МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА
ФІЗИКО-ЕНЕРГЕТИЧНИЙ ФАКУЛЬТЕТ
Кафедра інформаційних технологій в фізико-енергетичних системах

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи
за освітньо-кваліфікаційним рівнем магістр

«Гістограмний стегоаналіз зображень»

Виконав: студент 2 курсу, групи НФ-63
Волобуєв Є. В.
Спеціальність: 105 Прикладна фізика та наноматеріали
Освітня програма: Прикладна фізика енергетичних систем
Керівник: доцент Лісін Д. О.
Рецензент

Харків - 2018 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В.Н.Каразіна

Факультет фізико-енергетичний

Кафедра інформаційних технологій в фізико-енергетичних системах

Рівень вищої освіти (освітньо-кваліфікаційний рівень) магістр

Спеціальність 105 прикладна фізика та наноматеріали

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ проф.Немченко К.Е.

підпис

“____” _____20___року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ

Волобуєв Євгеній Володимирович

1. Тема роботи «Гістограмний стегоаналіз зображень»
керівник роботи доцент Лісін Д. О.
затверджені наказом по університету від “ 24 ” жовтня 2018 року № 0210-05/1991

2. Строк подання студентом роботи 30.11.2018 року

3. Перелік питань, які необхідно вирішити: розробити імовірнісний метод гістограмного стегоаналізу, який в просторової формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом, який реалізується за допомогою програми «MATLAB».

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір теми, узгодження, закріплення за кафедрою
2	Робота над літературою та іншими джерелами
3	Затвердження теми на кафедрі
4	Написання вступу до роботи та першого розділу
5	Написання другого розділу
6	Написання третього розділу
7	Завершення написання дипломної роботи(висновки і література)
8	Подача науковому керівнику, доробка зауважень
9	Відгук, рецензія, підготовка до захисту
10	Попередній захист на кафедрі
11	Захист

5. Дата видачі завдання 12 вересня 2018 року

Студент _____ **Волобуєв Є. В.**

підпис

Керівник роботи _____ **Лісін Д. О.**

підпис

РЕФЕРАТ

Магістерська робота виконана студентом Волобуєвим Євгенієм Володимировичем на тему: «Гістограмний стегоаналіз зображень».

Дипломна робота представлена на 39 сторінках, складається з вступу, 3 розділів та висновків, містить 6 малюнків, 1 додаток, список використаних джерел, 35 джерел.

Мета дипломної роботи – розробити імовірнісний метод гістограмного стегоаналізу, який в просторової формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом, який реалізується за допомогою програми «MATLAB».

Об’єктом дослідження дипломної роботи є пошук стеганографічних вкладень за допомогою гістограмного стегоаналізу.

Предметом дипломної роботи є розробка імовірнісного методу стегоаналіза, який в просторової формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом.

В даній дипломній роботі ознайомилися з роботою програми «MATLAB» та методами реалізацій програмного продукту, на основі вивченого було написано програму, яка за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом, практично використали функції для стегоаналіза послідовного вкладення.

КЛЮЧОВІ СЛОВА: СТЕГОАНАЛІЗ, ГІСТОГРАМА, MATLAB, ХІ-КВАДРАТ, СТЕГАНОГРАФІЯ, МЕТОД, СТАТИСТИЧНА, ЗОБРАЖЕННЯ, СКРИПТ, АЛГОРИТМ, ЗАСІБ, JPEG, КОЛІР, ФУНКЦІЯ, КОМПОНЕНТА, АНАЛІЗ.

ABSTRACT

Master's work performed by Volobuiev Evgeniy Vladimirovich on the topic: «Histogram steganaliz image».

The thesis is presented on 39 pages, consists of an introduction, 3 chapters and a conclusion, includes 6 drawings,1 application, list of references, 35 sources.

The aim of the thesis is to develop a probabilistic method of histogram stegoanalysis, which in the spatial form of image representation using the statistical Chi-square criterion searches for steganographic investments made by a certain algorithm, which is implemented using the MATLAB program.

The object of the research of the thesis is the search for steganographic attachments using histogram steganalysis.

The subject of the thesis is the development of a probabilistic method of stegoanalysis, which in the spatial form of image representation using the statistical Chi-square criterion searches for steganographic investments made by a certain algorithm.

In this thesis, we familiarized ourselves with the work of the MATLAB program and the methods of software product instances. Based on the studied program, a program was written that, using the Chi-square statistical criterion, searches for steganographic investments made by a specific algorithm, practically used functions for steganalysis of sequential investment.

KEYWORDS: STEGANALYSIS, HISTOGRAM, MATLAB, CHI-SQUARE, STEGANOGRAPHY, METHOD, STATISTICAL, IMAGE, SCRIPT, ALGORITHM, MEANS, JPEG, COLOR, FUNCTION, COMPONENT, ANALYSIS.

РЕФЕРАТ

Магистерская работа выполнена студентом Волобуевым Евгением Владимировичем на тему: «Гистограммный стегоанализ изображения».

Дипломная работа представлена на 39 страницах, состоит из введения, 3 глав и заключения, включает 6 рисунков, 1 приложение, список использованных источников, 35 источников.

Цель дипломной работы - разработать вероятностный метод гистограммного стегоанализа, который в пространственной форме представления изображения с помощью статистического критерия Хи-квадрат ищет стеганографические вложения, сделанные определенным алгоритмом, который реализуется с помощью программы «MATLAB».

Объектом исследования дипломной работы является поиск стеганографических вложений с помощью гистограммного стегоанализа.

