МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информатики и компьютерных систем

Аннотация к дипломной работе

«Влияние криптографического кодирования сообщений на качество стеганографического процесса»

Новоженина Александра Витальевна

Научный руководитель — профессор Садов В. С.

Минск, 2022

РЕФЕРАТ

Дипломная работа: 53 страницы, 41 рисунок, 12 использованных источников, 2 приложения.

СТЕГАНОГРАФИЯ, СТЕГАНОАНАЛИЗ, КРИПТОГРАФИЯ, ШИФРОВАНИЕ ИЗОБРАЖЕНИЙ, ГАММИРОВАНИЕ, LSB

Объект исследования – изображения формата BMP.

Цель работы – исследования результатов встраивания в изображения-контейнеры незашифрованных и зашифрованных изображений-сообщений.

Методы исследования – визуальный анализ, атака по критерию Хи-квадрат.

В исследовании используются два метода стеганоанализа: визуальная атака и статистическая атака. Эксперимент проводится над изображениями различных жанров в формате BMP.

В ходе исследования битовых плоскостей контейнеров на наличие в них зашумленных участков было выявлено, что наиболее пригодными битовыми плоскостями для встраивания являются три первые битовые плоскости. В результате эксперимента по встраиванию было выявлено, что изменение старших битовых плоскостей приводит к появлению визуальных артефактов в изображении, которые легко определяются человеческим глазом.

Для проведения эксперимента по изучению влияния шифрования на качество стеганографического встраивания исходные сообщения были зашифрованы при помощи метода гаммирования. Данное преобразование позволило, во-первых, увеличить стойкость стеганографичсекой системы и время, которое необходимо будет затратить злоумышленнику для извлечения секретного сообщения, а во-вторых, помогло улучшить степень встраивания за счет зашумливания, а, следовательно, и органичного встраивания сообщения.

Также были проанализированы результаты последовательного и случайного встраивания методом LSB. Было выявлено, что наиболее незаметным оказалось случайное встраивание, но размер сообщения при этом оказывается мал. А для последовательного встраивания сообщений больших размеров лучше всего подошли спутниковые снимки и изображения природы, но при этом обязательно шифрование сообщения.

РЭФЕРАТ

Дыпломная работа: 53 старонкі, 41 малюнак, 12 выкарыстаных крыніц, 2 прыкладання.

СТЭГАНАГРАФІЯ, СТЭГАНААНАЛІЗ, КРЫПТАГРАФІЯ, ШЫФРАВАННЕ МАЛЮНКАЎ, ГАМІРАВАННЕ, LSB

Аб'ект даследавання – выявы фармату BMP.

Мэта работы – даследаванне вынікаў убудавання ў выявы-кантэйнеры незашыфраваных і зашыфраваных малюнкаў-паведамленняў.

Метады даследавання – візуальны аналіз, атака па крытэрыі Хі-квадрат.

У даследаванні выкарыстоўваюцца два метаду стеганоанализа: візуальная атака і статыстычная атака. Эксперымент праводзіцца над выявамі розных жанраў у фармаце BMP.

Падчас даследавання бітавых плоскасцяў кантэйнераў на наяўнасць у іх зашумленных участкаў было выяўлена, што найболей прыдатнымі бітавымі плоскасцямі для ўбудавання з'яўляюцца тры першыя бітавыя плоскасці. У выніку эксперыменту па ўбудаванні было выяўлена, што змена старэйшых бітавых плоскасцяў прыводзіць да з'яўлення візуальных артэфактаў у малюнку, якія лёгка вызначаюцца чалавечым вокам.

Для правядзення эксперыменту па вывучэнні ўплыву шыфравання на якасць стэганаграфічнага ўбудавання зыходныя паведамленні былі зашыфраваны пры дапамозе метаду гаміравання. Дадзенае пераўтварэнне дазволіла, па-першае, павялічыць устойлівасць стеганаграфічнай сістэмы і час, якое неабходна будзе затраціць зламысніку для вымання сакрэтнага паведамлення, а па-другое, дапамагло палепшыць ступень убудавання за рахунак зашумливания, а такім чынам, і арганічнага ўбудавання паведамлення.

Таксама былі прааналізаваны вынікі паслядоўнага і выпадковага ўбудавання метадам LSB. Было выяўлена, што найбольш незаўважным аказалася выпадковае ўбудаванне, але памер паведамлення пры гэтым аказваецца малы. А для паслядоўнага ўбудавання паведамленняў вялікіх памераў лепш за ўсё падышлі спадарожнікавыя здымкі і выявы прыроды, але пры гэтым абавязкова шыфраванне паведамлення.

ABSTRACT

Diploma thesis: 53 pages, 41 drawings, 12 sources, 2 appendices.

STEGANOGRAPHY, STEGANALYSIS, CRYPTOGRAPHY, IMAGE ENCRYPTION, GAMMING, LSB

The object of research – BMP images.

Objective – research the results of embedding unencrypted and encrypted message in containers, which are images.

The methods – visual analysis, Chi-square attack.

The study uses two methods of steganoanalysis: visual attack and statistical attack. The experiment is carried out on images of various genres in the BMP format.

In the course of studying the bit planes of containers for the presence of noisy areas in them, it was found that the first three bit planes are the most suitable bit planes for embedding. As a result of the embedding experiment, it was revealed that changing the higher bit planes leads to the appearance of visual artifacts in the image, which are easily determined by the human eye.

To conduct an experiment to study the effect of encryption on the quality of steganographic embedding, the original messages were encrypted using the gamma method. This transformation made it possible, firstly, to increase the resistance of the steganographic system and the time that an attacker would need to spend to extract the secret message, and secondly, it helped to improve the degree of embedding due to noise, and, consequently, the organic embedding of the message.

The results of sequential and random embedding by the LSB method were also analyzed. It was found that the most imperceptible was random embedding, but the size of the message is small. And for consistent embedding of messages of large sizes, satellite images and images of nature are best suited, but encryption of the message is required.