muestran su efectividad en escenarios reales de operación, garantizando la integridad de datos y al mismo tiempo no interfiere con los protocolos de seguridad de los servicios en la nube.

Palabras Clave: Cifrado de flujo, mezcla caótica, ocultamiento reversible de datos en dominio cifrado, servicios de almacenamiento en la nube.

Abstract

Nowadays cloud storage services are used in a massive way. To protect the information in them and to face different types of cyber-attacks that could violate, and compromise stored data, they offer specific levels of security and information security protocols. In this scenario, there is an urgent need to develop technological tools that contribute to those one already developed and to offer additional protection. In the context of digital images, one of these tools is the reversible data hiding technique in the encrypted domain. In this article two techniques are being proposed that use stream encryption as the insertion domain, one of them combined with chaotic mixing. The experimental results are subject to real operational problems, guaranteeing the integrity of the data and at the same time without interfering with the security protocols used in the cloud services.

Keywords**:** *chaotic mixing, cloud storage services, reversible data hiding in encrypted domain, stream cipher.*

1. Introducción

Actualmente, el uso de diversos servicios en la nube es el común denominador de la gran mayoría de los usuarios de Internet. En ellos, se tiene la capacidad de almacenar o compartir información en diferentes dispositivos al mismo tiempo. Su seguridad, es responsabilidad de los llamados protocolos criptográficos, los cuales dejan abierta la posibilidad de que existan ataques cibernéticos específicos hacia la información y como consecuencia hacia el usuario. El concepto de servicio en la nube engloba un conjunto de aplicaciones y servicios informáticos cuya ley principal característica es que se encuentran alojados en Internet. En estos servicios, el usuario puede acceder instantáneamente y en cualquier momento a sus datos [Celaya, 2017]. Según el Instituto Nacional de Estándares y Tecnologías (NIST), la computación en la nube es un modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios [NIST, 2020]. De acuerdo con el Manual de Cifrado en la Nube [McAfee, 2018], el cifrado hace que la información sea inteligible

para cualquier persona sin conocimiento de las claves de cifrado. Pero cuando un proveedor de la nube cifra la información, los administradores del proveedor pueden ver dicha información. Según los artículos del Capítulo único de las obligaciones en materia de seguridad y justicia del Título octavo de la colaboración de la justicia de la Ley federal de telecomunicaciones [Ley federal de telecomunicaciones, 2014] y la sección 1 de la solicitud del capítulo ll de las intervenciones de comunicaciones de la Ley de Seguridad Nacional de México [Ley de Seguridad Nacional, 2005] se puede obligar al proveedor de la nube a proporcionar copias de su información a varios gobiernos de todo el mundo, sin notificarlo. En caso de incumplimiento, un ciberdelincuente que haya comprometido las claves de cifrado de un proveedor de la nube puede descifrar la información robada. Según el Informe sobre Adopción y Riesgos en la Nube: Trabajando desde Casa de McAfee [McAfee, 2020], que realizó un análisis de actividad durante enero y abril del 2020, la adopción de servicios en la nube ha aumentado un 50 %, el uso de herramientas de colaboración en la nube se disparó un 600 %, liderado por el sector educativo. Adicionalmente a eso, cabe destacar que, en la mayoría de las industrias, la organización promedio carga 13.9 TB de información a la nube, de la cual casi una cuarta parte puede clasificarse como confidencial, lo que compromete a las empresas o personas en caso de robo o divulgación de la información. De hecho, según McAfee, los datos confidenciales se están trasladando a la nube a una velocidad sin precedentes y las organizaciones están buscando formas de extender los controles de la política de cifrado a los nuevos sistemas de registro y sistemas de interacción basados en la nube. En este sentido, el 81.8% de los proveedores de la nube cifran datos en tránsito a través de protocolos criptográficos de tipo SSL o TLS y el 9.4% almacenan información cifrada [McAfee, 2018]. Debido a este gran aumento de actividad en los servicios en la nube, los ataques han aumentado un 630%, principalmente las amenazas dirigidas a plataformas de colaboración como Microsoft 365, con intentos a gran escala, de acceder a los servicios en la nube a través de credenciales robadas. Esto, junto con el hecho de que el intercambio de información confidencial en la nube aumenta un 53% cada año, hace que aquellos que no adopten una estrategia que incluya la protección de pérdida de información, auditorías de configuración y controles de

colaboración, pongan en peligro su seguridad. Lo anterior, deja abierta la posibilidad del uso de programas maliciosos (*malware*) como lo es *ransomware* o inclusive piezas de software encargadas de grabar las credenciales introducidas a través de un teclado (*keylogger*). O también dando oportunidad a ataques de suplantación de identidad (*phishing*), falsificación de solicitudes (*cross site request forgery*) y secuencia de comandos (*cross site scripting*). Esto, por ejemplo, a través del abuso de APIs (*Application Programming Interface*). Por medio de dichos ataques, la información personal del usuario puede ser utilizada para el uso de técnicas de generación de inteligencia de fuentes abiertas, en las cuales es posible obtener una recopilación de información que pudiese generar conflictos importantes, como la suplantación de identidad. Algunos de estos ataques pueden ser imperceptibles a la víctima, de modo que su detección podría tardar tiempo. Según apunta Ángel Ortiz, director regional de McAfee en España, mitigar los riesgos que suponen los agentes maliciosos dirigiendo sus ataques a la nube y los asociados a otros vectores de pérdida de información, requieren soluciones con controles de visibilidad y seguridad en todos los servicios en la nube. Este problema puede ser resuelto con la aplicación de la técnica de Ocultación Reversible de Datos (*Reversible Data Hiding* - RDH) [Qi, 2018], [García, 2018], [Shi, 2016], [Fridrich, 2001], [Fridrich, 2002], [Celik, 2005], [Xu, 2016], mediante la cual, se puede incrustar datos en un medio de cobertura, para posteriormente permitir que el usuario autorizado extraiga los datos incrustados del medio marcado. La principal característica de esta técnica es que el medio de cobertura también se puede recuperar sin pérdidas. Es decir, realiza un proceso que no interfiere con los protocolos criptográficos que aseguran la información en los servicios de la nube. Esta propuesta destaca por la aplicación de dicha técnica a los medios multimedia almacenados, específicamente en imágenes digitales, de modo que el medio sea la entrada del proceso para posteriormente procesarla y después cifrada, de forma tal que para la recuperación de la imagen original, dependerá de la o las claves que el emisor ofrezca al receptor, donde se presentarán tres casos posibles: extraer únicamente los datos insertados, descifrar la imagen preservando los datos ocultos o recuperar ambas cosas, los datos ocultos y la imagen original. En este sentido, en el año 2016 Yun-Qing Shi et