Предметом дипломной работы является разработка вероятностного метода стегоанализа, который в пространственной форме представления изображения с помощью статистического критерия Хи-квадрат ищет стеганографические вложения, сделанные определенным алгоритмом.

В данной дипломной работе ознакомились с работой программы «MATLAB» и методами экземпляров программного продукта, на основе изученного было написано программу, которая с помощью статистического критерия Хи-квадрат ищет стеганографические вложения, сделанные определенным алгоритмом, практически использовали функции для стегоанализа последовательного вложения.

КЛЮЧЕВЫЕ СЛОВА: СТЕГОАНАЛИЗ, ГИСТОГРАММА, MATLAB, ХИ-КВАДРАТ, СТЕГАНОГРАФИЯ, МЕТОД, СТАТИСТИЧНЫЙ, ИЗОБРАЖЕНИЕ, СКРИПТ, АЛГОРИТМ, СРЕДСТВО, JPEG, ЦВЕТ, ФУНКЦИЯ, КОМПОНЕНТА, АНАЛИЗ.

ЗМІСТ

ВСТУП **7**

1 ЛІТЕРАТУРНИЙ ОГЛЯД **9**

1.1. Середовище розробки MATLAB 9

1.2. Стеганографія 11

1.3. Класифікація методів стегоаналіза 16

2 РОЗРОБКА СТРУКТУРИ СИСТЕМИ **19**

2.1. Предметна область розробки методу 19

2.2. Гістограмний статистичний стегоаналіз. Практична реалізація 21

3 MATLAB СКРИПТ ДЛЯ ГІСТОГРАМНОГО СТАТИСТИЧНОГО СТЕГОАНАЛІЗА **23**

3.1. Опис створеної програмної системи 23

ВИСНОВОК **31**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **32**

ДОДАТОК А……..**36**

ВСТУП

З розвитком інформаційних технологій і перекладом основних потоків інформації в цифрову форму, набула актуальності проблема забезпечення інформаційної безпеки. При цьому єдиним вихідом для збереження конфіденційності та цілісності інформації є створення комплексної системи захисту інформації. Важливу роль у забезпеченні інформаційної безпеки відіграє підсистема управління доступом. Однак стандартні методи і засоби контролю інформації на даний момент орієнтовані на перевірку лише обмеженого числа явних атрибутів і сучасні засоби приховування інформації - цифрова стеганографія дозволяє долати існуючі системи контролю доступу до мережевих ресурсів. Приховані канали передачі інформації дозволяють подолати обмеження стандартних засобів контролю трафіку. Інформація може бути прихована в будь-якому форматі даних, який дозволений до передачі даних користувачем в зовнішню мережу, в тому числі в певних полях мережевих пакетів, запитуваних посиланнях та інших об'єктах. В якості носія прихованої інформації в цифровій стеганографії можуть бути використані оцифровані аналогові сигнали, тексти документів, виконані код, пакети мережевого трафіку і т.д. зі збереженням семантики. Таким чином, принципово можлива організація прихованих каналів витоку при наявності будь-якої надмірності в вихідному трафіку. Застосування стеганографічних засобів для приховання інформації в файлах, що передаються потім на сайти мультимедіа-контенту і файлообмінні сервери дозволяє приховано організовувати і координувати проведення різного роду протиправних дій. При отриманні доступу організованими злочинними угрупованнями до передавальних засобів стільникового та стаціонарного телефонного зв'язку, супутниковим каналам зв'язку, телебачення і радіомовлення можлива організація прихованих каналів передачі інформації глобальних масштабів. У цих умовах особливо актуальною стає задача виявлення прихованої інформації, її вилучення та знищення, а також аналіз стійкості існуючих

стеганографічних алгоритмів, і розробка нових методів виявлення прихованої інформації - стегоаналіза.

Об’єктом дослідження дипломної роботи є пошук стеганографічних вкладень за допомогою гістограмного стегоаналізу.

Предметом дипломної роботи є розробка імовірнісного методу стегоаналіза, який в просторової формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом.

Мета дипломної роботи – розробити імовірнісний метод гістограмного стегоаналізу, який в просторової формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом, який реалізується за допомогою програми «MATLAB». Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Ознайомитися з роботою програми «MATLAB» та методи реалізацій програмного продукту;
2. Написати програму, яка за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом;
3. Практично використати функції для стегоаналіза послідовного вкладення.

1 ЛІТЕРАТУРНИЙ ОГЛЯД

1.1. Середовище розробки MATLAB

MATLAB - один з найпотужніших на сьогоднішній день пакетів обробки даних. Назва розшифровується як Matrix Laboratory. Матрична Лабораторія, якщо по-російськи. Можливості програми покривають практично всі області математики. Так, користуючись Матлаб, Ви зможете:

Виробляти всілякі операції над матрицями, вирішувати лінійні рівняння, працювати з векторами;

Обчислювати корені многочленів будь-якого ступеня, виробляти операції над многочленами, диференціювати, екстраполювати і інтерполювати криві, будувати графіки будь-яких функцій;

Проводити статистичний аналіз даних з використанням цифрової фільтрації, статистичної регресії;

Вирішувати диференціальні рівняння. У приватних похідних, лінійних, нелінійних, з граничними умовами - не важливо, МАТЛАБ все вирішить;

Виконувати операції цілочисельний арифметики. Крім усього цього можливості MATLAB дозволяють візуалізувати дані аж до побудови тривимірних графіків і створення анімованих роликів. Крім передбачених виробником можливостей і функцій існує величезна кількість інструментів МАТЛАБ, написаних просто ентузіастами або іншими компаніями.

