

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

Кафедра телекоммуникаций и информационных технологий

ВЯТКИН
Данила Артурович

**КРИПТОГРАФИЧЕСКОЕ КОДИРОВАНИЕ СООБЩЕНИЙ
ПРИ ИХ СТЕГАНОГРАФИЧЕСКИМ СОКРЫТИИ**

Аннотация к дипломной работе

Научный руководитель – кандидат техн. наук,
профессор В.С. Садов

Минск, 2023

РЕФЕРАТ

Дипломная работа: 85 с., 92 рис., 6 табл., 14 источников, 1 прил.

СТЕГАНОГРАФИЯ, СТЕГОАНАЛИЗ ИЗОБРАЖЕНИЯ,
СТЕГАНОГРАФИЯ LSB, СТЕГОКОНТЕЙНЕР, БИТОВЫЕ ПЛОСКОСТИ,
КРИПТОГРАФИЯ, МЕТОДЫ ШИФРОВАНИЯ, ПОТОЧНЫЕ ШИФРЫ,
БЛОЧНЫЕ ШИФРЫ

Объект исследования – десктопное приложение для шифрования и сокрытия информации в цифровых изображениях.

Цель работы заключается в оценке результатов совместного использования стеганографического сокрытия в паре с криптографическим кодированием.

Работа посвящена исследованию процессам стеганографического встраивания информации в изображения. В ходе работы проведен статистический и визуальный анализ младших битовых плоскостей в заполненном, не заполненном контейнере; как при зашифрованном, так и незашифрованном встроенном сообщении. Оценено значение шифрования встраиваемого сообщения в обнаружении стеганографических модификаций в изображениях-контейнерах.

Установлено, что при шифровании сообщения улучшаются статические характеристики битовой плоскости, что уменьшает вероятность обнаружения сокрытия.

Создано соответствующее программное обеспечение, необходимое для выполнения исследований.

РЭФЕРАТ

Дыпломная праца: 85 с., 92 мал., 6 табл., 14 крыніц, 1 дад.

СТЕГАНОГРАФІЯ, СТЕГААНАЛІЗ МАЛЮНКА, СТЕГАНОГРАФІЯ LSB, СТЕГОКАНТЕЙНЕР, БІТАЎ ПЛОСКАСЦІ, КРЫПТАГРАФІЯ, МЕТАДЫ ШЫФРАВАННЯ, СТРУМЕНЕВЫЯ ШЫФРЫ, БЛОКАВЫЯ ШЫФРЫ

Аб'ект даследавання – дэсктопнае прыкладанне для шыфравання і ўтойвання інфармацыі ў лічбавых малюнках.

Мэта работы заключаецца ў ацэнцы вынікаў сумеснага выкарыстання стеганографічнага ўтойвання ў пары з крыптаграфічным кадаваннем.

Праца прысвечана даследаванню працэсам стеганографічнага ўбудавання інфармацыі ў малюнкi. У ходзе работы праведзены статыстычны і візуальны аналіз размеркавання біт малодшых бітавых плоскасцяў ў запоўненым, ня запоўненым кантэйнеры; як пры зашыфраваным, так і незашыфраваным убудаваным паведамленнем. Ацэнена значэнне шыфравання ўбудаванай паведамленні ў выяўленне стеганографічных мадыфікацый ў малюнках-кантэйнерах.

Устаноўлена, што пры шыфраванні паведамлення павялічваюцца статычныя характарыстыкі бітавай плоскасці, што памяншае верагоднасць выяўлення ўтойвання.

Створана адпаведнае праграмнае забеспячэнне, неабходнае для выканання даследаванняў.

ABSTRACT

Thesis: 85 p., 92 fig., 6 tab., 14 sources, 1 appl.

STEGANOGRAPHY, IMAGE STEGANALYSIS, LSB STEGANOGRAPHY, STEGOCONTAINER, BIT PLANES, CRYPTOGRAPHY, ENCRYPTION METHODS, STREAM CIPHERS, BLOCK CIPHERS

The object of research is a desktop application for encrypting and hiding information in digital images.

The purpose of the work is to evaluate the results of the joint use of steganographic concealment paired with cryptographic coding.

The work is devoted to the study of the processes of steganographic embedding of information in images. In the course of the work, a statistical and visual analysis of the lower bit planes in a filled, unfilled container was carried out; both with an encrypted and unencrypted embedded message. The value of embedded message encryption in detecting steganographic modifications in container images is estimated.

It is established that when encrypting a message, the static characteristics of the bit plane are improved, which reduces the probability of detection of concealment.

The corresponding software necessary for carrying out research has been created.