Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

SISTEMA ESTEGANOGRÁFICO GEHEIM

Ing. Maria Alejandra Gerardino García MSc.
Ing. Andrés Martínez Marín MSc.
Ing. Francy Rios Rosas MSc.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

El rápido crecimiento en el mundo de las redes ha obligado al desarrollo de técnicas de seguridad para la transmisión de datos a través de las redes de comunicaciones. Este trabajo resume el desarrollo de un software basado en un esquema de llaves esteganográficas generadoras de secuencias pseudos aleatorias tomadas como mecanismo para la inserción de información bajo una imagen digital. El Software denominado GEHEIM combina tres de las principales técnicas que contempla el estudio de seguridad en redes como lo son criptográfia, esteganografía y watermarking.

Palabras Claves:
Criptografía, Esteganografía, Marcas de Agua, Aplicación, Sistemas.

Abstract

Fast growing of computer networks have obliged every day more to development of reliable secure techniques for common channels data transmission. This work summarize the implementation of a software based in a schema using stego keys to create pseudo random sample sequences in the way to prove secure algorithms to hide information in digital images. GEHEIM Software is a combination of the first three technician that closed the study of security networks as are: Critography, steganography and watermarking

Keys Works:
Critography, Steganography, Watermarking, Software, Systems.

INICIO

Una técnica de recién desarrollo, en el campo de la seguridad informática, es la de ocultar información. En los últimos años ha recibido una significativa atención por parte de la industria y la academia. El principal propósito de la criptografía es el uso de códigos para convertir datos, de modo que sólo un receptor específico será capaz de leerlos con la ayuda de una clave (Delfs H. y Knebl H.). El objetivo de la esteganografia, como una nueva forma de encubrir las comunicaciones, es transportar un mensaje de manera que no se sepa su existencia, lo cual puede hacerse bajo una imagen o dentro de cualquier señal de sonido (Zöllner J), sin embargo, estas dos técnicas pueden ser combinadas encriptando primero el mensaje secreto y posteriormente encubriéndolo bajo datos aparentemente inocuos. Otra técnica similar a la esteganografia es la Marca de Agua, que es principalmente usada para protección de derechos del autor en productos electrónicos (Lin, E. y Delp E).

En este trabajo se presenta la combinación de estas técnicas en un software para la obtención de un sistema robusto, es decir, que sea capaz de funcionar bien o continuar funcionando bajo situaciones de posibles ataques informáticos que pueden estar presentes en la transmisión de información en el entorno de la red. Además, este sistema enmarca medidas de seguridad para la transmisión del mensajes conocidas como autentificación, servicio que asegura al receptor que el mensaje pertenece a la fuente de la que dice proceder, además de confidencialidad, protección de los datos transmitidos por medios de ataque pasivos, es decir, en forma de escucha o de observación no autorizadas. (William Stallings)

Métodos Usados

El diseño del software se centra en modelos de cifrados simétricos, es decir, el uso de una misma llave para activar el algoritmo de cifrado, así como el de descifrado. Este procedimiento, se utiliza para cumplir con tal transformación, involucra como requisitos dos de los elementos básicos que definen este tipo de código como lo son mensaje original y una clave secreta respectivamente. (Lucena M.)

Para el sistema esteganográfico la herramienta seleccionada en la construcción de este proyecto se encuentra categorizada dentro del grupo del Dominio de la Imagen. Las herramientas de dominio de imagen abarcan entre sus métodos el del bit- Más Significativo que aplican sobre la inserción de un bit de más baja significación (least significant bit, LSB) y la manipulación de ruido. Los formatos de imagen normalmente usado, en estos métodos esteganográfico, son aquellos que presentan bien definidos los componentes de estructuras del modelo de color tales como matiz, saturación, valor y brillantes, además de ser bien dinámicos para la manipulación y recuperación de la data. (Fridrich J., Du R. y Long M)

Marca de Agua es la última de estas técnicas de seguridad empleada para la construcción de este software y al contrario de lo anteriormente expuesto, en la citada técnica se elije como herramienta de trabajo el Método del Dominio, el cual está fundamentado en una aproximación desde el dominio de imagen, independientemente del formato de la imagen.

La marca de agua perceptible o visible es el logo de una empresa u otro tipo de imagen, que indica quien es el propietario de los datos. Algunas de las propiedades exigidas a este tipo de marcas son:

Ser obvios para cualquier persona con visión normal o corregida.