MATLAB - це мова програмування, що використовується безпосередньо при роботі з програмою. Не будемо вдаватися в подробиці, скажемо тільки, що програми, написані на мові MATLAB, бувають двох видів: функції і скрипти. Основний робочий файл програми - М-файл. Це нескінченний текстовий файл, і саме в ньому відбувається безпосередньо програмування обчислень. До речі, нехай Вас не лякає це слово - для того, щоб працювати в MATLAB, зовсім не потрібно бути професійним програмістом.

М-файли поділяються на:

‘М-сценарії. М-сценарій - найпростіший тип М-файлу, у якого відсутні вхідні і вихідні аргументи. Цей файл використовують для автоматизації багаторазово повторюваних обчислень.

М-функції. М-функції - це М-файли, що допускають наявність вхідних і вихідних аргументів.

Щоб показати, як відбувається робота в MATLAB, наведемо нижче приклад створення функції в Матлаб. Ця функція буде обчислювати середнє значення вектора.

```
function y = average (x)
% AVERAGE Середнє значення елементів вектора.
% AVERAGE (X), де X - вектор.
% Якщо вхідний аргумент не є вектором, генерується помилка.
 [M, n] = size (x);
 if (~ ((m == 1) | (n == 1)) | (m == 1 & n == 1))
 error ( 'Вхідний масив повинен бути вектором')
 end
y = sum (x) / length (x); % Власне обчислення
```

Рядок визначення функції повідомляє системі MATLAB, що файл є М-функцією, а також визначає список вхідних аргументів. Так, рядок визначення функції average має вигляд:

function y = average (x)

де:

function - ключове слово, яке визначає М-функцію;

y - вихідний аргумент;

average - ім'я функції;

x - вхідний аргумент.

Отже, щоб написати функцію в Матлаб, необхідно пам'ятати, що кожна функція в системі MATLAB містить рядок визначення функції, подібну наведеної. В даний час MATLAB, з одного боку, дуже популярний серед фахівців багатьох наукових і інженерних галузей. З іншого боку, можливість

роботи з великими матрицями робить MATLAB незамінним інструментом фінансових аналітиків, що дозволяє вирішити набагато більше завдань, ніж, наприклад, відомий всім Excel. Детальніше про те, як зробити презентацію на комп'ютері ви можете прочитати в оглядовій статті.

Недоліки роботи з MATLAB

Які є труднощі в роботі з MATLAB? Труднощі, мабуть, всього одна. Але фундаментальна. Щоб повністю розкрити можливості MATLAB і з легкістю вирішувати поставлені перед Вами завдання, доведеться попітніти і спочатку розібратися з самим MATLAB (як створити файл, як створити функцію і ін.). А це не так просто, бо потужність і широкі можливості вимагають жертв.

1.2. Стеганографія

Серед дисциплін, пов'язаних із захистом інформації від несанкціонованого доступу, в останнє десятиліття впевнено заявила про себе стеганографія - наука про приховування даних. На відміну від криптографії, при приховуванні є невідомим не тільки зміст даних, але і сам факт їх наявності.

Методи стеганографії використовувалися задовго до криптографічних методів: згадаймо класичні приклади з головою раба, симпатичним чорнилом, мікроточки, згадаємо твори ченця Трітеміуса і т.п. У XX столітті були розроблені теоретичні основи криптографії і широко використовуються практичні схеми, витіснили з застосування стеганографічні способи. Однак все розвивається по спіралі. Повсюдна комп'ютеризація, успіхи в області цифрового відео, аудіо в кінці минулого століття привели до появи нового напряму захисту інформації - цифровий стеганографії, в основі якої лежать методи цифрової обробки сигналів. Спільною рисою мультимедійної інформації є можливість її передачі не точно, а з деякими спотвореннями, непомітними для людського ока. Саме ця особливість і дозволяє впроваджувати приховану інформацію, з іншого боку, вона ж використовується в алгоритмах стиснення повідомлень з втратами.

Можливості стеганографії

Безпечне впровадження інформації використовується не тільки для її прихованої передачі, але і в інших цілях. Серед додатків стеганографії можна виділити:

• стійкість перед перешкодами аутентифікацію мультимедійної інформації, її імітозащіти;

• контроль цілісності даних;

• захист прав власника мультимедійної інформації;

• відстеження поширення інформації.

Ці додатки стеганографії зазвичай називають технологіями цифрових водяних знаків - по аналогії з водяними знаками цінних паперів. Більшість відкритих досліджень по стеганографії присвячено саме технологіям цифрових водяних знаків. Наприклад, в останні роки ряд фірм-виробників мультимедійного контенту фінансує дослідження в цій області, сподіваючись покласти край піратству. Також виступають в якості спонсора розробок і ВПС США, чий інтерес лежить в області перешкодостійкою аутентифікації і імітозащіти зображень аерофотозйомки.

Як і у всіх сферах життя, кожна дія породжує протидію. Для стеганографії такою протидією є стегоаналіз. Шляхом ретельного вивчення використовуваного стеганографічного алгоритму і змінених з його допомогою даних стегоаналітик намагається знайти вразливість алгоритму або протоколу його застосування, за допомогою якої з'являється можливість організації атаки на стегосистему, в результаті якої застосування стегосистеми не досягає своєї мети.