al. en [Shi, 2016] presentan y discuten la historia de los desarrollos técnicos, el estado del arte actual y las posibles investigaciones futuras sobre la tecnología RDH, mostrando una clasificación de seis categorías 1) RDH en el dominio espacial de la imagen; 2) RDH en dominio comprimido de imagen (por ejemplo, JPEG); 3) RDH adecuado para autenticación de imagen semi-frágil; 4) RDH con mejora de contraste de imagen; 5) RDH en imágenes cifradas, que se espera, tenga una amplia aplicación en la computación en la nube; y 6) RDH en video y audio. Finalmente, en el año 2018, Qi Li Bin Yan et al. [Qi, 2018] propusieron un algoritmo de ocultamiento reversible de datos para proteger la privacidad en algunos entornos abiertos, en dominio cifrado basado en una permutación de bloque combinada y cifrado de flujo en el paso de cifrado y aumento de la tasa de inserción al proponer el reemplazo de bits en el error de predicción. Por otra parte, García Olivares et al. [García, 2018] propusieron un esquema de ocultamiento reversible de datos en dominio cifrado, basado en la modificación del histograma de una imagen digital en el dominio cifrado, compuesto de dos etapas para ocultar datos de manera reversible y dos etapas de cifrado de imágenes digitales. Las etapas de ocultamiento de datos consisten en un método de desplazamiento del histograma, así como una técnica de permutación de los bits del histograma, ambas para la inserción de bits respectivamente. Por otro lado, los procesos de cifrado se basan en mezclas caóticas, así como cifrado de bloque principalmente. Considerando los aspectos mencionados con anterioridad, este artículo tiene como objetivo principal implementar dos métodos basados en el ocultamiento reversible de datos en dominio cifrado de la imagen, que coadyuven con las herramientas tecnológicas ya existentes para incrementar la seguridad de la información en servicios de almacenamiento en la nube de imágenes digitales. El primer algoritmo considera en su diseño la técnica de mezcla caótica en conjunto con el cifrado de flujo RC4, mientras que el segundo algoritmo considera el cifrado de bloque AES en modo OFB, ambos realizan el ocultamiento de datos por sustitución de bit menos significativo en los criptogramas de las imágenes antes de que estas sean almacenadas en el servicio en la nube. Los detalles de ambas propuestas se explican más adelante.

2. Métodos

En esta Sección se presentan los detalles de cada uno de los procesos que componen la propuesta de solución. En el contexto de las imágenes digitales, la ocultación reversible de datos (RDH), permite al usuario la incrustación datos en un medio, donde solo el usuario autorizado extrae la información sin pérdidas. Esta técnica considera tres entidades primordiales en su proceso, la primera es el propietario del contenido quien cifra, elige la clave de cifrado y realiza un preprocesamiento a la imagen. La segunda entidad es el ocultador de datos, quien incrusta los bits adicionales al medio y usa la clave de ocultación para la seguridad. Finalmente, la tercera entidad es el receptor, quien tiene la opción de descifrar, extraer los datos o generar un medio recuperado. En algunos escenarios de aplicación, un asistente inferior o un administrador de canales puede añadir algún mensaje adicional, como la información de origen, la notación de la imagen o los datos de autenticación. Dentro de los medios cifrados, aunque no conoce el contenido original, el método apunta a incrustar información adicional en datos cifrados sin revelar el contenido de texto plano y recuperar el contenido original de texto plano sin errores de lado del receptor.

Cifrado de flujo

Dentro del ámbito de la criptografía de llave simétrica que complementa la técnica de RDH, es común utilizar un algoritmo de cifrado de flujo, el cual se encarga de operar bit a bit con una función booleana OR-exclusiva. Sin embargo, es bien sabido que es posible configurar un algoritmo de cifrado de bloque para que funcione como un cifrador de flujo. Esto, vía los modos de operación, tal es el caso del modo de operación OFB (*Output Feedback*), con el cual se obtiene un comportamiento similar al que tienen los algoritmos de cifrado de flujo. Uno de los algoritmos de cifrado de flujo posible para este escenario es el RC4 [Goutam, 2011], diseñado por Ron Rivest para RSA security en 1987. El proceso de cifrado/descifrado es muy rápido ya que utiliza la función booleana OR-exclusiva bit a bit entre el texto plano/texto cifrado y una secuencia cifrante cuyos bits van cambiando dinámicamente. Su proceso consiste en 3 partes: *Key-Scheduling Algorithm* (KSA), *Pseudo-Random Generation*

Algorithm (PRGA) y el cifrado/descifrado, el cual, en términos generales se puede definir por las ecuaciones 1, 2 y 3.

$$\sigma_{i+1} = f(\sigma_i, k) \tag{1}$$

$$z_i = g(\sigma_i, k) \tag{2}$$

$$c_i = h(z_i, m_i) \tag{3}$$

Donde σ_i es el estado inicial que puede determinarse a partir de la llave simétrica k, que acuerdan emisor y receptor, f es la función del siguiente estado y g es la función que produce la secuencia cifrante z_i, h es la función de salida que se combina, a través de la función booleana OR-exclusiva, con el texto plano m_i para producir el texto cifrado c_i. El algoritmo de bloque más utilizado a nivel mundial es el Rijndael, contenido en el Estándar de Cifrado Avanzado (*Advanced Encryption Standard* - AES) [FIPS PUBS, 2001], no es de tipo Feistel, procesa bloques completos de texto plano de 128 bits con posibles claves de 128, 192 o 256 bits, las cuales definen la cantidad de rondas que ejecutará el algoritmo de la siguiente forma:

- Para una clave de 128 bits, el algoritmo realizará 10 vueltas.
- Si la clave es de 192 bits serán 12 vueltas.
- Para una clave de 256 bits, el proceso de cifrado ejecutará 14 vueltas.

