SiPoIn: sistema de protección de información basado en estegoalgoritmo.

Víctor Manuel Valentín Barajas Carrera
Instituto Tecnológico Superior de Irapuato
victor.z.barajas@gmail.com

Gerardo Trejo Caballero
Instituto Tecnológico Superior de Irapuato
getrejo@itesi.edu.mx

Resumen

En este trabajo se presenta la implementación de un sistema de protección de información (SiPoIn) basado en la aplicación de un algoritmo de esteganografía sobre imágenes digitales. Desarrollado como una interfaz gráfica de usuario, el sistema permite de forma sencilla ocultar información dentro de una imagen denominada portadora. La información oculta, presentada en forma de imagen binaria y denominada imagen huésped, sustituye uno de los planos de la imagen portadora para pasar inadvertida por el ser humano. El sistema permite recuperar y guardar de forma sencilla los mensajes ocultos por medio de la obtención de los planos de bit de cualquier imagen portadora. Los resultados sugieren que el sistema propuesto puede ocultar satisfactoriamente hasta dos mensajes en los planos menos significativos de la imagen portadora.

Palabras clave — Esteganografía, imagen digital, plano de bit.

Descripción del proyecto

En una imagen digital, un pixel está conformado por el valor de intensidad f(x,y) asociado a la posición (x,y). Así mismo, el plano de bit es un espacio de memoria que registra un único bit correspondiente a la profundidad o intensidad de cada pixel (Borah y Borah, 2015). Se le denomina plano porque es una matriz que

contiene en las coordenadas de cada pixel el estado de un bit del valor de intensidad del pixel (González y Woods, 2009).

La Esteganografía es un conjunto de diferentes técnicas que permiten ocultar información dentro de un objeto denominado portador. La principal ventaja de éstas técnicas es que la información oculta (huésped) pasa desapercibida y puede ser guardada o enviada de forma segura a través del medio portador (Niels, 2001).

El Sistema de Protección de Información (SiPoIn) basado en estegoalgoritmo e imágenes digitales, es una aplicación basada en el entorno de desarrollo de Matlab que implementa un algoritmo de Esteganografía utilizando como medio portador una imagen digital. SiPoIn obtiene los planos bit de la imagen portadora y sustituye uno de estos planos por la imagen binaria que contiene el mensaje o información que, al ser alojada en la imagen portadora, pasa inadvertida a la visión humana [3]. El sistema ha sido integrado como una interfaz gráfica de usuario sencilla e intuitiva que permite al usuario sustituir cualquier plano de bit de la portadora. Las pruebas sugieren que deben utilizarse los planos de bit menos significativos para obtener resultados satisfactorios que sean independientes de la imagen portadora. El sistema incorpora una función destinada a extraer los mensajes que han sido ocultados dentro de una imagen digital.

Objetivo

Implementar un sistema de protección de información basado en técnicas de esteganografía aplicadas sobre imágenes digitales que permita ocultar y recuperar información al usuario de forma sencilla e intuitiva.

Justificación

Actualmente se tiene una gran dificultad para guardar, recibir y enviar información sin que un agente externo tome posesión de la información que no ha sido destinada a este. Las personas a lo largo del tiempo han buscado métodos que les

permita comunicarse con otras personas sin que su información caiga en manos indeseadas antes que a los receptores a quienes va dirigida, uno de estos métodos es codificar la información para que personas que no tuvieran conocimiento de este código no puedan decodificar la información y apoderarse de ella. En la actualidad un método comúnmente utilizado para proteger información es la criptografía, que consiste en mandar un mensaje que solo podrá leerlo la persona que cuente con la contraseña para poder leer este mensaje, sin embargo, desafortunadamente dicho método tiene la desventaja de que el solo hecho de cifrar o enviar un mensaje con caracteres sin sentido llama la atención de personas u organizaciones que desean obtener esa información y pueden simplemente impedir que el mensaje llegue a su destino o en el peor de los casos, obtener la información y utilizarla en pro de sus objetivos mediante el empleo de técnicas de descifrado.