Завдання стегоаналіза розрізняються залежно від області застосування. Розглянемо тільки стегоаналіз систем прихованої передачі повідомлень.

Для аналізу стегосістем прихованої передачі найбільш актуальним завданням є визначення факту наявності прихованої інформації з достатнім ступенем впевненості. У деяких роботах під завданнями стегоаналіза

розуміється також виділення прихованого повідомлення і його дешифрування. На наш погляд, це невірно.

Звичайно, завжди існує ймовірність помилкового визначення прихованого повідомлення в "порожньому" зображенні - ймовірність помилкової тривоги. Тоді практично значимий показник ефективності для порівняння алгоритмів стегоаналіза можна сформулювати так: "мінімізація ймовірності помилкової тривоги при ймовірності виявлення прихованого повідомлення не нижче заданої".

Наприклад, якщо замовника задовольняє ймовірність виявлення 80% (тобто 8 Стего з 10 будуть визначені як Стего), то алгоритм, що забезпечує можливість виявлення 80% при ймовірності помилкової тривоги 10%, буде з точки зору цього показника ефективніше алгоритму, що забезпечує ймовірності 95/15%.

З іншого боку, замовник може задати допустиму величину ймовірності помилкової тривоги. Тоді показник ефективності можна сформулювати так: "максимізація ймовірності виявлення прихованого повідомлення при ймовірності помилкової тривоги не вище заданої". З точки зору цього показника другий алгоритм буде краще першого. Можливо також використання комплексного показника ефективності: "максимізація різниці між вірогідністю першого і другого роду".

Основи стегоаналіза систем прихованої передачі

За аналогією з криптографією можливі інформаційно-теоретичний та теоретико-сложностний підходи до стегоаналізу. Перший підхід має на увазі необмежені обчислювальні і тимчасові витрати для приховує і для аналітика. При другому підході враховується обмеженість ресурсів, і мова йде про умовно стійкою стегосистеми. На практиці все стегосистеми можна вважати умовно стійкими, що як раз і відкриває можливість для проведення стегоаналіза.

Більшість методів стегоаналіза засноване на виявленні відхилення спостерігається мультимедійної інформації (Стего) від його очікуваної моделі.

Клас статистичних методів стегоаналіза використовує безліч статистичних характеристик, таких як: оцінка ентропії, коефіцієнти кореляції, ймовірність появи і залежності між елементами послідовностей, умовні розподілу, розрізнення розподілів за критерієм Хі-квадрат і багато інших. Найпростіші тести оцінюють кореляційні залежності елементів контейнерів, в які можуть впроваджуватися приховувані повідомлення.

Загальний недолік статистичних методів стегоаналіза полягає в тому, що побудова математичної моделі "природного зображення", або "природного аудиосигнала", є виключно складною і досі не вирішеним завданням. Можна сказати, що між приховує інформацію і стегоаналітіком відбувається змагання: хто з них володіє кращою моделлю контейнера, той і переможе в протиборстві.

Відомі методи стегоаналіза, спрямовані проти конкретних стегоалгоритму або працюють для конкретних форматів даних. Наприклад, методи стегоаналіза зображень, в яких проводиться впровадження в найменший значущий біт, досліджують розподіл цих бітів, а також кореляційні зв'язки між ними і більш значущими бітами.

Методи стегоаналіза зображень, стиснутих за алгоритмом JPEG, засновані на виявленні неможливих для порожніх JPEG-контейнерів конфігурацій коефіцієнтів дискретного косинусного перетворення. Специфічні методи стегоаналіза, як правило, більш ефективні, ніж універсальні методи для конкретного алгоритму впровадження, на який вони "налаштовані".

Стегоаналіз в світі

Як відомо, в США діє закон DMCA, що забороняє застосування програмного забезпечення, призначеного для злому алгоритмів захисту (згадайте історію з Дмитром Скляровим). Так ось, в деяких штатах США вже прийнятий, а в інших поки що розглядається ряд законів, сукупність яких отримала найменування SDMCA - "Super" DMCA. Противники цих законів справедливо говорять про те, що їх дія ставить під сумнів законність використання навіть міжмережевих екранів і анонімайзерів при роботі в

Мережі. Одним з "постраждалих" від SDMCA став мічіганец Нільс Прово, чиї дослідження в області стегоаналіза стали незаконними, і він був змушений помістити свої результати на сервер в Нідерландах. Н. Прово і П. Аніменом був розроблений алгоритм стегоаналіза (в основному орієнтований на пошук модифікацій молодших біт) і в 2001 р проаналізовано 3 млн зображень Інтернету. Ні в одному з них не було знайдено слідів стеганографії.

З іншого боку, в схожому дослідженні Дж. Келінана і Д. Кеміка з Піттсбурга (2003 рік) було знайдено багато підозрілих зображень (20 000 з 200 000 перевірених). Автор книги по стеганографії Ерік Коул взагалі знайшов 1/3 підозрілих картинок (правда, у читачів його книги рівень знань даного експерта може викликати сумніви).

В даний час в світі існує багато вільно розповсюджуваних програм стеганографії, так що застосувати їх може будь-хто. Є і програмні засоби протидії. Наприклад, компанією Wetstone в ході виконуваної за контрактом з ВПС США роботи було розроблено і в даний час продається ($ 1995) Засіб стегоаналіза StegoSuite. Звичайно, можна скористатися і безкоштовними засобами стегоаналіза - Out-Guess, StegDetect і т.п.