En cada una de estas vueltas, se usará una clave distinta generada a partir de la clave simétrica. Usa matrices de estado de tamaño 4x4 y cada celda de la matriz contiene un byte, definido por la ecuación 4.

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \quad + b_0 = \sum_{i=0}^{7} b_i x^i \tag{4}$$

De tal forma que este algoritmo de bloque forma un cuerpo algebraico definido en el campo de Galois *GF*(2^8).

Los 16 bytes de la matriz de estado van cambiando de valor de acuerdo con las funciones de cifrado/descifrado que ejecuta el algoritmo en el siguiente orden: *AddRoundKey, SubBytes/InversoSubBytes, ShiftRows/InversoShift Rows, MixColumns/InversoMixColumns.*

Mezcla caótica

En lo que respecta al procesamiento de la imagen, la mezcla caótica, se define como una técnica de cifrado que tiene la capacidad de producir una imagen digital totalmente ilegible. Es decir, la imagen mezclada o permutada no tiene ningún sentido o significado ante el sistema visual humano. Además, mantiene intactos los valores de las intensidades de cada píxel [Voyatzis, 1997]. En términos generales, el método de mezcla caótica viene dado por la ecuación 5.

$$I^{(i)} = A_N^i(k)I^{(0)}, \quad i = 1,2,\dots,P-1 \tag{5}$$

Donde $I^{(i)}$ es la iteración i-ésima que produce la imagen mixta, $I^{(0)}$ es la imagen original, P es el número de iteraciones y ${A_N}^{(k)}$ mapeo dado por la ecuación 6.

$$A_N(k) = L_N \to L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \tag{6}$$

Donde L_N es un índice bidimensional establecido en el rango $[1, N]$, N es el tamaño de $I^{(0)}$, $(x_n, y_n) \in L_N$ y $k \in [1, N] \subset \mathrm{Z}$.

El procedimiento inverso de la mezcla caótica viene dado por la ecuación 7.

$$I^{(0)} = B_N^i(k)I^{(i)}, \quad i = 1,2,\dots P-1 \tag{7}$$

Donde B viene dado por la ecuación 8.

$$B_N(k) = L_N \to L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} k+1 & -1 \\ -k & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \tag{8}$$

Propuesta solución basada en mezcla caótica, cifrado RC4 y sustitución LSB

Se propone el uso de la técnica básica de ocultación reversible de datos a la seguridad en el escenario del servicio en la nube, basado en dominio cifrado con sustitución de bit menos significativo (LSB), permutación de píxeles vía mezcla caótica y cifrado de flujo RC4, mismo que puede ser aclarado gráficamente en la figura 1. El proceso de aplicación consiste en la entrada de una imagen en blanco y negro con dimensiones de 512 X 512 para leer su contenedor de datos comprimidos y así afianzar la capacidad de hacer reversible los datos, ya que no se realiza un cambio en su estructura. Una vez ingresada la imagen se emplea el algoritmo de mezcla caótica generando la llave de iteraciones $(K1)$ y la de aplicación de la técnica $(K2)$. Una vez obtenida la imagen con mezcla caótica, ya considerada ilegible, se

procede al cifrado de flujo RC4 aplicado píxel por píxel, en la que se define la llave de cifrado – descifrado $(K1)$, ofreciendo la imagen cifrada. La imagen cifrada es procesada por el ocultador de datos, donde se crea la llave de ocultamiento de datos; este proceso se realiza mediante la sustitución de LSB de la imagen. Una vez aplicados los tres procesos se crea un criptograma con datos ocultos disponible para su almacenamiento en la nube.

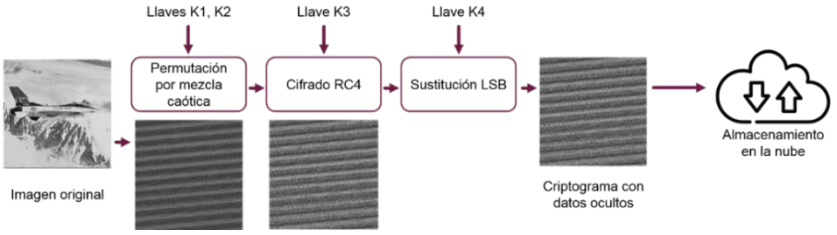


Figura 1 Esquema general de ocultamiento reversible de datos en dominio cifrado RC4.

De acuerdo con las características de la técnica, para la recuperación de la imagen original dependerá de las llaves que el emisor le ofrezca al receptor, como se muestra en la figura 2, donde se presentarán tres posibles casos: el primero es si el emisor le ofrece al receptor la llave de ocultamiento de datos $(K4)$ que únicamente le permitirá la extracción de los datos incrustados.

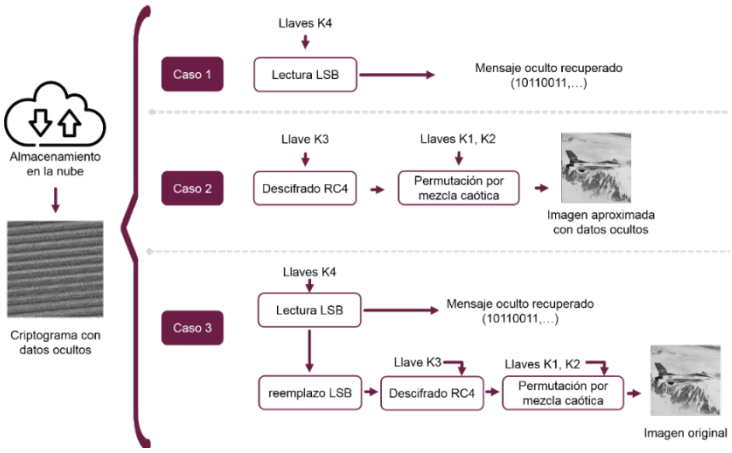
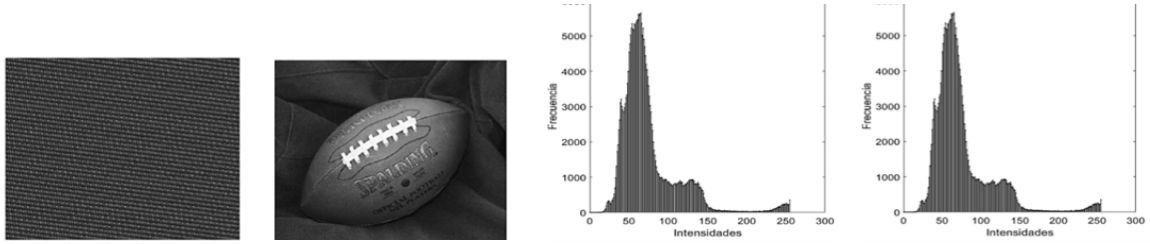