Tener características que formen una imagen por si mismos e identifique la institución u organización original.

Permitir que todas las partes de la imagen original sean vistas en la imagen marcada.

Deben ser difíciles de remover y falsificar. (Pfitzmann B.)

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Requerimientos y especificaciones

Del análisis practico del software desarrollado por Toby Sharp (Sharp, T) se extrae, para el desarrollo del sistema GEHEIM (nombre asignado al sistema proveniente del vocablo alemán geheim que significa secreto), el esquema de trabajo del Bit de Más Baja Significancia (LSB) como método de incrustación de datos bajo la imagen así como el uso de claves stego como semillas iniciales de un proceso pseudos-aleatorio. Haciendo referencia al ejemplo típico de un sistema esteganográfico: Alice y Bob, se describe de manera más clara la explotación de los procesos usados para la realización de este proyecto.

La figura 1 muestra el diagrama básico para un sistema de comunicaciones de seguridad ideal, donde se resalta primeramente la función del emisor. El emisor dentro este esquema está constituido por dos procesos para encriptar los datos y la integración de los mismos con la cobertura o imagen. Para la implementación, el proceso de encriptación de datos fue dividido en tres subprocesos: Pseudo Generador Aleatorio A, Pseudo Generador Aleatorio B y Codificación. Al mismo tiempo el proceso de integración también fue dividido en dos subprocesos: Esteganografia y Marca de Agua.

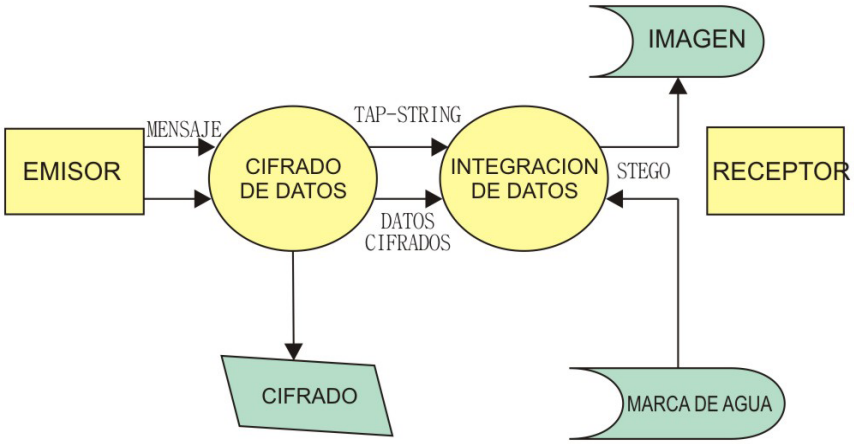

Figura 1. Diagrama de Emisor.

Cuando Alice necesita enviar un mensaje oculto a Bob. Alice edita el mensaje y simultáneamente genera una clave secreta (secuencia de caracteres alfa - numéricos definidos por el usuario del sistema). En el software GEHEIM esta clave sirve como semilla iniciadora de un proceso pseudo generador aleatorio A que toma ese resultado para la realización de dos tareas especiales:

1. Para iniciar un segundo Pseudo Generador Aleatorio B, desde el cual es generada una cadena de caracteres aleatoria (tap-string), que indica cuales pixeles de la imagen serán visitados para el proceso de incrustación de cada carácter del mensaje cifrado debajo de la imagen.

2. Para iniciar el proceso de codificación, donde será usado un flujo de cifrado como método de encriptación en vista de que no es conocido el tamaño del texto introducido por Alice. El cifrado resultante de este proceso se almacena en una base de datos para usarse posteriormente en el proceso de extracción, además será empleado junto al tap-string como dato de origen para el subproceso de esteganografia (ver figura 2).