Перспективи

Цифрова стеганографія / стегоаналіза є поки ще дуже молодий дисципліною, але вже можна констатувати факт народження нової області досліджень серед наук про захист інформації. Причому назва цієї міждисциплінарної науки поки ще не стабілізувався. Так, в США в даний час отримав ходіння термін Intelligence and Security Informatics, і IEEE з 2005 р проводить конференції з аналогічною назвою. У проекті ECRYPT, спонсируемом Європейською комісією, зазначається виняткова важливість досліджень в цьому напрямку і пропонується термін "Secure Media" .На наш погляд, актуальною є не тільки розробка технічних аспектів стеганографії, а й надання їй законного статусу, а також нормативне регулювання стеганографії в Росії .

1.3. Класифікація методів стегоаналіза

Як і будь-яке складне явище, стегоаналітичні методи можна класифікувати за багатьма критеріями.

У російськомовному середовищі ще немає усталеної традиції написання слова стегоаналіза. Якщо виходити зі світової практики то правильніше писати стегоаналіза від англійського варіанту написання (steganalysis). Однак якщо слідувати написання популярних вітчизняних книг з даної тематики: Конахович Г.Ф., Пузиренко А.Ю. "Комп'ютерна стеганографія. Теорія і практика" або В. Г. Грібунін, І. Н. кайданів, І. В. туринців "Цифрова стеганографія", ... слід писати стеганоаналіз. Спираючись на кількість результатів пошуку того і іншого варіантів (пошук проводився в google і yandex) більш уживаний в інтернет співтоваристві термін стегоаналіза.

За широтою аналізу контейнерів, в яких ховаються дані, методи стегоаналіза діляться на:

методи, призначені для виявлення даних, прихованих певним алгоритмом;

методи "сліпого" розпізнавання.

Звичайно ж, вузькоспрямовані методи, тобто орієнтовані на певний алгоритм, мають кращі показники знаходження прихованих даних. Їх недоліком є те, що в разі невеликої зміни алгоритму приховування, шукані дані вже можуть не виявлятися. Перевагою "сліпих" або ж універсальних методів є широкий спектр стеганографічних алгоритмів приховування, над якими вони можуть працювати. Разом з тим ці методи потребують "навчанні", від якості якого залежать їх стегоаналітіческіе можливості.

За впливом на файл-контейнер, який містить приховані дані, стегоаналітіческіе методи діляться на:

методи пасивного стегоаналіза, які визначають наявність / відсутність прихованих даних в стегоконтейнер, або що визначають алгоритм, за яким відбувалося вбудовування.

методи активного стегоаналіза, які визначають довжину вбудованого документа, його розташування, деякі параметри алгоритму вбудовування, а також вилучають приховану інформацію.

По об'єкту пошуку в стегоконтейнер стегоаналітичних методів можна розділити на такі типи:

сигнатурні методи, побудовані на пошуку в стеганограмах так званих "відбитків пальців" (fingerprints), - фрагментів коду, які залишають після своєї роботи стеганографічні програми;

імовірнісні методи, які засновані на аналізі імовірнісних показників, характерних для стегосообщеній.

До методів сигнатурного типу відносяться:

візуальна атака на стегосистеми;

аналіз відповідності формату даних (пошук зайвих включень).

Так в певних видах зображень виявляються досить тісні зв'язки всіх біт зображення. Використовуючи для таких зображень програми-фільтри, можна побачити вбудовану інформацію, яка порушує наявні залежності. Візуальна атака повністю ґрунтується на здатності аналізувати людським зором зорові образи і виявляти істотні розбіжності в порівнюваних зображеннях.

Прикладами "зайвої" інформації є додаткові байти інформації, які дописують в кінець графічного файлу, або дублювання квітів, в палітрі.

До імовірнісним методам можна віднести:

аналіз статистики Хі-квадрат;

метод дослідження статистичних моделей вищого порядку.

Ідея статистичного стегоаналіза полягає в порівнянні теоретичного розподілу найменш значущих біт малюнка з фактичним розподілом цих же біт в цьому ж малюнку. При цьому міра подібності теоретичного і фактичного розподілу є мірою достовірності вбудовування прихованої інформації. Статистичні моделі вищого порядку грунтуються, наприклад, на вейвлет-декомпозиції зображень. За результатами декомпозиції будується "характеристичний" вектор, який використовується для диференціювання

зображень з прихованими даними і «чистих». Найкращі результати модель дає після "тренування" на деякому наборі зображень-контейнерів і відповідних їм стегозображень.

За формою подання досліджуваного зображення, методи стегоаналіза можна розділити на:

методи, які аналізують зображення безпосередньо, тобто в просторової форми подання;

методи, які аналізують частотні форми представлення зображення, тобто після переведення його до частотної формі за допомогою дискретного перетворення косинуса, або вейвлет-перетворення.

По виду математичних інструментів, які використовуються для визначення факту вбудовування, розрізняють:

методи, які використовують статистичні критерії згоди (Хі-квадрат);

методи, які застосовують заходи подібності цифровий сукупності;

метод визначення JPEG- сумісності.

2 РОЗРОБКА СТРУКТУРИ СИСТЕМИ

2.1. Предметна область розробки методу

Стегоаналіз - це протидія стеганографії, як криптоаналіз - це протидія криптографії. Основна мета стеганографії - приховати факт передачі даних. Отже, основна мета стегоаналіза - виявити факт приховування передачі даних. Розглянемо метод виявлення послідовного вбудовування в LSB на прикладі зображення формату BMP. Існує думка, що Дороговкази в LSB зображень є випадковими. Насправді це не так! Хоча людське око і не помітить змін зображення при зміні останнього біта, статистичні параметри зображення будуть змінені. Перед приховуванням дані зазвичай архівуються (для зменшення обсягу) або шифруються (для забезпечення додаткової стійкості повідомлення при попаданні в чужі руки). Це робить біти даних дуже близькими до випадкових. Послідовне вбудовування такої інформації замінить LSB зображення випадковими бітами. І це можна виявити.