Figura 2 Descarga-recuperación de información en el esquema RDH-ED con RC4.

El segundo caso, es cuando el emisor ofrece las llaves de número de iteraciones usado por el algoritmo de mezcla caótica $(K1)$, la llave del algoritmo de mezcla

caótica (K) y la llave de cifrado – descifrado del algoritmo RC4 $(K3)$ con las que podrá descifrar la imagen preservando los datos ocultos, es decir, obtiene un medio aproximado al original. Finalmente, el último caso es cuando se ofrece al receptor todas las llaves $(K1, K2, K3, K4)$ permitiendo recuperar la imagen original y los datos ocultos. La aplicación de la técnica de mezcla caótica ofrece la capacidad de producir una imagen totalmente ilegible al realizar una permutación de los valores de la imagen como se muestra en figura 3a comparado con figura 3b, sin alterar sus valores de intensidad como se muestra en figuras 3c y 3d.



a) Mezcla imagen original. b) Imagen inicial. c) histograma de imagen original. d) Histograma de mezcla

Figura 3 Aplicación de técnica de técnica de mezcla caótica.

La aplicación en una imagen del cifrador RC4 provisto en este posible caso, genera un ligero cambio en ella, sin embargo, ésta continúa siendo visible a la percepción humana como se puede observar en figura 4a en contraste con la imagen original mostrada en figura 4b.

a) Imagen Cifrada con RC4). b) Imagen Original

Figura 4 Aplicación de técnica de cifrado RC4 a imagen.

Dado que la aplicación del cifrado RC4 a la imagen mantiene visible los detalles del contenido, es necesario aplicar la técnica de mezcla caótica previo al cifrado, para

obtener un criptograma completamente ilegible a la visión humana. De este modo, la combinación de ambos procedimientos generaría un resultado más favorable como se puede observar en figura 5b, comparada con figura 5a que muestra la aplicación única del cifrado.

a) Imagen cifrada con RC4 sin mezcla caótica. *b) Imagen cifrada con RC4 con mezcla caótica.*

Figura 5 Combinación de técnicas de mezcla caótica y cifrado RC4.

Propuesta solución basada en cifrado de bloque AES modo OFB y sustitución LSB

La segunda propuesta está basada en dominio cifrado con cifrado AES en modo OFB y sustitución de bit menos significativo (LSB), figura 6.

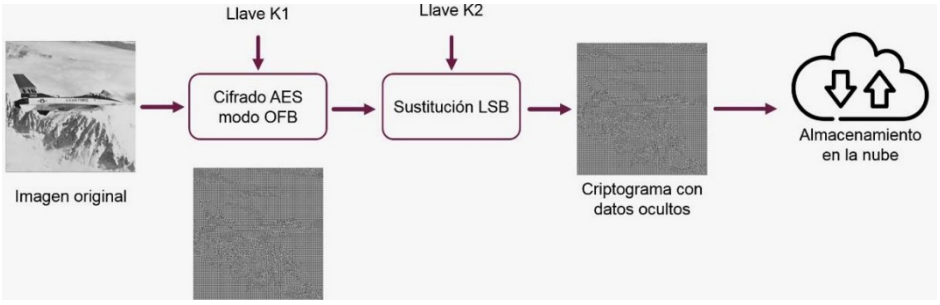


Figura 6 Esquema general de ocultamiento reversible de datos en dominio cifrado AES.

La aplicación de esta propuesta también está basada en las mismas características para la imagen de la propuesta anterior. Esta imagen es cifrada a través del algoritmo AES modo OFB donde es generada la llave de cifrado – descifrado $(K1)$, generando así la imagen cifrada. Esta imagen entra al proceso de ocultación de datos donde se obtiene llave de ocultamiento de datos $(K2)$ a través del proceso de sustitución de LSB generando el criptograma con datos ocultos disponible para su almacenamiento en la nube.

De igual manera y recordando el proceso de recuperación de la imagen original se presentarán los mismos tres casos posibles como se muestra en la figura 7: el primero es si el emisor le ofrece al receptor la llave de ocultamiento de datos $(K2)$ donde únicamente se le permitirá la extracción de los datos incrustados. El segundo caso, es cuando se ofrece al receptor la llave de cifrado – descifrado del algoritmo AES $(K1)$ con la que se obtiene el medio aproximado al original. Finalmente, el último caso es cuando se ofrecen al receptor ambas llaves $(K1, K2)$ que le permitirán recuperar la imagen original y los datos ocultos en la misma.

