# Esteganografía por sustitución múltiple, Implementación en Matlab.

Mg. Ing. Guillermo Sergio Navas[1]
Mg. Ing. Carlos Gustavo Rodríguez Medina[2]

Gabinete de Computación / Fac. de Ingeniería / Univ. Nacional de San Juan [1,2]

Av. Libertador Gral. San Martin 1109 (oeste) – San Juan
0264-4211700 (Int. 285[2] / 435[1])
snavas@unsj.edu.ar [1], grodriguez@unsj.edu.ar [2]

## RESUMEN

Las técnicas para implementar esteganografía digital en portadores multimedia, para comunicación encubierta, deben responder a tres parámetros: Perceptibilidad, Capacidad y Detectabilidad. La tercera condición es imprescindible solo para casos especiales donde interesa que el portador con mensaje sea resistente al estegoanálisis. La premisa aquí es obtener las máximas capacidades, pero resulta en una solución de compromiso, ya que un aumento de Capacidad implica un incremento de perceptibilidad (y de detectabilidad).

Diversas técnicas se han propuesto, algunas son muy utilizadas hoy día, pero proveen *Capacidad* portadora más bien baja [1][2][3].

En el presente trabajo se expone una técnica, que llamamos "Sustitución Múltiple". En ella, para inyectar el mensaje, básicamente, se utilizan franjas de bits de los bytes correspondientes a cada canal de color de una imagen RGB. Actúa sobre las capas componentes inferiores consecutivas y completas de la imagen. No se aconseja utilizar más allá de las 4 primeras con este método.

Se logra así alcanzar un 37,5%[1] de capacidad en forma directa y segura, y hasta el 50% con elección de portador por análisis de ruido [4], lo cual es muy superior a otras técnicas en uso. Se propone también una variante resistente en cierto grado al estegoanálisis. Incrementos indirectos en la capacidad se obtienen por previa aplicación de algoritmos de compresión sobre el mensaje. Se suma importante aporte a la seguridad utilizando previos algoritmos de criptografía.

Se presenta también la implementación en Matlab, como programa piloto, que incluye la técnica propuesta y algoritmos de detección de ruido.

**Palabras clave:** Esteganografía, Sustitución Múltiple, Matlab.

## CONTEXTO

El presente tratado expone una metodología esteganográfica, propuesta e implementada a nivel software, que incluye nueva técnica esteganográfica por Sustitución Múltiple y detección de ruido en imágenes; en el marco de un actual proyecto que fuera originado luego las tesis de posgrado *"Exploración de efectos esteganográficos sobre portadores imagen de mapa de bits utilizando diferentes técnicas y algoritmos" y "Estudio, análisis, desarrollo y propuestas de algoritmos para la selección óptima de métodos de sustitución en aplicaciones esteganográficas"[5][6],* de Maestrías en Informática de la UNLaM.

Al proyecto lo conforma un equipo de investigación en la temática, en la Facultad de Ingeniería de la UNSJ.

## 1. INTRODUCCIÓN

La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador, de modo que pase inadvertido el hecho. La esteganografía juega un

[1] Estos extremos son siempre sin cobertura de *Detectabilidad*. Provee niveles muy altos de *capacidad* con *perceptibilidad* baja.

papel importante en la Seguridad de la información. Constituye una línea de investigación muy vigente, que se enmarca en lo concerniente a Seguridad Informática. Sus aplicaciones más comunes son: Comunicación encubierta y Protección de propiedad intelectual. Aquí nos enfocamos en la primera.

Los portadores preferidos son los archivos multimedia (imagen, video, sonido). El presente tratado se enfoca particularmente en portadores imagen BMP RGB[2] de 24 bits por la facilidad de analizar y exponer la técnicas.

Un imagen puede ser utilizada para ocultar, a la vista de intrusos cualquier mensaje u objeto software (archivo), codificándolo como sutiles cambios en los colores de los píxeles, en áreas poco significativas, que no deben ser percibidos por el ojo humano; de tal forma que el portador que contiene el mensaje, llamado *"Estegoportador"*, pueda ser transmitido, sin detectar el hecho. El receptor aplicará el proceso inverso (decodificación) para recuperar el mensaje oculto [5].

Las técnicas digitales empleadas para implementar esteganografía deben responder a tres parámetros: Perceptibilidad, Capacidad y Detectabilidad. La tercera condición resulta una exigencia en caso que se requiera resistencia al estegoanálisis[3]; son los casos, por ejemplo de aplicaciones militares, gubernamentales, espionaje, etc. Fuera de estos casos específicos, interesa más obtener un rendimiento o *Capacidad* lo más alta posible.