Для прикладу візьмемо одну колірну компоненту повнокольорового зображення BMP і на ній покажемо процес відшукання вбудовування. Яскравість колірної компоненти може приймати значення від 0 до 255. У двійковій системі числення - від 0000 0000 до 1111 1111.

Розглянемо пари:

0000 0000 <-> 0000 0001;

0000 0010 <-> 0000 0011;

...

1111 1100 <-> 1111 1101;

1111 1110 <-> 1111 1111.

Дані числа розрізняються між собою тільки в LSB (виділені жирним). Таких пар для колірної компоненти BMP зображення: 256/2 = 128

У разі стеганографічного вбудовування тобто заміни LSB на випадкову послідовність, кількість пікселів в парах вирівняється. Гістограма стане сходинками (по два сусідніх значення яскравості см.рис.2.1.)

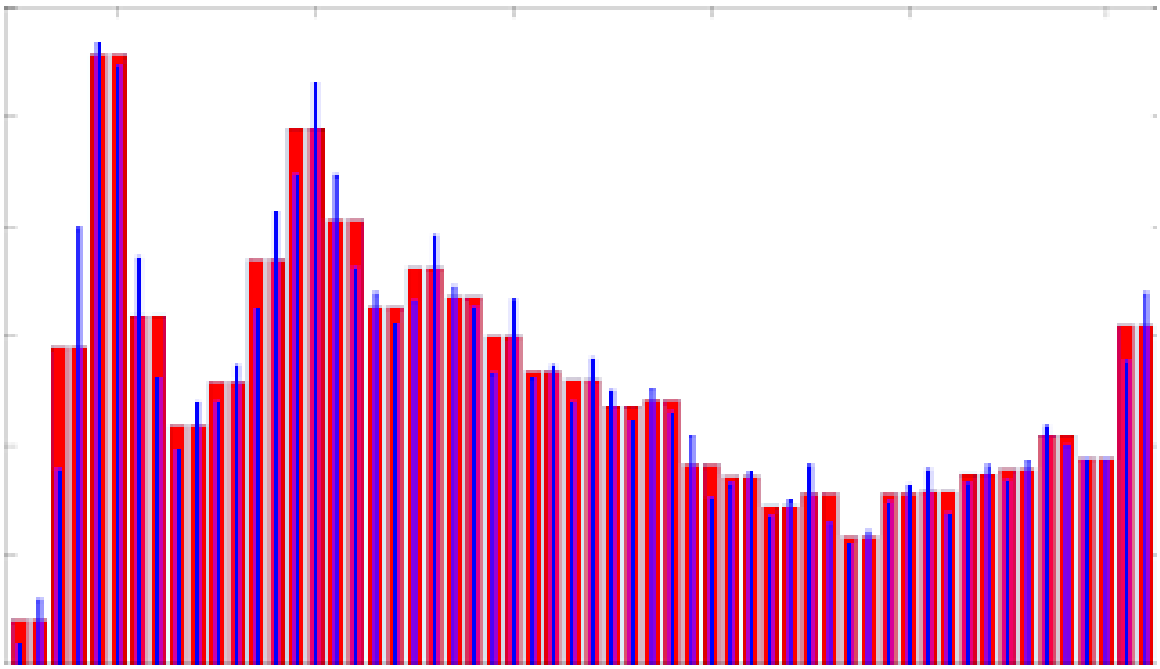


Рис. 2.1. Сусідні значення яскравості

На рис. 2.2. синім кольором позначена гістограма зображення без вбудовування, а червоним - гістограма того ж зображення після вбудовування заархівірованих даних замість останнього шару. Порівняння двох гістограм і дає можливість стегоаналізу послідовно приховуваних біт.