¿Pero, y si pudiéramos enviar información sin que nadie pueda darse cuenta que es enviada?, no habría sospecha en algo que no puedes detectar y el mensaje sería enviado con éxito, de esta cuestión surge la necesidad de implementar un sistema de protección de información basado en la Esteganografía que nos permitirá guardar y enviar información de forma segura es decir la información solo podrá ser vista por la persona que tenga conocimiento del algoritmo utilizado para guardar la información y donde fue alojada que en el caso de este trabajo se utilizarán imágenes digitales.

Metodología

El sistema de Esteganografía implementado consta de tres etapas con las cuales se consiguen remplazar hasta un 1.1764% de la información de la imagen portadora con un mensaje huésped sin alterar la imagen original lo suficiente como para que las modificaciones sean perceptibles a la visión humana.

En la primera etapa, se obtienen los 8 planos de bit de la imagen portadora tal y como se representa en la Figura 1. En la segunda etapa, se sustituye un plano de

bit de la imagen portadora, por una imagen huésped que corresponde con el mensaje que se desea ocultar, siendo dicha imagen huésped una imagen binaria con las mismas dimensiones que la imagen portadora, tal y como se aprecia en la Figura 2. Finalmente, en la tercera etapa, se construye la imagen de salida conformada por la imagen portadora y la imagen huésped, tal y como se representa en la Figura 3.

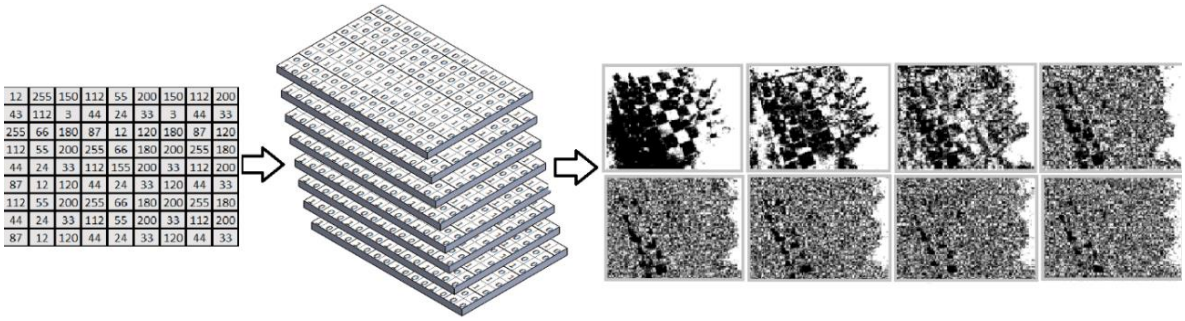


Figura 1. Primera etapa: obtención de los planos de bit.

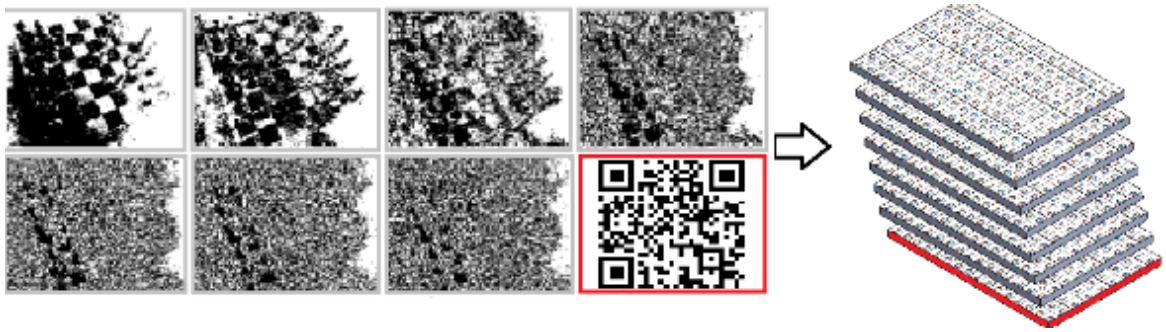
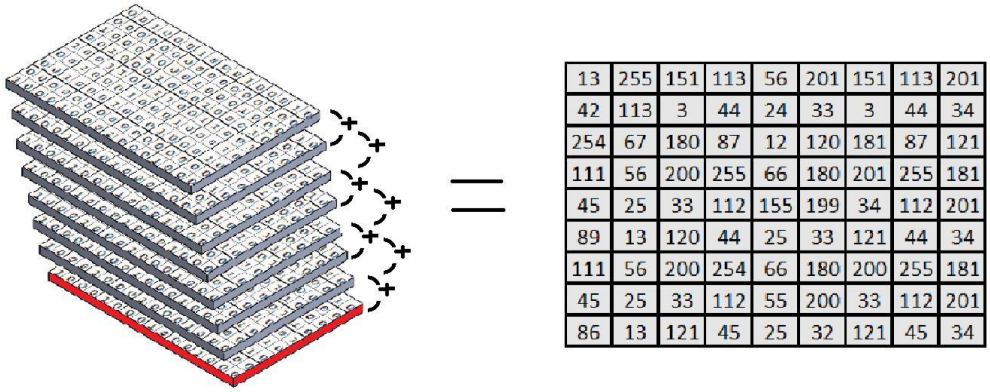