Ello resulta en una solución de compromiso, ya que un aumento de *Capacidad* incrementa la *perceptibilidad* (y *detectabilidad*).

En la presente propuesta, "*Sustitución Múltiple*", lo que prima es la obtención de elevada *Capacidad* en el portador, manteniendo un nivel aceptable de *Perceptibilidad*. Aunque una variante, que se mostrará, permite la cobertura a ataques comunes de estegoanálisis, es decir, cubre también *Detectabilidad*, lo cual se logra en detrimento de la *Capacidad*.

Diversas técnicas han sido propuestas, y son muy utilizadas actualmente, aunque proveen *Capacidad* relativamente baja, lo cual puede obligar a desmembrar el mensaje en varios portadores, con las consecuentes complicaciones. Así por ejemplo, en el dominio del espacio, se presentó en 2016 una mejora de BPHM (Block Pixel Hiding Method), llamada IPHM (Improved Pixel Hiding Method) [1], que logra duplicar la capacidad de la primera, la eleva a 25%, *pero posee una severa limitante*: un 5% de pérdida del mensaje, ello la limita a que los "archivos mensajes" solo puedan ser imágenes en tonos de grises, ya que ellas sí pueden ser interpretadas a pesar de la perdida. Se tiene también la conocida técnica LSB (Least Significant Bit) [2], quizá la más popular y una de las más utilizadas, que permite una máximo de 12,5%, ésta, además de su acotada *Capacidad,* tiene la desventaja de que es sumamente detectable. En el dominio de la frecuencia está la muy utilizada técnica basada en DCT (Discrete Cosine Transform) [3], aplicable a portadores JPG, la que suma propiedad de Robustez[4], pero con menor capacidad que a las otras.

**Nota:** la característica de Robustez se requiere solo para aplicaciones especiales, tales como watermarking y huellas digitales para copyright. Pero no es necesaria para comunicación encubierta.

En la técnica expuesta aquí se propone sustituir, de determinada manera, más de un bit del mensaje en cada byte del portador, múltiples de hecho, en general N, donde N=1...8. /

Se puede entender a una imagen RGB 24bits como compuesta de 8 capas, capas simples serían por cada canal de color, y compuestas las constituidas por los tres canales simultáneos. Una capa es una de sus imágenes binarias componentes. Cuando se aplica filtrado por capas lo que se obtiene es la vista de una ellas, o más de una solapadas (Ej. la capa 1, o la 2 y 3 juntas). Véase Fig. 1.

[2] Imágenes bitmap con tres canales de color, RGB proviene de sus siglas en inglés, Red, Green y Blue.

[3] El estegoanálisis es la disciplina dedicada al estudio de la detección de mensajes ocultos usando esteganografía.

[4] Propiedad esteganográfica que permite que el estegoportador sea sometido a compresiones, rotaciones, encuadres, etc. sin que se pierda el mensaje oculto.

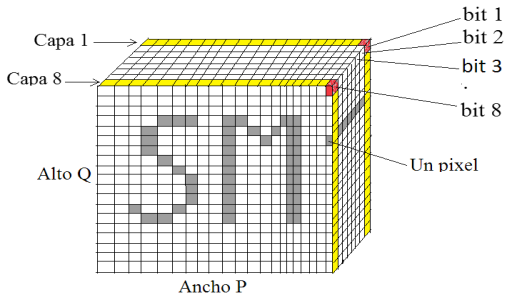



Fig. 1 - Modelo de representación de una imagen de 8 bits (un canal de RGB) de PxQ pixels.

El método de *Sustitución Múltiple* inserta el mensaje usando una o más capas de la imagen (una franja), utiliza N capas en general.

Usando una capa cualquiera de un solo canal de color (un mismo bit de todos los bytes de un color) estaríamos usando 1 bit por cada 3 bytes de la imagen (el pixel tiene 3 bytes: R G y B), ello daría una capacidad de 1/8x1/3= 0.04166, el 4.67%. Si lo hacemos en forma simultánea en los tres canales (capa compuesta), sustituiríamos 3 bits, 1 bit en cada una de la capas de color, con lo cual la capacidad se triplica, entonces Cap=0.04166x3=1/8=0.125, es decir se obtiene una utilización del 12.5%. La técnica de Sustitución Múltiple trabaja así, en los tres canales simultáneamente, es decir en las capas compuestas, de modo que por cada una (unidad de N) obtenemos 12.5% de capacidad. Si N=2 la capacidad es 25%, si N=3 es 37.5%. *El valor de N no solo hace referencia a la cantidad de capas a usar, sino también a su posición, contándose la primera como la capa 1* (Véase Fig. 1). Obviamente a medida que usamos más capas la *Perceptibilidad se incrementa*. Si N=1 se está manipulando la primer capa del portador.