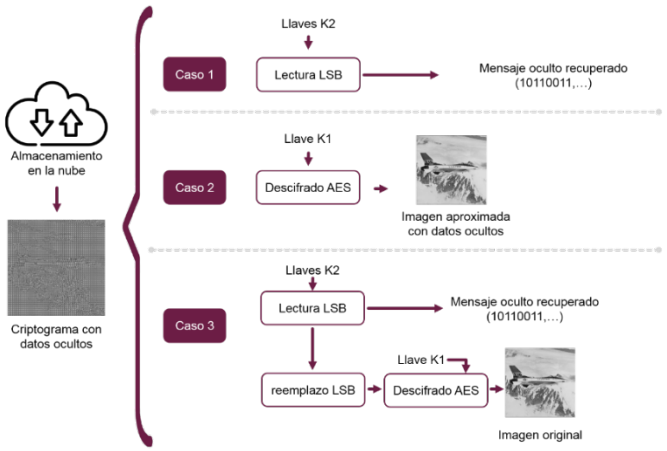
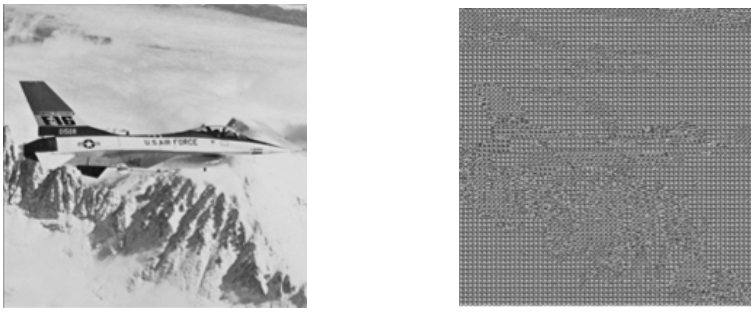


Figura 7 Descarga-recuperación de información RDH – AES.

La aplicación del cifrado AES en modo OFB en la imagen original mostrada en figura 8a, genera un cambio significativo al convertirla ilegible a la percepción humana como se observa en figura 8b de la misma figura.



a) Imagen original. *b)Imagen cifrada con AES.*

Figura 8 Aplicación de técnica de cifrado AES a imagen.

Para el proceso de ocultamiento de datos en ambas propuestas, se plantea su realización por medio de la técnica de modificación del LSB (*Least Significant Bit* por sus siglas en inglés), usando imágenes digitales con 8 bits/píxel de resolución como señal huésped del mensaje a ocultar. La figura 9 ilustra el proceso de sustitución LSB en dominio cifrado, así como los 3 casos que se pueden llevar a cabo dependiendo de las llaves que posea la entidad receptora.

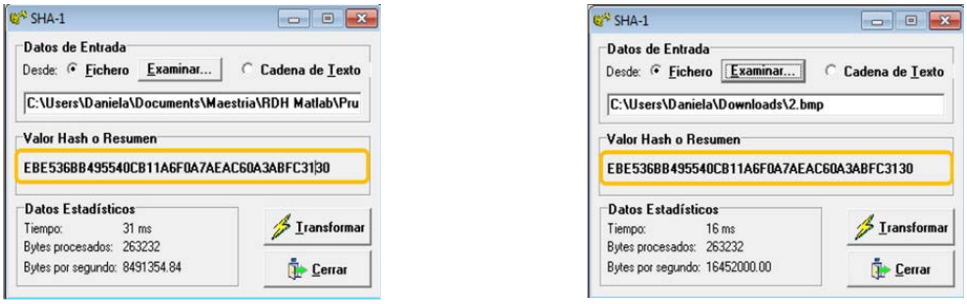
Figura 9 Ejemplo de modificación del LSB.

3. Resultados

En esta sección se presentan los resultados experimentales del método de RDH-ED propuesto en este artículo, desde un punto de vista de imperceptibilidad y capacidad de ocultamiento de datos respectivamente, así como la prueba de integridad de los datos almacenados en los servicios en la nube.

Integridad de datos en la nube

Se realizó una prueba básica de integridad en imágenes almacenadas en el servicio de nube conocido como OneDrive [Microsoft, 2020], a través de la aplicación CriptoRes [CriptoRES, 2020], donde se obtuvo el valor hash de la imagen antes y después de ser almacenada. Esta prueba permite confirmar con precisión que los datos almacenados son los mismos que los datos extraídos, es decir, ofrece la posibilidad de identificar cualquier manipulación en el medio ante algún cambio en el valor obtenido. En este caso, se obtuvo el valor hash del archivo original, como se observa en figura 10a, y posteriormente el valor después del almacenamiento, donde se puede apreciar que el segundo valor es igual al original, como se observa en figura 10b.



a) Valor hash de imagen original. *b) Valor hash de imagen almacenada en OneDrive.*

Figura 10 Prueba básica de integridad de datos en la nube.

Este proceso es aplicable a todo archivo digitalizado y tiene utilidad para garantizar la integridad de los datos, ya que no se pueden encontrar dos valores hash iguales, a no ser, que el segundo archivo sea completamente idéntico al primero. De este modo, se considera que no existe una alteración en el archivo.

Imperceptibilidad

La figura 11 se muestra los efectos de distorsión visual una vez que el receptor descifra la imagen directamente usando la llave de descifrado correspondiente, cuando el cifrado es de tipo RC4. La figura 12 muestra los resultados cuantitativos de la figura 11 en términos de relación señal ruido pico (PSNR) [Wang, 2004]. Por su parte, la figura 13 muestra los efectos de distorsión visual una vez que el receptor descifra la imagen directamente usando la llave de descifrado correspondiente, cuando el cifrado es de tipo AES modo OFB. La figura 14 muestra los resultados cuantitativos de la figura 13 en términos de relación señal ruido pico (PSNR).

Figura 11 Distorsión visual con diferentes planos de inserción usando cifrado RC4.

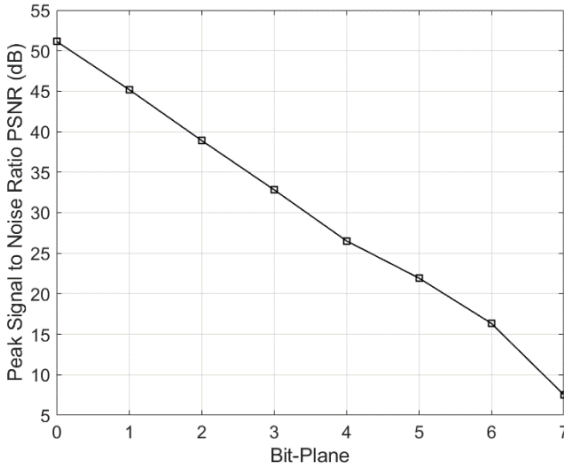


Figura 12 PSNR para diferentes planos de inserción usando cifrado RC4.