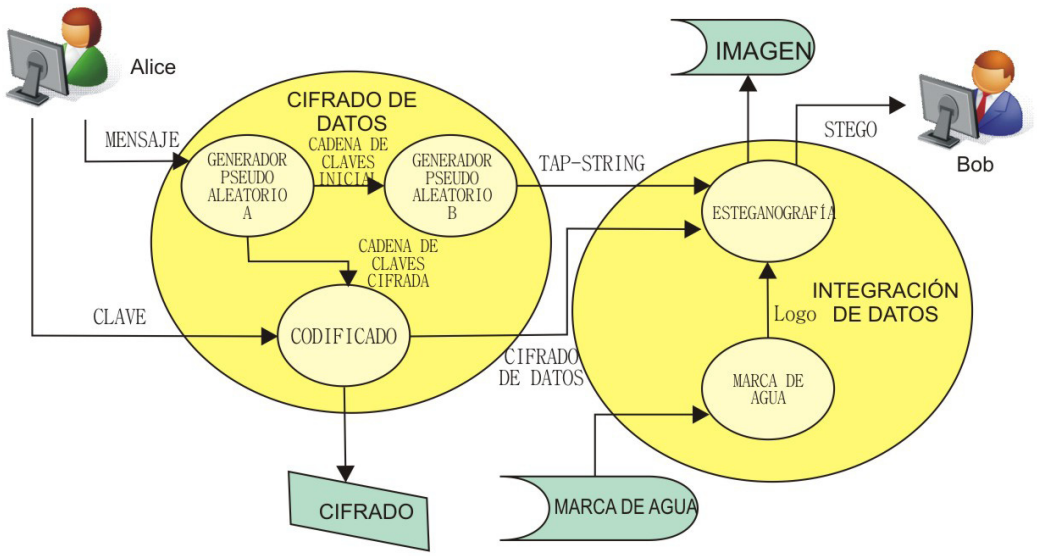

Figura 2. Diagrama del Emisor (Definición de Procesos).

Con respecto al proceso de integración, fue considerado dentro del subproceso esteganográfico un algoritmo basado en el método de bit de más baja significancia para la incrustación de los datos en la imagen, además de un subproceso, proporcionado por la técnica de marca de agua visible, para proporcionar seguridad extra, autenticación de la cubierta. Ambos sub procesos son alimentados por diferentes bases de datos, de acuerdo con los requerimiento necesitados por cada uno de ellos. Finalmente este proceso permite a Bob obtener el stego designado, es decir, la imagen con el mensaje incrustado bajo de ella.

De la misma manera que el diagrama del emisor fue diseñado el diagrama del receptor, el cual indica el esquema del proceso empleado para obtener por parte del receptor el mensaje original grabado bajo la imagen enviada por el emisor (ver figura 3).

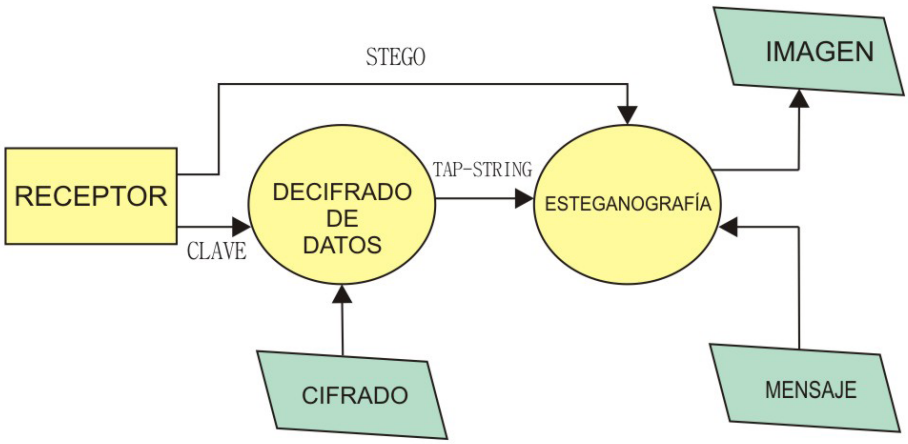

Figura 3. Diagrama del Receptor.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Bob, con el conocimiento de la clave secreta usada previamente por Alice, inicia el subproceso Pseudo Generador Aleatorio A contenido en el proceso de descifrado, tomando de la cadena resultante: el mensaje descifrado y la imagen original respectivamente.