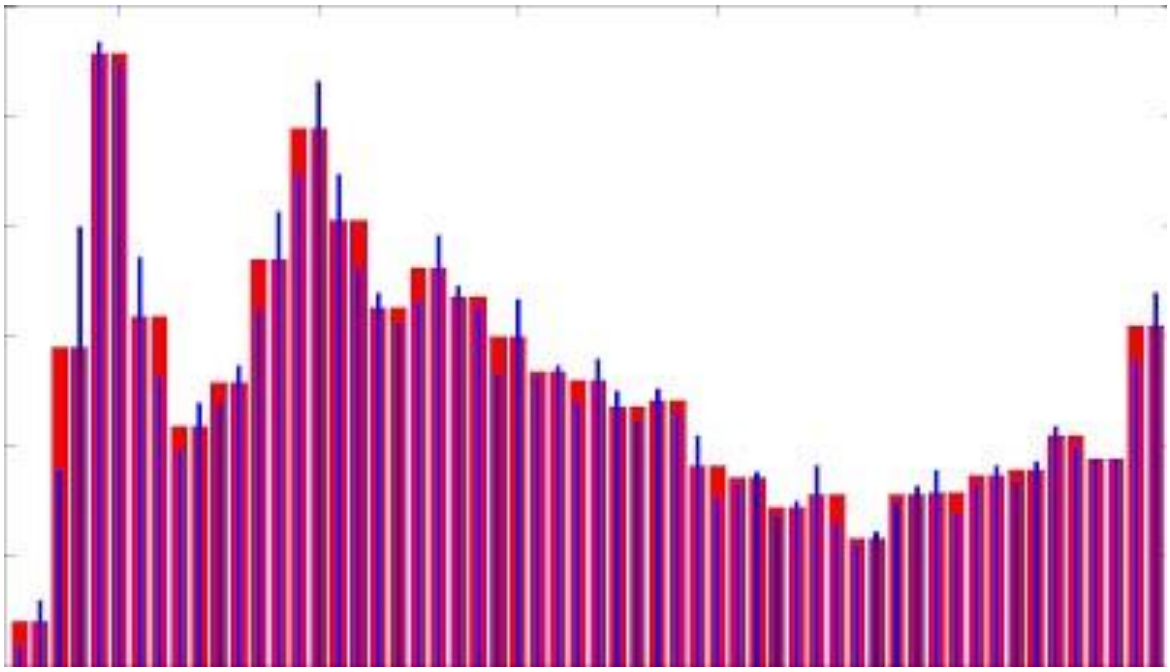


Рис. 2.2. Гістограма порожнього і заповненого зображень

2.2. Гістограмний статистичний стегоаналіз. Практична реалізація

У російськомовному інтернеті неможливо знайти хоч яку-небудь працюючу програму для стегоаналіза. Однак, теоретичні та практичні (комерційні) розробки в світі зробили крок вельми далеко.

Не будемо відставати і створимо наш власний скрипт для Matlab, який буде відшукувати послідовне вкладення. (Вбудувати вкладення можна, за допомогою раніше описаного методу). Метод виявлення послідовного вбудовування будемо розробляти для 24 бітного BMP зображення.

За наведеною раніше класифікації, описуваний метод стегоаналіза відноситься до імовірнісного методу, який в просторової формі подання зображення за допомогою статистичного критерію Хі квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом.

Загальний опис алгоритму:

1. Розбиваємо зображення на колірні компоненти.
2. Кожну кольорову компоненту розбиваємо на непересічні прямокутні блоки достатньої величини (Що таке «достатня величина» вимагає особливого дослідження).
3. Для кожного блоку будуємо емпіричну гистограмму яскравості. (Емпіричний - заснований на досвіді, вивченні фактів, що спирається на безпосереднє спостереження, експеримент.) На малюнку 1 гістограма позначена синім кольором.
4. Для кожного блоку будуємо теоретичну гистограмму на основі емпіричної. Для побудови теоретичної гістограми знайдемо середнє арифметичне кількості пікселів з сусідніми яркостями.

Сусідніми будуть яскравості 0 <-> 1. 2 <-> 3 ... 254 <-> 255, або в двійковій системі числення:

0000 0000 <-> 0000 0001;

0000 0010 <-> 0000 0011;

...

1111 1110 <-> 1111 1111.

Теоретична гістограма спостерігається при встановленні даних в кожен біт (піксель) колірної компоненти. На малюнку 1 - позначена червоним кольором. Можна сказати, що при встановленні кількість пікселів в сусідніх парах розподілено рівновірогідно.

5. Для кожного блоку порівняємо схожість теоретичної і емпіричної гістограм за допомогою статистики Хі квадрат (Пірсона). Якщо теоретична і емпірична гістограми розрізняються несуттєво, то ймовірно, що в кожен піксель колірної компоненти досліджуваного блоку вбудована прихована інформація. Обчислюємо значення статистики для перевіряємого блоку колірної компоненти:

$$X^2_{empirich} = \sum_{i=1}^{N} \frac{(Empiich_i - Theor_i)^2}{Theor_i} \quad (2.1)$$

Теоретична і емпірична гістограми вважаються схожими, якщо отримане емпіричне значення статистики Хі квадрат менше теоретичного значення статистики Хі квадрат при заданому рівні значущості а і кількості ступенів свободи k-1.

$$X^2_{empirich} < X^2_{\alpha}(\kappa - 1) \quad (2.2)$$

Якщо така нерівність справедлива, то ми виявили вбудовування в перевіряємий блок.

3 MATLAB СКРИПТ ДЛЯ ГІСТОГРАМНОГО СТАТИСТИЧНОГО СТЕГОАНАЛІЗА

3.1. Опис створеної програмної системи

Даний скрипт є функцією, яку можна викликати з командного рядка MATLAB.

На вхід функції подаються: адреса аналізованого зображення, розмір непересічних прямокутних блоків по горизонталі і вертикалі, рівень значущості a (рекомендується 0.9).

На виході отримуємо зображення трьох колірних компонент: red1_out, green1_out, blue1_out.