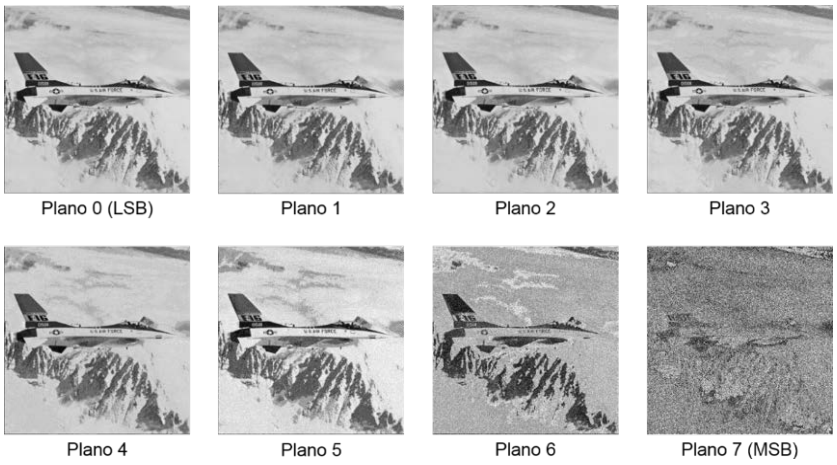


Figura 13 Distorsión visual en diferentes planos de inserción usando AES modo OFB.

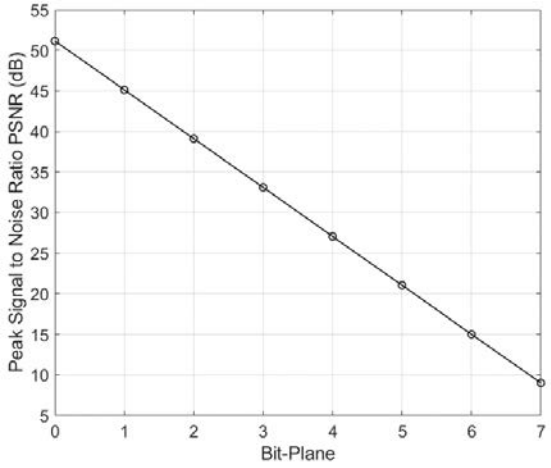


Figura 14 PSNR para diferentes planos de inserción con cifrado AES modo OFB.

De las figuras 11, 12, 13 y 14 se observa que en ambos cifrados (RC4 y AES modo OFB) la inserción llevaba a cabo en los primeros 3 planos (Plano 0, 1 y 2) no afecta demasiado la calidad visual de la imagen descifrada que contiene información oculta en ella, obteniendo en ambos casos valores de PSNR superiores a 38 dB. Por otra parte, si el ocultamiento de datos se lleva a cabo a partir del plano 3, la calidad de la imagen descifrada disminuye de manera considerable, obteniendo valores PSNR menores a 33 dB.

Capacidad de ocultamiento de datos

Derivado de los resultados de imperceptibilidad presentados en la sección anterior, en la figura 15 se muestran los resultados de capacidad de ocultamiento de datos con tasas que van desde los 0.1 bits por píxel (bpp) hasta 1 bpp.

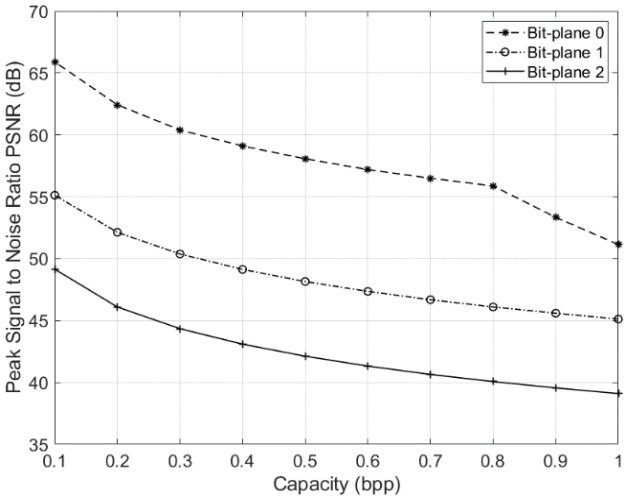


Figura 15 Capacidad de ocultamiento de datos con diferentes tasas de inserción.

De la figura 15 se observa que usando el cifrado RC4 o bien AES modo OFB, el plano-0 LSB obtiene los mejores resultados de imperceptibilidad, obteniendo valores PSNR que van desde los 66 dB hasta los 52 dB cuando la tasa de inserción va desde 0.1 hasta 1 bpp respectivamente. Si se desea usar el plano 1 para ocultar la información dentro de la imagen, los valores PSNR decrecen de 55 dB hasta los 45 dB para tasas desde 0.1 hasta 1 bpp respectivamente. Por último, si se ocupa el plano 2 para ocultar datos, los valores PSNR correspondientes van desde los 49 dB

hasta los 39 dB para tasas de 0.1 a 1 bpp. Este comportamiento es interesante ya que para incrementar la seguridad del esquema ante tareas de estegoanálisis, la información puede ocultarse de manera permutada entre estos tres planos de bits, sin afectar la calidad visual de la imagen que contiene la información oculta.

Comparativa de rendimiento

En esta sección se lleva a cabo un comparativo de rendimiento con las propuestas reportadas en [Qi, 2018] y [Xu, 2016] respectivamente, en términos de PSNR entre imagen original y cifrada, tasas máximas de ocultamiento de datos y tiempos de ejecución de los diferentes procesos que componen un esquema RDH-ED. Para una comparación equitativa, los algoritmos fueron implementados usando Matlab 2013b ©. La figura 16 muestra las imágenes de prueba empleadas para llevar acabo el comparativo de esta sección.