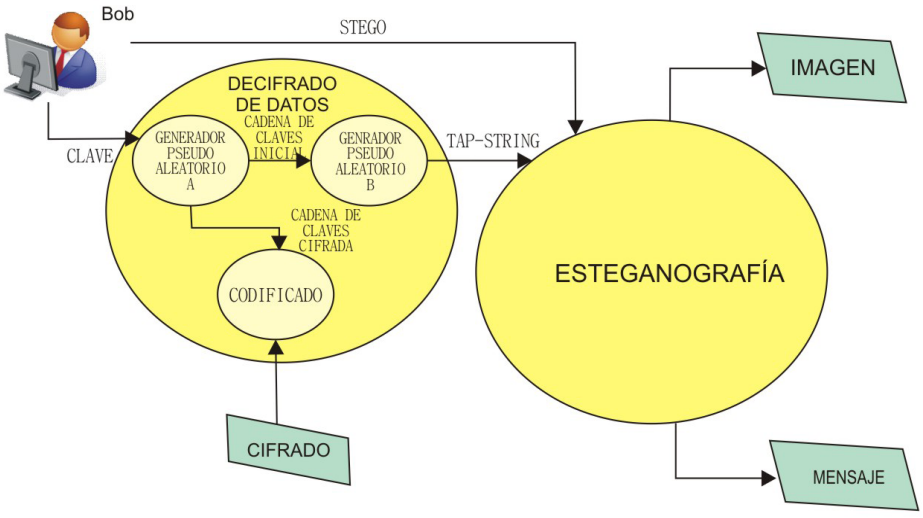

Figura 4. Diagrama del Receptor (Definición de Procesos).

Algoritmos y Estructura de Datos

El algoritmo del sistema GEHEIM fue construido a través de una combinación de métodos. Primero fue considerado para la encriptación del mensaje un algoritmo de flujo, dado que no se conoce con exactitud la longitud del mensaje transmitido por el emisor.

El algoritmo de cifrado transforma el texto plano (mensaje original) en texto cifrado, un bit a la vez. Tal como se muestra en la figura 5. El generador de flujos de claves produce un flujo de bits: k_1, k_2, k_3,…k_j. Este flujo de claves es calculado por una operación lógica XOR y un flujo de bits de texto plano, p_1, p_2, p_3, …p_i, para producir el flujo de bits de texto cifrado C.

$$C_i = p_i \oplus k_i$$

Del lado contrario para el proceso de descifrado, a los bits del texto cifrado se les aplica un XOR con un flujo de claves idéntico a la original con el fin de recuperar los bits del texto original.

$$P_i = c_i \oplus k_i$$

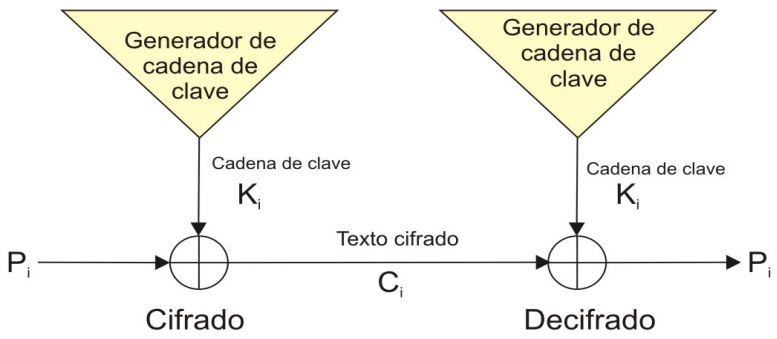

Figura 5. Algoritmo de Cifrado.

La seguridad del sistema depende enteramente del interior del generador de flujo de clave.

Si la salida del generador de flujo de claves termina en un flujo de ceros, el texto cifrado será igual al texto original y toda la operación será un fracaso. Si el generado de claves de flujo expulsa un patrón repetido de 16 bits, el algoritmo será un simple XOR con una seguridad insignificante, debido que en periodos determinado, el proceso de cifrado generará operaciones repetitivas, condicionando este al sistema como muy vulnerable a potenciales ataques informáticos. Si el generado de flujos de claves expulsa un flujo sin fin de bits aleatorios, se obtiene de una vez un bloque confiable de naturaleza pseudo - aleatoria. El generador de flujo de claves genera un flujo de bits que parece aleatorio, pero es realmente un flujo determinístico que puede ser perfectamente reproducido en tiempo de descifrado (Schneier, B.).

