



CRIPTOGRAFÍA Y SEGURIDAD

TRABAJO PRÁCTICO N°2

Secreto Compartido en Imágenes con Esteganografía

Autores:

Pablo Ballesty - 49359

Nicolás Magni - 48008

11 de junio de 2012

Resumen

El objetivo del presente informe es detallar las decisiones tomadas durante el diseño y la implementación del Trabajo Práctico. Así también, se presentan los resultados obtenidos a partir de las imágenes que envió la cátedra y se realiza un análisis de los mismos. Se detallan las dificultades encontradas, y las soluciones propuestas. También se presentan conclusiones y posibles extensiones del algoritmo.

1. Introducción

El Trabajo Práctico consiste en la implementación de un algoritmo de secreto compartido, aplicado a imágenes. Los algoritmos de secreto compartido, consisten en ocultar información sensible, la cual llamaremos *el secreto*, utilizando n claves, de las cuales, para la recuperación del secreto, serán necesarias k (con $k \leq n$).

Como en este caso, las claves son imágenes, al momento de generar las mismas, se utiliza una técnica de *esteganografía* con el fin de que el ojo humano no note, que se trata de claves.

El algoritmo que se utiliza en el trabajo se extrajo de la publicación *“Improvements in Geometry-Based Secret Image Sharing Approach with Steganography”* realizada por Mustafá Ulutas, Vasif V. Nabiyev y Guzin Ulutas, de la Universidad de Karadeniz, Turquía.

2. Desarrollo

La implementación del algoritmo no resulta difícil de implementar, sin embargo, precisa de cuidado en ciertos aspectos, para obtener resultados exitosos. A continuación, se detallan las dificultades que presenta el algoritmo, y como fueron resueltas en la práctica.

2.1. Sistemas compatibles determinados

2.2. Validación de la distribución