

Universidad Nacional del Litoral
Facultad de Ingeniería y Ciencias Hídricas

Captura y Procesamiento Digital de Señales e
Imágenes



*Implementación de algoritmo para esteganografía
utilizando la paleta de colores de una imagen*

Dabin, Alejandro - Guerin, Fernando

05/11/2004

Resumen

En este trabajo se implementó un algoritmo de esteganografía para ocultar y extraer archivos dentro de una imagen. El mismo oculta los datos usando la paleta de colores de una imagen indexada, la cual debe tener hasta 128 colores, ya que el algoritmo duplica la cantidad de colores de la paleta. En este algoritmo la codificación no se hace en el espacio RGB sino en el HSI, para hacer menos sospechosa la paleta de colores.

Introducción

La palabra esteganografía significa literalmente *escritura oculta* y consiste codificar información secreta ocultando su existencia mediante alguna cubierta . Se intenta que la información pase inadvertida y no despierte sospechas en terceras personas. Diversas técnicas han sido utilizadas desde épocas antiguas. Uno de los primeros documentos que describen la esteganografía está en las historias de Herodotus. En la antigua Grecia, los textos eran escritos en tablas cubiertas de cera. En una historia, Demeratus quería notificar a Sparta que Xerxes intentaba invadir Grecia. Para no permitir la captura, quitó la cera de las tablas y escribió un mensaje en la madera de debajo. Luego cubrió de nuevo las tablas con cera. Las tablas parecían vacías y sin uso entonces pasaron la inspección sin problema.

La esteganografía puede ser vista como parecida a la criptografía. Ambas han sido usadas a través de los tiempos para proteger información. Algunas veces estas tecnologías parecen converger, mientras que sus objetivos son diferentes. Las técnicas de criptografía cifran el mensaje de manera que si es interceptado no se pueda entender. Por otro lado, la esteganografía camufla el mensaje sin modificar su estructura, para ocultar su existencia y con ello hacerlo invisible, mientras que de hecho se está enviando un mensaje. Un mensaje encriptado puede levantar sospechas, mientras que un mensaje “invisible” no lo hará. Sin embargo, se considera que si se detecta la presencia de un mensaje (aunque no pueda ser leído), el método ha fallado.

Un sistema de codificación esteganográfica recibe una imagen para usar de cubierta (X) y los datos a ocultar (D), los procesa y genera una imagen de salida (Z), como se ve en la Figura 1. Esta última debe parecerse a la cubierta ante una inspección no exhaustiva.

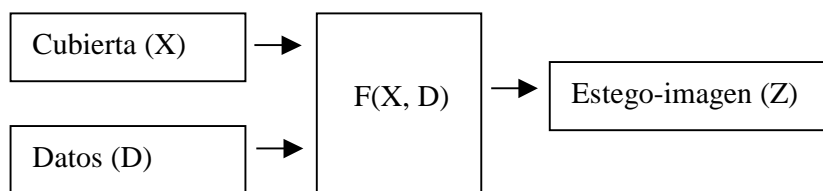


Figura1. Codificación esteganográfica.

La técnica es utilizada ampliamente en los siguientes campos: protección de copyright, etiquetado de características y comunicaciones secretas.

Materiales y métodos

El algoritmo oculta la información codificando cada bit con el bit menos significativo del componente azul del color indexado en la paleta de colores. Para esto se duplica la paleta creando colores similares a los originales, intentando que no se repitan. Por lo tanto, se tiene la limitación de que no se puede utilizar una imagen con una paleta de más de 128 colores.

La paleta de colores original se convierte al espacio HSI. El procedimiento consiste en procesar cada color de la siguiente manera:

1. Hacer que el componente de tono sea par.
2. Si este color no está en la paleta nueva, agregarlo. De lo contrario, aplicar pequeñas variaciones sobre los componentes saturación e intensidad hasta obtener un color que no esté en la nueva paleta y agregarlo. Si no se logra, igualmente se agrega.
3. Hacer que el componente tono del punto 1 sea impar y aplicar el mismo secuencia que en el punto 2.

Los colores similares siempre van guardados de a pares, el primero tiene su componente de tono par y el segundo impar. Esta disposición es utilizada para guardar la información. El uso de un componente de tono par codifica un bit 0, y el de uno impar un bit 1. Cuando se termina de codificar todo el archivo, se rellena el espacio restante con datos aleatorios. Para hacer más sencilla la recuperación se guardan como cabecera la cantidad de bytes del archivo y su extensión.

La paleta obtenida puede resultar sospechosa por el ordenamiento descrito en párrafo anterior; para evitarlo se la ordena por intensidad . Luego se transforma esta paleta al espacio de RGB.