Nótese que el máximo posible es N=8, máxima cantidad capas. Claro está, si bien es posible una sustitución con N=8, se estaría causando alteraciones en todas las zonas de la imagen, así la característica de *imperceptibilidad* no sería conseguida. En ese sentido, en el trabajo [5] se hizo un examen exhaustivo de la profundidad de bits, la posición de la capa usada y los efectos causados en las imágenes y se declaran los valores máximos permitidos para lograr una imperceptibilidad razonable, y según el nivel de ruido de la imagen ("categoría de imagen") [4].

Entonces, surge un interrogante lógico: ¿Cuántas capas y en qué posición se pueden utilizar sin notar alteraciones en el portador?

No hay una respuesta directa, y surgen propuestas que optimizan el proceso esteganográfico, analizando tipo de imagen, efectos sobre ella y características del portador [5].

Para tratar de dar una respuesta acotada y centrarse en la descripción de la técnica de interés, se puede decir que en primera instancia *un valor seguro para baja perceptibilidad es N=3*, más allá de ése dependerá del ruido del portador. N=4 se puede usar, pero para asegurar la imperceptibilidad se debe utilizar la técnica acompañada de algoritmos de selección de portador por nivel de ruido [4]. De aquí derivan las máximas capacidades asociadas a la técnica "Sustitución Múltiple": N=3, Cap=12.5% x 3 = 37.5%; y N=4, Cap = 12.5% x 4 = 50% (cada capa provee 12.5%).

*Descripción y algoritmia de la técnica Sustitución Múltiple:*

Una imagen color bitmap de 24 bpp está formada por tres canales de color, Rojo, Verde y Azul, cada uno de un byte de profundidad. Estas tríadas se disponen de forma consecutiva en la imagen. La conjunción de los tres canales forman cada pixel de la imagen.

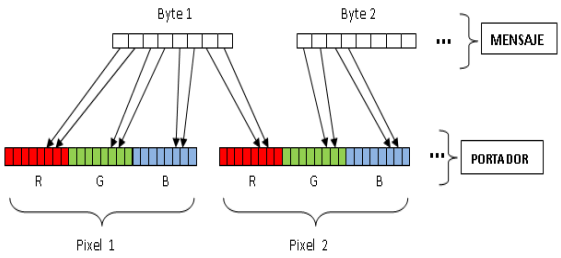



Figura 2. Implementación con N=2 partiendo desde la segunda capa. Cap. 25%. Cubre Detectabilidad.

Como se mencionó, en la técnica de Sustitución Múltiple, se reemplaza N bits de cada canal R, G y B; por sendos bits consecutivos del mensaje, en los pixeles necesarios de la imagen, hasta lograr ocultar todo el mensaje.

En la Fig. 2 se observa un diagrama para N = 2, donde se aprecia que cada dos bits correspondientes a los bytes del mensaje sustituye a 2 bits del canal R, análogamente para

los canales G y B. Luego se continúa ocultando los restantes bits del mensaje en cada uno de los siguientes pixeles del portador, de la misma forma, hasta que completar el mensaje.

Nótese que este caso ejemplo se están utilizando las capas 2 y 3, véase Fig. 1.

Observar que en este caso son necesarios *4* bytes del portador para ocultar *1* byte del mensaje, porque se están utilizando 2 capas; *capacidad recepción* resulta 25% (1/4x100).

Existe una relación de tamaños portador/mensaje a cumplir necesariamente, ella depende mucho de la técnica utilizada.

Respecto de otras técnicas en uso, la capacidad alcanzada aquí es muy superior, permite ocultar mayor cantidad de datos en un portador, incrementando la *capacidad de ocultamiento* en función del aumento del valor N.