El Sistema GEHEIM fue implementado un generador de flujo de claves basado en un cambio de registro. Un ciclo de cambio de registro realizado en dos partes: un cambio de registro y una función de retroalimentación (ver figura 6). El registro cambiado en una secuencia de bits. Cada vez que un bit es necesario, todos los bits en el registro cambiado son desplazados, 1 bit a la derecha. A la izquierda nuevos bits son computados como función de otros bits en el registro. La salida del registro cambiado es 1 bit, generalmente el bit menos significante. El periodo de un registro cambiado es la longitud de la secuencia de salida antes de que comience a repetirse. En un LFSR (siglas en ingles para Registro cambiado por realimentación a la izquierda) de n bits puede ser una secuencia pseudo aleatoria de uno a 2(n – 1) bit de longitud antes de repetirse. En otras manos la función de realimentación es simplemente un XOR lógico de ciertos bits en el registro; la lista de esos bits es llamada la secuencia llave (Tap String) (SCHNEIER, B.).

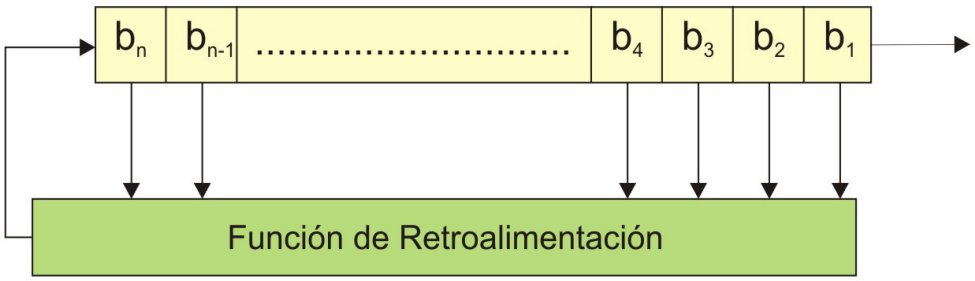

Figura 6. Ciclo de cambio de registro (GOLIC, J., Dawson, E., Clark, A., Millan, W., Penna, L. y Simpson, L).

El esquema aplicado para el LFSR en el sistema GEHEIM toma 128 bits surgidos de la llave-stego como un arreglo de palabras el cual es la longitud del LFSR, con la posición de cada bit en las palabras representando un LFSR diferente, entonces cada bit en la secuencia llave es operada por una función de XOR lógico con la salida del generador y reemplazado con la salida de este, transformándose en un nuevo bit más a la izquierda. Normalmente esta operación enmarcada en el estudio de las teorías de números se llama configuración de Galois.Un esquema de ésta puede verse en la siguiente figura.

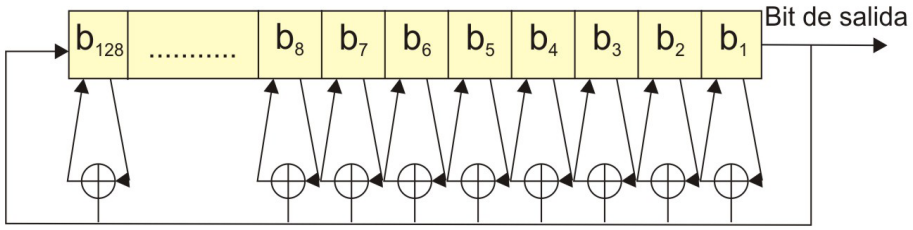

Figura 7. LFSR de Galois (GOLIC, J., Dawson, E., Clark, A., Millan, W., Penna, L. y Simpson, L.)

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Otra referencia es el generador de flujo de claves LILI-128 (GOLIC, J., Dawson, E., Clark, A., Millan, W., Penna, L. y Simpson, L.) el cual es un cifrador de flujo sincrónico basado en LFSR con una llave de 128 bits. Este produce secuencias de salida con propiedades probables con respecto a los requerimientos criptográficos básicos anteriormente descritos, tales como: mensaje original, clave, algoritmos de cifrado y descifrado, también proporciona seguridad contra los ataques criptoanalíticos comúnmente conocidos como: obtención del contenido del mensaje, análisis del tráfico, suplantación de identidad y repetición. (Westfeld A. y Pfitzmann A)

El generador de flujos de claves LILI-128 usa dos LFSR's binarios y dos funciones para generar secuencias de flujos de clave binarias pseudo aleatorias. La estructura del generador de flujo de claves LILI está ilustrada en la figura 8. Los componentes del generador de flujos de clave pueden ser agrupados en dos subsistemas basados en las funciones que realizan: control de reloj y generación de datos. El LSFR para el subsistema de control de reloj está regularmente sincronizado. La salida de este subsistema es una secuencia de enteros los cuales controlan la sincronización del LFSR con respecto al subsistema de generación de datos (Golic, J., Dawson, E., Clark, A., Millan, W., Penna, L. y Simpson, L.).

