**Universidad de Granada**

*DEPARTAMENTO DE ÁLGEBRA*

Criptografía

**Esteganografía**

**Autores**: Alexander Moreno Borrego

Carlos Jesus Fernandez Basso

**Correos:** [alexmobo@correo.ugr.es](mailto:alexmobo@correo.ugr.es)

[karloos@correo.ugr.es](mailto:karloos@correo.ugr.es)

**DNI:** 39906263-K

75927137-C

**Profesor**:

Contenido

[Introducción 3](#_Toc355128343)

[¿Qué es la esteganografía? 3](#_Toc355128344)

[Terminología básica 3](#_Toc355128345)

[Esteganografía clásica (historia) 3](#_Toc355128346)

[Esteganografía moderna 3](#_Toc355128347)

[Conclusiones 3](#_Toc355128348)

[Bibliografía 3](#_Toc355128349)

[Chang, F., Dean, J., Ghe 3](#_Toc355128350)

Introducción

¿Qué es la esteganografía?

El termino esteganografía viene del griego *στεγανος* (steganos): cubierto u oculto, y *γραφος* (graphos): escritura.

A diferencia de la criptografía, que transforma el mensaje original para que nadie más que el receptor puede hacer la transformación inversa y entenderlo, la esteganografía oculta el mensaje original para que no pueda verse a simple vista pero no lo transforma de ninguna manera.

Estos mensajes se escribían, en claro a través de un canal encubierto no encriptado, dentro de otros, llamados portadores, de manera que no se percibiera si existencia. Se pretendía, incluso, que el propio hecho de la comunicación pasara inadvertido.

Terminología básica

El conjunto de componentes necesarios que permiten llevar a cabo la comunicación esteganográfica se denomina **esquema esteganográfico**.

* El **portador** es todo aquel conjunto de datos que es susceptible de ser alterado para incorporarle el mensaje que queremos mantener en secreto.
* Un **mensaje-legítimo** es el mensaje transportado por el portador.
* Se llama **mensaje esteganográfico** al mensaje que queremos mantener en secreto y queremos esconder dentro del portador.
* **Estego-algoritmo** es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del mensaje que queremos mantener en secreto en el portador.
* La acción de ocultar el mensaje dentro del portador se denomina **embeber**.
* **Estego-mensaje** al resultado de embeber el mensaje esteganográfico dentro del portador.
* La acción de la recuperación, a partir del estego-mensaje, del mensaje oculto esteganográfico se denomina **extraer**.
* El emisor es también llamado **embebedor** y el receptor **extractor**.
* Se llama **esteganalista** o **estegoanalista** a la persona que intenta determinar la existencia o ausencia de un mensaje esteganográfico. Basta con determinar la existencia. Es el que hace estegoanálisis.
* Los **canales de selección** consisten en canales adicionales al portador utilizado para embeber donde se comunica qué posiciones del portador se utilizan para la comunicación esteganográfica.
* Las **clases de equivalencia** corresponden a pares de elementos del portador utilizado que tienen una interpretación semántica equivalente en la comunicación legítima, pero el uso de un elemento u otro tiene un significado acordado en la comunicación esteganográfica.

Esteganografía clásica (historia)

Esteganografía moderna

Conclusiones

Bibliografía