En la tabla 1 se presenta un comparativo en términos de PSNR entre la imagen original y su versión cifrada.

a) Lena *b) Boat* *c) Man* *d) Peppers* *e) Baboon*

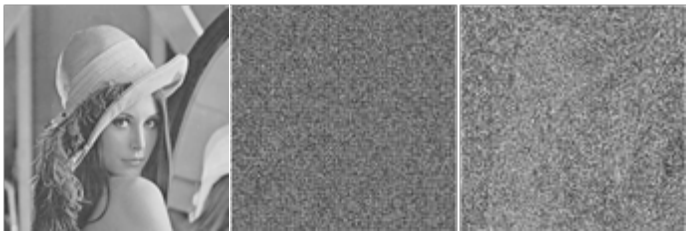
Figura 16 Imágenes de prueba.

Tabla 1 Comparativa de PSNR entre la imagen original y cifrada.

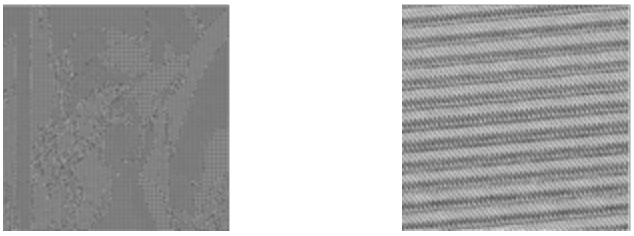
Imagen	Método en [Qi, 2018]	Método en [Xu, 2016]	Método Propuesto RC4-Mezcla Caótica	Método Propuesto AES modo OFB
Lena	8.50 dB	8.21 dB	8.23 dB	9.27 dB
Boat	7.19 dB	7.59 dB	8.38 dB	8.79 dB
Man	8.25 dB	8.66 dB	8.00 dB	8.13 dB
Peppers	7.28 dB	7.48 dB	7.76 dB	8.40 dB
Baboon	8.01 dB	9.00 dB	7.87 dB	9.27 dB

Como se puede observar, todos los métodos en la tabla 1 presentan un valor de PSNR por debajo de los 10dB, esto indica que la versión cifrada de la imagen no

contiene detalles visibles de la versión original, como se muestra en la figura 17, donde se muestra el resultado de aplicar el cifrado a la imagen Lena. Como se puede observar, los métodos que se proponen en este artículo son competitivos con lo reportado previamente en la literatura científica.



a) Original *b) [Qi, 2018]* *c) [Xu, 2016]*



d) Método AES modo OFB *e) Método RC4-Mezcla Caótica*

Figura 17 Imágenes cifradas de Lena.

En la tabla 2 se presenta una comparativa de tasas de ocultamiento de datos máximas representadas en bits por píxel (bpp). Como se puede observar, los métodos propuestos en este artículo son superiores obteniendo ambos la capacidad de ocultar 1 bpp, mientras que el método de [Qi, 2018] logra tasas de 0.5 bpp y el método de [Xu, 2016] alcanza una tasa máxima de 0.25 bpp. Finalmente, la tabla 3 muestra una comparativa de tiempos de ejecución promedio (segundos) de las etapas de cifrado de imagen, inserción de datos, descifrado de imagen con datos ocultos en ella, y extracción de datos con descifrado de imagen.

Tabla 2 Comparativa de tasas de ocultamiento de datos máximas (bits por píxel bpp).

Imagen	**Método en [Qi Li, 2018]**	**Método en [Xu, 2016]**	**Método Propuesto RC4-Mezcla Caótica**	**Método Propuesto AES modo OFB**
Lena	0.5 bpp	0.25 bpp	1 bpp	1 bpp
Boat	0.5 bpp	0.25 bpp	1 bpp	1 bpp
Man	0.5 bpp	0.20 bpp	1 bpp	1 bpp
Peppers	0.5 bpp	0.25 bpp	1 bpp	1 bpp
Baboon	0.5 bpp	0.10 bpp	1 bpp	1 bpp

Tabla 3 Comparativa de tiempos de ejecución promedio (segundos).

Método	Cifrado de Imagen	Inserción de Datos	Descifrado con datos ocultos	Extracción de datos y descifrado de imagen
[Qi, 2018]	1.53 s	0.14 s	1.6 s	1.73 s
[Xu, 2016]	0.81 s	0.48 s	0.9 s	1.37 s
AES(OFB)	5.68 s	1.39 s	5.74 s	6.9 s

Como se puede observar en la tabla 3, el método propuesto en este artículo que esta basado en cifrado AES modo OFB tiene tiempos de ejecución para cifrar y descifrar una imagen digital mayores a 5.6 segundos, y para ocultamiento de datos tiene tiempos superiores a 1.3 segundos. Es claro que nuestro método es superado en tiempos de ejecución por las propuestas reportadas en [Xu, 2016] y [Qi, 2018], por tal motivo, consideramos como trabajo futuro mejorar los tiempos de ejecución migrando el código hacia algún lenguaje de programación que ofrezca mejor rendimiento, como por ejemplo el lenguaje C o bien C++.

4. Discusión

Como se puede observar en la sección de resultados experimentales, el proceso de ocultamiento reversible de datos en dominio cifrado (Reversible Data Hiding in Encrypted Domain RDH-ED) no se ve alterado en su funcionamiento por los esquemas de seguridad implementados en los servicios de almacenamiento en la nube. Esto permite que las imágenes que son procesadas por la propuesta RDH-ED presentada en este artículo, posean un nivel adicional de seguridad dado que el dominio cifrado llevado a cabo ya sea por la combinación de los algoritmos RC4-Mezcla Caótica o bien AES modo OFB, permiten un nivel de confidencialidad y seguridad adicional aún si la imagen llegase a ser descifrada o intervenida por terceras partes dentro del propio servicio de almacenamiento en la nube. Otra característica interesante que permite la propuesta RDH-ED es ocultar información en imágenes cifradas, este aspecto es relevante ya que por medio de diferentes llaves que posean las entidades autorizadas se podrá descifrar la imagen sin tener acceso a los datos ocultos en ella, extraer los datos ocultos sin poder revelar el contenido de la imagen que los contiene, o bien realizar ambas tareas. Los

resultados experimentales de las pruebas de integridad en conjunto con las pruebas de imperceptibilidad y capacidad de almacenamiento permiten que se puedan crear diversas configuraciones dependiendo de las necesidades que requiera la aplicación en cuestión. Es decir, es posible ajustar la cantidad de bits a almacenar dentro de la imagen, así como la selección del plano de bits y el tipo de cifrado de flujo para obtener un desempeño requerido de la aplicación.