Figura 2. Segunda etapa: sustitución de un plano por mensaje (imagen huésped).



13	255	151	113	56	201	151	113	201
42	113	3	44	24	33	3	44	34
254	67	180	87	12	120	181	87	121
111	56	200	255	66	180	201	255	181
45	25	33	112	155	199	34	112	201
89	13	120	44	25	33	121	44	34
111	56	200	254	66	180	200	255	181
45	25	33	112	55	200	33	112	201
86	13	121	45	25	32	121	45	34

Figura 3. Tercera etapa: construcción de imagen de salida.

La metodología implementada por el sistema de protección de información (SiPoIn) se detalla a continuación:

Se considera una matriz con los valores de intensidad asociados a una imagen en escala de grises con dimensiones M x N y una profundidad de color de 8 bits. A continuación, se obtienen los 8 planos de bit de la imagen, identificados como los planos B0, B1, B2, B3, B4, B5, B6, B7. Enseguida, el mensaje huésped que corresponde con una imagen binaria de dimensiones M x N, debe ser insertada en uno de los planos con menor aporte de valor de intensidad a la imagen portadora, siendo estos los planos B0 y B1.

Una vez remplazado el plano de bit por la imagen binaria se obtiene el valor de intensidad para cada pixel de la imagen con el mensaje huésped a partir de los ocho planos de bit mediante la suma del aporte de intensidad de cada plano de bit. El aporte de intensidad de cada plano está dado por la Ecuación 1 y solo aporta este valor a los pixeles en la posición donde los bits están en estado 1.

$$\alpha_i = 2^{i-1}. \qquad (1)$$

Donde α es el aporte de intensidad a la imagen del plano con que contiene los bits de la posición i del número de intensidad de cada pixel y el subíndice i es el número de la posición del bit asignado a cada plano empezando de derecha a izquierda.

El sistema SiPoIn, implementado bajo el entorno de desarrollo de Matlab, implementa la metodología antes mencionada y permite cumplir el objetivo de este trabajo. El sistema SiPoIn, contiene un panel de selección de planos (elemento 1 en la Figura 4), en el cual se permite seleccionar el plano de la imagen portadora que deseamos sustituir por nuestra imagen huésped (elemento 2 en la Figura 4) y una ventana de vista previa, la cual muestra el aspecto de la imagen portadora con el mensaje huésped insertado en el plano seleccionado (elemento 3 de la Figura 4).