La mayoría autores y desarrolladores considera que la utilización de más allá de la primer capa es inapropiada porque causa efectos visuales perceptibles. Hemos realizado rigurosos estudios, con ayuda herramientas software diseñadas al efecto, que demuestran que con *la utilización de hasta la tercera capa no se percibe a simple vista los efectos*, y esto es contando con la imagen original a los fines comparativos; difícilmente se detectarían alteraciones con N=3 sin usar herramientas, y de hecho, un intruso no dispondrá normalmente de la imagen original, por tanto le resultará imposible notar alteraciones. *La única condición para que resulte muy efectivo, el caso de N=3, es tratar de no utilizar portadores que tengan zonas de colores planos.*

En el ejemplo de la Fig. 2, se utilizaron dos capas, la segunda y tercera, *evitando la primera*. Se hace notar que de haber utilizado las 3 primeras capas (tres bits por byte de canal) el *efecto sobre perceptibilidad sería el mismo*, pero la capacidad sería del 37.5%. Entonces ¿Cuál es la ventaja de no usar la capa 1? Ella radica en que *aquí se tuvo en cuenta el factor Detectabilidad.* Los software de estegoanálisis[5] normalmente analizan la primera capa de una imagen, buscando alteraciones estadísticas por canal (son tres imágenes monocromo a procesar). Por una parte es porque así trabaja la mayoría de las técnicas esteganográficas más utilizadas, por otra, porque analizar varias capas apareja de un alto costo computacional, si se considera que el estegoanálisis suele ser realizado en línea mientras circulan las imágenes, y el tráfico es demasiado alto.

Así se ha intentado mostrar no solo el método de Sustitución Múltiple, sino *una variante* de él, que permite cubrir la detectabilidad. Obviamente, para casos especiales (aplicaciones militares, espionaje, etc.) el requerimiento es mayor, una Indetectabilidad muy alta; en tales casos se utiliza otra metodología, que escapa al alcance de este tratado.

Finalmente, un incremento indirecto de la capacidad se puede obtener aplicando al mensaje previamente un algoritmo de compresión, tal como el LZW (Lempel Ziv Welch). Y, por si un intruso lograra extraer el mensaje de un estegoportador es conveniente aplicar previamente al mensaje algún algoritmo de encriptación. Ambas cosas, compresión y encriptación, podrían ser parte de un software esteganográfico de usuario final que se desarrolle; pero si no lo provee, se puede usar, por ejemplo, 7-Zip, de alto ratio por LZMA (Lempel-Ziv-Markov) y LZMA2 y que puede cifrar los datos bajo el estándar AES de 256 bits [7].

*Implementación Matlab:*

Matlab es un software matemático que ofrece un entorno de desarrollo integrado (IDE) con un lenguaje de programación propio. Matlab es ampliamente utilizado en desarrollos científicos y en el ámbito académico.

Se ha optado por trabajar con este software, por la potencialidad que presenta para el procesamiento de imágenes, opera sobre ellas tratándolas como matrices. Por cada archivo imagen que se abre desde Matlab, se generan tres matrices, una para cada canal de color (Ver Fig 1). Se utiliza en conjunto con el Toolbox de procesamiento de imágenes. [6]

Se ha programado, según lo descrito en el apartado anterior, Fig.2, una función que implementa el algoritmo que aplica la Sustitución Múltiple. El formato es el siguiente:

*SM(N) – Sustitución Múltiple*

[5] El estegoanálisis representa la corriente contraria a la esteganografía, cuya finalidad es detectar mensajes ocultos en portadores.

*N es el número de capas o bits por byte a sustituir en cada canal de color del portador, desde la 1ra.*

*SMV(N) – Variante que omite capa 1.*

*N es el número de capas o bits por byte a sustituir en cada canal de color del portador, desde la 2da.*

Desde la línea de comando de Matlab se ejecuta función "*SM(N)*".Pide el ingreso de N, cantidad de bits por byte o capas que se desea usar del portador en sus canales de color.

La ejecución de la función solicita seleccionar el archivo de la imagen portadora, luego se selecciona el archivo de mensaje. Posteriormente, la función aplica el algoritmo de *Sustitución Múltiple* y presenta gráficamente una ventana con la imagen portadora original y otra con la imagen estegoportadora.

## 2. LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

La línea de investigación corresponde a la temática de *Esteganografía*, la que se enmarca en el área de Seguridad Informática. Los autores del presente trabajo han elaborado dos tesis de Maestría en este tema. Mantienen un proyecto que avanza en estudios y desarrollos de esteganografía. También han realizado publicaciones en diferentes congresos, particularmente en varias WICC. Los Trabajos realizados desde el año 2006 al presente, aportan resultados innovadores en el área.