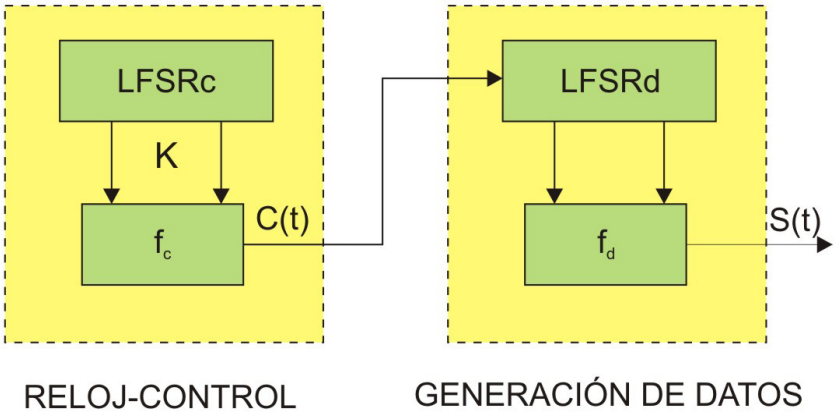

Figura 8. Generador de flujo de claves LILI-128 (GOLLMANN, D.).

El generador de flujo de claves de GEHEIM fue implementado de forma similar al LILI-128, pero se incluyó una modificación en el LFSR y el reloj (Gollmann, D.).

La salida binaria es usada con dos propósitos:

> Alimentar un segundo generador de flujos de clave del cual se obtendrá la secuencia de pixeles de la imagen que serán visitados para la integración de la data
>
> El resto de la cadena de salida es operada por un XOR lógico por cada bit de los datos. El cifrado obtenido es almacenado en una matriz bidimensional donde posteriormente se manipularan cambiando filas por columnas.

Aunque la codificación por bit de mínima significancia es extremadamente sensible a cualquier tipo de filtrado o manipulación de la imagen stego, fue tomada como método de integración en este trabajo.

Una imagen digital consiste en una matriz de valores de color e intensidad. En una típica imagen en escala de grises, son usados 8 bits/pixel. En una típica imagen a full color existen 24 bits/pixel, 8 asignados a cada componente de color. Las técnicas de esteganografia simples integran los bits del mensaje directamente en el plano del bit menos significativo de la cubierta de la imagen en una secuencia determinística. El modulando del bit menos significativo no resulta en una diferencia perceptible al humano porque la amplitud del cambio es mínima.

El método antes mencionado se desarrolla cuando el usuario ya ha seleccionado el LOGO (técnica de marca de agua visible) como soporte a la cubierta. Una vez que el logo es integrado en la imagen se inicia el proceso de incrustación de los datos. Realizado bajo una rutina cíclica, este último proceso determina el orden en el que serán visitados los pixeles en la imagen y puede ser comparado con la escalera que desciende de cualquier edificio, la cual toma como limite el último pixel a la derecha de la imagen.

En el proceso contrario para recuperar el mensaje oculto es necesario introducir en el sistema la clave stego numérica empleada en el proceso de integración así como el siego, es decir la imagen con la data cifrada incrustada. Con esto será nuevamente activado el correspondiente generador de flujo de clave, permitiendo obtener el texto de datos original y la imagen con su respectivo logo denotando autentificación. Este proceso es posible porque se ha implementado un reloj regular en el generador de flujo, que permite el orden pseudo-aleatorio.

Resultados

Los métodos esteganográficos usados en el diseño del sistema GEHEIM prueban una recuperación de los mensajes incrustado, con preservación de la integridad de los mismos. El sistema esteganográfico puede resistir una variedad de ataques estándares. Adicionalmente GEHEIM es amigable con el usuario y confiable para ocultar información. Cuando se comparan diferentes técnicas de ocultamiento, las siguientes restricciones y características son deseables.