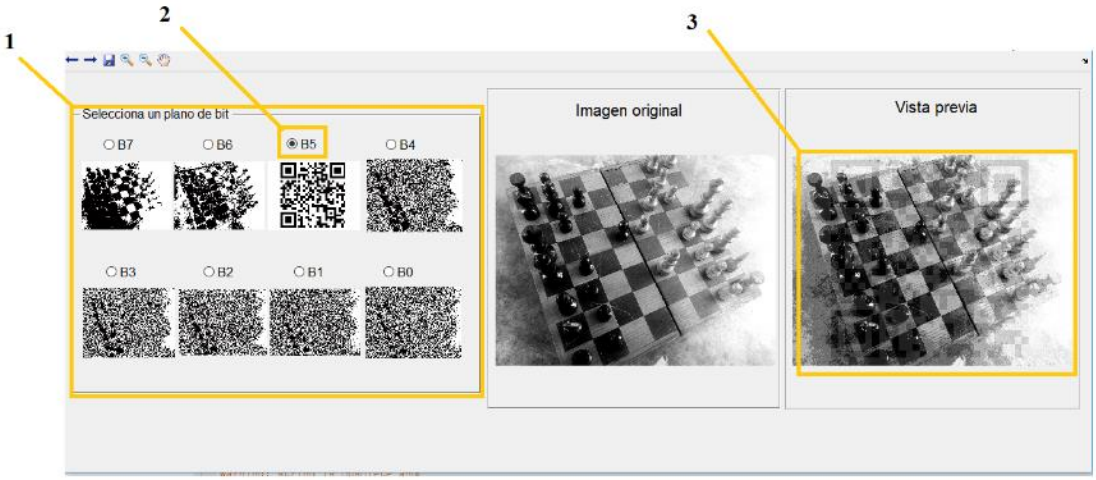


Figura 4. Interfaz gráfica de usuario desarrollada, SiPoIn.

Resultados

En la Figura 5 se muestran un ejemplo de imagen portadora y dos ejemplos de imágenes huésped utilizadas en las pruebas realizadas. La Figura 6b, muestra el resultado de insertar el mensaje huésped 1 en el plano B0. La Figura 6c, muestra el resultado de insertar dos mensajes huésped en la imagen portadora: el mensaje huésped 1 en el plano B0 y el mensaje huésped 2 en el plano B1.

Figura 5. En a) imagen portadora, en b) imagen binaria asociada al mensaje huésped 1, en c) imagen binaria asociada al mensaje huésped 2.

a) b) c)

Figura 6. Resultados obtenidos al insertar en la imagen portadora de la extrema izquierda, uno y dos mensajes huésped (centro y extrema derecha respectivamente).

A. Discusión

La Figura 6 sugiere que la inserción de uno o dos mensajes ocultos en forma de imágenes huésped es posible y viable sobre la misma portadora, siempre y cuando sean introducidos en los planos de bit menos significativos, preferentemente en los planos B0 y B1. Lo anterior queda de manifiesto al observar que prácticamente las tres imágenes contenidas en la Figura 6 se perciben iguales (por el ser humano).

Es importante señalar, que la inclusión de mensajes ocultos en forma de imágenes huésped en planos diferentes al B0 y B1 es posible, pero su viabilidad estará comprometida de manera importante y sujeta a las particularidades de la composición de los mensajes e incluso, de la imagen portadora.

Conclusiones

El sistema de protección de información basado en estegoalgoritmo e imágenes digitales hace posible la protección de información mediante el procesamiento digital de imágenes. El sistema consigue ocultar exitosamente hasta dos imágenes binarias dentro de una imagen en escala de grises, además permite recuperar los mensajes ocultos de forma sencilla mediante la obtención de los planos de bit de cualquier imagen en escala de grises.

El sistema fue validado mediante la observación directa de los cambios en al aspecto visual de una imagen en escala de grises, obteniendo resultados satisfactorios al ocultar las imágenes huésped en los planos de bit menos significativos de la imagen portadora.

Referencias

Borah, A. & Borah, B., (2015). A Spatial Domain Reversible Visible Watermarking Technique for Textured Images. *International Journal of Computer Applications*, 129(14), 0975 – 8887.

González, R. C., & Woods, R. E. (2009), *Digital Image Processing*, (third edition), New Jersey, Prentice Hall.

Niels, P., (2001). *Defending Against Statistical Steganalysis*. In Proceedings of the 10th USENIX Security Symposium, pp 323–335. recovered from: https://www.usenix.org/legacy/publications/library/proceedings/sec01/full_papers/provos/provos_html/index.html