La cantidad de bytes de información que se puede almacenar es menos de un octavo del tamaño en pixels de la imagen de cubierta.

Para la decodificación de la imagen se convierte la paleta al espacio HSI y se decodifican los bits originales según el bit menos significativo del componente de tono. El tamaño del archivo guardado en la cabecera se utiliza para saber hasta donde leer.

Resultados

En la Figura 2 se muestra la imagen a codificar, en la Figura 3 la de cubierta y en la Figura 4 la que se transmite.

A simple vista es imposible notar la diferencia entre la imagen original y la final. Tampoco es detectable por el bit menos significativo de los componentes RGB, ya que la codificación se hace en el espacio HSI. Además, el componente de tono (Hue) es el componente del conjunto HSI que menos información subjetiva aporta a la imagen.

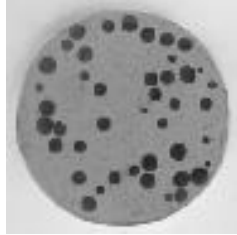


Figura 2: Imagen a codificar.

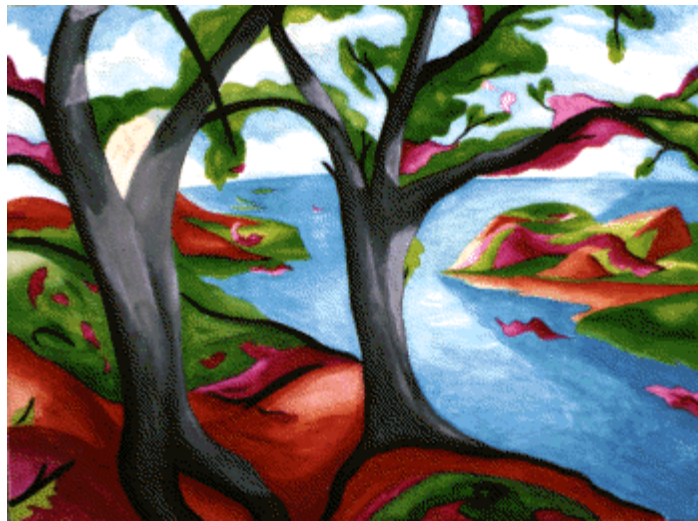


Figura 3: Imagen de cubierta

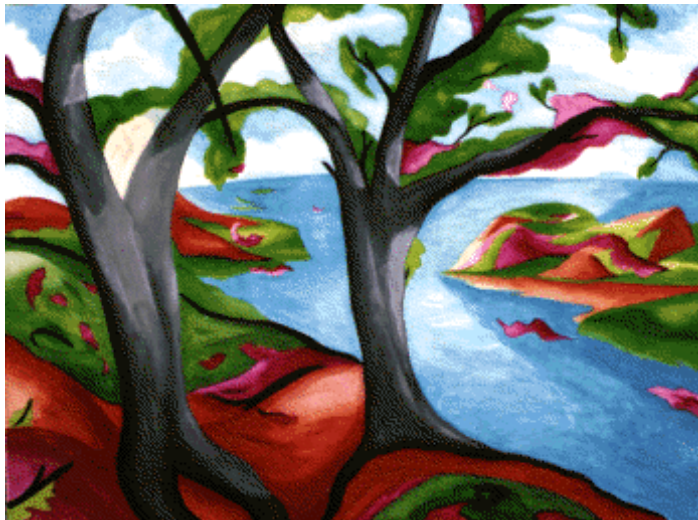


Figura 4: Imagen final

Conclusiones

El algoritmo utilizado tiene una implementación medianamente sencilla y provee un buen método para ocultar información cuando su tamaño es menor a un octavo de la imagen de cubierta. Es muy difícil percibir que la imagen ha sido alterada si se desconoce la original. Aún teniendo las diferencias son mínimas.

El método no es robusto porque cualquier ruido altera el mensaje oculto.

Se puede ampliar la capacidad de almacenamiento si se utilizan componentes HS que se diferencian en un bit. Esto permite codificar más de un bit en cada byte de la imagen de cubierta. Sin embargo, depende de la cercanía de los colores en paleta HSI e incrementa la complejidad de la implementación.

El receptor debe saber la forma en la que fue codificado el archivo por el emisor.

Bibliografía

1. Lin, E. T. y Delp, E. J., *A Review of Data Hiding in Digital Images*, Purdue University, USA, 1999.
2. John, Corinna, *Steganography - Indexed Images and their Palettes*, <http://www.codeproject.com/csharp/steganodotnet11.asp>
3. Jonson, N. F., *Steganography*, <http://www.jjtc.com/stegdoc/steg1995.html>