5. Conclusiones

Actualmente el uso masivo de los servicios de almacenamiento en la nube continúa creciendo de forma exponencial, por lo que, para proteger la información almacenada por los usuarios, las infraestructuras de tecnologías de la información ofrecen diversos niveles de protección basados en protocolos de seguridad informática y de la información respectivamente con la finalidad de mitigar posibles amenazas y ataques cibernéticos que pueden vulnerar y comprometer los datos almacenados. Ante este escenario, surge la necesidad de desarrollar herramientas tecnológicas que coadyuven con las ya existentes para ofrecer protección adicional a los archivos multimedia almacenados. En un contexto de imágenes digitales, en este artículo se proponen dos técnicas de ocultamiento reversible de datos en dominio cifrado, que utilizan los cifrados de flujo RC4 y AES modo OFB como dominios de inserción de datos en conjunto con la técnica de sustitución de bits en imágenes digitales. Los resultados experimentales muestran el rendimiento de ambas propuestas en términos de imperceptibilidad y capacidad de almacenamiento de datos que pueden contener las imágenes digitales en sus diferentes planos de bits, concluyendo que los primeros tres planos ofrecen el mejor rendimiento. Sin embargo, para garantizar la confidencialidad de los datos, el cifrado RC4 necesita un proceso adicional de mezcla caótica que agrega una complejidad computacional adicional a dicha propuesta, hecho que la pone en desventaja con la que se basa únicamente en cifrado AES modo OFB. Para ambas propuestas, la recuperación de datos ocultos, así como de la imagen original dependerá de la o las llaves que la entidad receptora posea, en este sentido se pueden realizar las siguientes tareas: a) Extraer únicamente los datos ocultos, b) Descifrar la imagen

preservando los datos ocultos en ella, o c) Extraer los datos ocultos y recuperar la imagen original. Se demostró la efectividad de estos esquemas RDH-ED en escenarios reales de operación en el servicio OneDrive, garantizando la integridad de datos y al mismo tiempo no interfiriendo con los protocolos de seguridad de los servicios en la nube.

6. Bibliografía y Referencias

[1] Celaya Luna, Cloud: Herramientas para Trabajar en la Nube, España: ICB Editores, 2017.

[2] Celik Mehmet Utku, Sharma Gaurav, Murat Tekalp Ahmet, Saber Eli. Lossless generalized-LSB data embedding, IEEE Transactions on Image Processing, 14(2), pp. 253–266. Febrero 2005.

[3] CriptoRES: hash MD5 y SHA-1. http://www.criptored.upm.es/software/sw_m001h.htm Consultado en mayo 2020.

[4] Federal Information - Processing Standards Publications (FIPS PUBS). Announcing the Advanced Encryption Standard (AES), November 2001.

[5] Fridrich, J., Goljan, M. and Du, R. Invertible Authentication, Security and Watermarking of Multimedia Contents III, 4314, pp. 197–208. August 2001.

[6] Fridrich, J., Goljan, M. and Du, R. Lossless data embedding-new paradigm in digital watermarking, Eurasip Journal on Applied Signal Processing, pp. 185–196. febrero 2002.

[7] García Olivares D., Cedillo Hernández M. Ocultamiento reversible de datos en el dominio cifrado de imágenes digitales. ICMEAE, Julio 2018.

[8] Goutam Paul, Subhamoy Maitra. RC4 Stream Cipher and Its Variants, November 2011.

[9] Jiménez Javier. ¿Copias de seguridad contra el ransomware? Redes Zone. marzo 2020.

[10] Ley Federal de Telecomunicaciones. Título octavo de la colaboración de la justicia, Capítulo único de las obligaciones en materia de seguridad y justicia. Diario Oficial de la Federación de los Estados Unidos Mexicanos, 14 de julio de 2014.

[11] Ley de Seguridad Nacional. Capítulo ll de las intervenciones de comunicaciones, Sección 1 de la solicitud. Diario Oficial de la Federación de los Estados Unidos Mexicanos, 31 de enero de 2005.

[12] McAfee. Cloud Adoption and Risk Report. 2019.

[13] McAfee. The Cloud Encryption Handbook: Encryption Schemes and Their Relative Strengths and Weaknesses. Abril, 2018.

[14] Menezes Alfred J., Van Oorschot Paul C., Vanstone Scott A. Handbook of Applied Cryptography. Octubre, 1996. CRC Press.

[15] Microsoft OneDrive: https://www.microsoft.com/es-mx/microsoft-365/onedrive/online-cloud-storage Consultado en junio 2020.

[16] Morris Dworkin (NIST). Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Diciembre 2001.

[17] NIST. (22 de junio de 2020). Computer Security Resource. Recuperado el 20 de septiembre de 2020, Information Technology Laboratory Center: https://csrc.nist.gov/Projects/Cloud-Computing

[18] Qi Li Bin Yan, Hui Li Na Chen. Separable reversible data hiding in encrypted images with improved security and capacity. Multimedia Tools and applications. Junio 2018.

[19] Shi Yun-Qing, Li Xiaolong, Zhang Xinpeng, Wu Hao-Tian, Ma Bin. Reversible data hiding: Advances in the past two decades. Julio 2016. IEEE Access. IEEE, 4, pp. 3210–3237.

[20] Seguridad y privacidad en Google Cloud. https://support.google.com/googlecloud/answer/6056693?hl=es#. Consultado mayo 2020.

[21] Voyatzis G., Pitas I., Embedding Robust Watermarks by Chaotic Mixing. Julio 1997, Proc. of Conf. Int. Digital Signal Processing. Vol. 1. pp. 213-216.

[22] VpnMentor. https://es.vpnmentor.com/. Consultado en junio 2020.

[23] Wang Zhou, Bovik Alan C., et al. Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing, 13(4), pp. 600–612. Abril 2004.

[24] Xu D.W., Wang R.D. Separable and error-free reversible data hiding in encrypted images. Signal Processing, vol. 123, pp. 9–21, 2016.