Debe ser muy poco perceptible

Puede ser directamente codificado en el medio, tanto en la cabecera como en la cubierta.

Puede incluir códigos de corrección de errores desde la manipulación de la cubierta del medio a menudo problemas con la integridad de datos.

Puede ser auto-sincronizado o arbitrariamente re-entrante. Esto significa que si sólo una parte de la cubierta del medio está disponible, la información oculta en esa parte puede ser extraída.

Adicionalmente GEHEIM valida aspectos como:

El texto a ser codificado tiene una dimensión mayor a la imagen.

La clave es no numérica

La imagen seleccionada no es en escala de grises o está en formato BMP.

Si no hay mensaje a integrar.

Si no se ha seleccionado una imagen de cubierta para integrar los datos.

Si no se selecciona una imagen PNG en el proceso de recodificación.

Si no se introduce la clave numérica correcta en el proceso de descodificación.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Conclusión

GEHEIM confirma que mediante la combinación de operaciones determinísticas y no determinísticas se obtiene un sistema robusto con alta seguridad.

En adición al seguro mecanismo de integración, fue agregado al software GEHEIM una marca de identificación única para el stego que será transmitido, el cual es mostrado como una opción para el usuario. Esta marca de agua visible es uno de los factores que ofrece una gran confidencialidad y robustez al sistema puesto que si bien poseen como requisitos ser fácilmente discretas se caracterizan a su vez por ser muy difíciles de eliminar y susceptibles de ser insertadas de forma consistente en lotes de imágenes muy diferentes.

La inserción de marcas de agua está muy relacionada con la esteganografia, por lo cual es una técnica que está basada en el disimular (para ocultar) la presencia de un mensaje secreto. Con los métodos esteganográficos la información a ser ocultada no se relacionada con su "cubierta" mientras que la marca de agua puede ser considerada como un atributo de la "cubierta", ofreciendo información adicional.

Bibliografía

Delfs H. y Knebl H., "Introduction to Cryptography: Principles and Applications" Springer-Verlag, Berlin Heidelberg, 2002.

Fridrich J., Du R. y Long M., "Steganalysis of LSB Encoding in Color Images", [en línea], International Conference on Multimedia and Expo (ICME). New York City, USA, 2000. <http://dde.binghamton.edu/publications.php> [cunsultado: 27 de febrero de 2008]

Golic J., Dawson E., Clark A., Millan W., Penna L. y Simpson, L., "The LILI-128 Keystream Generator", Information security Research Centre, Queensland University of Technology, Brisbane, Australia.

_____, Dawson E., Clark A., Millan W., Penna L. & Simpson L., [en línea] <http://www.isrc.qut.edu.au/resources/lili/> [consultado: 27 de febrero de 2008].

Gollmann D., "Pseudo random properties of cascade connections of clock controlled shift register", Springer-Verlag Lecture Notes in Computer Science, Vol 209, 1985, pp. 93-98.

_____, "On the Randomness of Chambers and Gollmann Keystream Generator", IEICE Trans. Fundamentals, Vol. E84-A. No.1, 2001.

Lin, E. y Delp E., "A Review of Data Hiding in Digital Images", Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering Purdue University, West lafayatte, Indiana.

Lucena M., "Criptografía y Seguridad en Computadores", Departamento de Tecnología de la Información, Universidad de Jaen, España, 1999.

Pfitzmann B., "Information Hiding Terminology - First international workshop", Processings Lecture notes in computer science, vol 1147, Berlin: Springer, 1996.

Schneider B., "Applied Cryptography: Protocols, Algorithms and Source Code in C", John Wiley & Sons, 1995.

Sharp T., "An Implementation of key-Based digital Signal Steganography", Springer-Verlag Lecture Notes in Computer Science, Vol. 2137, 2001, pp. 13-26.

Stalllings W, "Fundamentos de Seguridad en Redes. Aplicaciones y Estándares". Segunda edición. Pearson Educaction, S.A., Madrid, 2004

Westfield A. y Pfitzmann A., "Attacks on Steganographic Systems", Springer-Verlag Lecture Notes in Computer Science, Vol. 1768, 2000.

Zöllner J., Federrath H., Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G. y Wolf G., "Modeling the Security of Steganographic Systems". Springer-Verlag Lecture Notes in Computer Sciente, Vol. 1525, 1998.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079