## 3. RESULTADOS OBTENIDOS

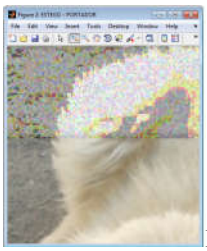
Se ha expuesto la técnica de Sustitución Múltiple y una variante que cubre detectabilidad; mencionando sus ventajas asociadas y la forma de aplicarla exitosamente. Exponiendo también el desarrollo de un software piloto implementado en Matlab. Con esa aplicación esteganográfica se puede realizar diversos ensayos con diferentes valores de "N". Ello permite realizar variadas pruebas y ver cómo influye en la imagen original la sustitución en distintas cantidades de capas. También se pueden aplicar realces de los efectos esteganográficos “no visibles”, con el fin de observar la porción y/o proporción ocupada por el mensaje. Adicionalmente se brindan algunos datos, como el porcentaje que ocupa el mensaje en el portador, y otros de interés.

A- Portador bmp.

B- Mensaje bmp

Figura 3. Portador y mensaje utilizados.

A- Estegoportador.



B- Realce y Ampliación

Figura 4. Estegoportador con Realce de efectos y ampliación de imagen.

Para observar resultados con N=3, se selecciona un portador imagen BMP 24 bpp, de 400x418 pixeles y tamaño 490KB, Fig. 3-A.

Como mensaje se usó un archivo copia de pantalla de 42KB (portada del trabajo), Fig. 3-B. El mensaje podría haber sido de cualquier tipo (imagen, doc, ejecutable, etc.). El resultado, estegoportador, se muestra en la Fig. 4-A; observar que resulta ser visualmente idéntica a la original. A los fines demostrativos, se ha hecho un realce del efecto esteganográfico y ampliación de la zona, se aprecia el área ocupada por el mensaje oculto (que bajo condiciones normales no es visible), ello se expone en la figura 4-B.

## 4. FORMACIÓN DE RECURSOS HUMANOS

En la temática de Esteganografía, los integrantes del grupo de investigación vienen trabajando desde el año 2005. A fines de 2006, el primer autor de este trabajo defendió su Tesis de Maestría que trata del tema en profundidad. En octubre de 2015, el segundo autor realizó su defensa de Tesis de Maestría en Informática, que deriva y amplía la anterior, continuando el tratamiento del tema.

Actualmente se prosigue con el estudio, habiendo sumado un miembro más, que tiene en curso su tesis, en la misma maestría.

## 5. BIBLIOGRAFÍA


[1] Renza, Diego et al. *Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color* [en línea]. Ingeniería y Ciencia, vol. 12, núm. 23, pp. 145-162. 2016. Universidad EAFIT. Colombia. Disponible en: http://www.scielo.org.co/pdf/ince/v12n23/v12n23a09.pdf

[2] Rodríguez, Gustavo; Navas, Sergio; *Esteganografía: Sustitución LSB 1 bit utilizando MatLab*. XVIII WICC, Universidad Nac. de Entre Ríos. 2016. Libro digital 1094p. Pág. 859-864, ISBN 978-950-698-377-2.

[3] Velasco Bautista et al. *Esteganografía en una imagen digital en el dominio DCT*. Científica [en línea] 2007. ISSN 1665-0654. Disponible en: https://www.redalyc.org/pdf/614/61411403.pdf

[4] Navas, G. Sergio; Rodríguez, Gustavo; Eterovic, Jorge; *Aplicación del filtro de Canny a la esteganografía digital*. Libro electrónico del XVI WICC. Ushuaia, Tierra del Fuego. 2014. Publicación digital ISBN 978-950-34-1084-4 .

[5] G. Sergio Navas. *Exploración de efectos Esteganográficos sobre portadores imagen de mapa de bits utilizando diferentes técnicas y algoritmos*. Argentina. Univ. Nacional de la Matanza – Escuela de Posgrado. Dic. de 2006.

[6] C. Gustavo Rodríguez M. *Estudio, análisis, desarrollo y propuestas de algoritmos para la selección óptima de métodos de sustitución en aplicaciones esteganográficas*. Argentina. Univ. Nacional de la Matanza – Escuela de Posgrado. Nov. de 2015.

[7] Shubhi Mittal, Shivika Arora, Rachnma Jain, *PData security using RSA encryption combined with image steganography, Information Processing* (IICIP). 1st India International Conference on, pp. 1-5, 2016. Disponible en: https://ieeexplore.ieee.org/document/7975347