Сірим кольором показані місця, де сусідні пари яркостей мають рівновіроятний розподіл, тобто передбачається вбудовування. Червоним, зеленим і синім кольором, відповідно, позначені місця колірних компонент, де вбудовування немає.

```
function [red1_out,green1_out,blue1_out] =
histogr_chit2_steganalys(IMG_in,step1X,step1Y,Probb);
% pirson_Xi_2_Analiz
```

Читаємо картинку з файлу, розкладаємо її на колірні компоненти, обчислюємо її розмір.

```
Image = imread(IMG_in,'bmp');
Red1 = Image (:,:,1);
Green1= Image (:,:,2);
Blue1 = Image (:,:,3);
[Pheight,Pwidth] = size(Red1);
```

Створюємо індексні змінні для блоків, на які буде розбито зображення.

```
a_ind_X = 1:step1X:Pwidth;
 a_ind_Y = 1:step1Y:Pheight;
```

Підраховуємо, скільки блоків по горизонталі і по вертикалі у нас буде.

```
countX = size(a_ind_X,2);
```

```
countY = size(a_ind_Y,2);
```

Додаємо до зображення широку «межу» з пікселів, щоб крайні блоки були обрізані межою зображення.

```
brdrdd_Red1 = [Red1;Red1((count1Y-1)*step1Y:-1:(count1Y-2)*step1Y+1,:)];
brdrdd_Red1 = [brdrdd_Red1,brdrdd_Red1(:,(count1X-1)*step1X:-1:(count1X-2)*step1X+1)];
brdrdd_Green1 = [Green1; Green1((count1Y-1)*step1Y:-1:(count1Y-2)*step1Y+1,:)];
brdrdd_Green1 = [brdrdd_Green1, brdrdd_Green1(:,(count1X-1)*step1X:-1:(count1X-2)*step1X+1)];
brdrdd_Blue1 = [Blue1;Blue1((count1Y-1)*step1Y:-1:(count1Y-2)*step1Y+1,:)];
brdrdd_Blue1 = [brdrdd_Blue1,brdrdd_Blue1(:,(count1X-1)*step1X:-1:(count1X-2)*step1X+1)];
```

Формуємо зображення з доданими межами.

```
brdrdd_ Image (:,:,1) = brdrdd_Red1(:,:);
brdrdd_ Image (:,:,2) = brdrdd_Green1(:,:);
brdrdd_ Image (:,:,3) = brdrdd_Blue1(:,:);
```

Задамо розміри масивів для зберігання гістограми, що спостерігається значення Xi квадрат - ArrayRealn і теоретичного значення Xi квадрат - ArrayTheor:

```
HistogrTheor=zeros(1,256);
ArrayRealn = zeros(size(a_ind_Y,2),size(a_ind_X,2));
ArrayTheor = zeros(size(a_ind_Y,2),size(a_ind_X,2));
```

У циклі будемо звертатися послідовно до першої, другої і третьої колірної компонентів.

```
for Z = 1:3
IMG = brdrdd_ Image (:,:,Z);
```

Для кожної колірної компоненти послідовно переберемо все, досліджувані на предмет вбудовування, блоки. Для кожного блоку визначимо емпіричне і

теоретичне значення Xi квадрат (процес досить докладно прокоментований в самому коді).

```
for Y = 1:step1Y:Pheight
for X = 1:step1X:Pwidth
areaXY = IMG(Y:Y+step1Y,X:X+step1X);
% побудова емпіричної гістограми
% результат – горизонтальний вектор #HistogrEmpirich#
HistogrEmpirich = imhist(areaXY);
% транспонування вектора #HistogrEmpirich#
% результат – горизонтальний вектор #HistogrEmpirich#
HistogrEmpirich = transpose(HistogrEmpirich);
% побудова теоретичної гістограми #HistogrTheor#
% результат – горизонтальний вектор #HistogrTheor#
k = 1:2:256;
 HistogrTheor(k) = (HistogrEmpirich (k)+HistogrEmpirich (k+1))/2;
 HistogrTheor(k+1) = (HistogrEmpirich (k)+HistogrEmpirich (k+1))/2;
%**************************************************************
% розрахунок вірогідностей емпіричної та теоретичної яркостей #VarTheor# #VarEmpirich#
% результат – горизонтальний #VarEmpirich# #VarTheor#
VarEmpirich = HistogrEmpirich;
VarTheor = HistogrTheor;
zero_ind = find(VarTheor <=20);
VarEmpirich (zero_ind) = [];
VarTheor(zero_ind) = [];
% розрахунок массива-сировини для розрахунку реального значення #Xi2#
% результат – горизонтальний вектор  #Xi2#
Xi2 = ((VarEmpirich-VarTheor).^2)./VarTheor;
% видалення помилкових значень ділення на нуль з #Xi2#
```

```
Xi2 = Xi2(~isnan(Xi2));
%розрахунок реального значення #Xi2#
Xi2Realn = sum(Xi2);
% розрахунок табличного #Xi2#
Xi2Theor = chi2inv(Probb,size(Xi2,2)-1);
% формування наглядних массивів реального та табличного значення #Xi2#
 ArrayRealn((Y-1)/step1Y+1,(X-1)/step1X+1) = Xi2Realn;
 ArrayTheor((Y-1)/step1Y+1,(X-1)/step1X+1) = Xi2Teor;
 end;
 end;
```

Результати розрахунків статистик Хі квадрат занесемо до відповідних масивів для першої, другої і третьої колірних компонент. Масиви ArrayCompare зберігають логічні значення для кожної з аналізованих областей: «1» - вбудовування є, «0» - вбудовування немає.

```
 if (Z == 1)
 red1_ArrayRealn = ArrayRealn;
 red1_ArrayTheor = ArrayTheor;
 red1_ArrayCompare = uint8(red1_ArrayRealn
 end;
 if (Z == 2)
 green1_ArrayRealn = ArrayRealn;
 green1_ArrayTheor = ArrayTheor;
 green1_ArrayCompare = uint8(green1_ArrayRealn
 end;
 if (Z == 3)
 blue1_ArrayRealn = ArrayRealn./ArrayTeor;
 blue1_ArrayTheor = ArrayTheor./ArrayTheor;
 blue1_ArrayCompare = uint8(blue1_ArrayRealn
 end;
  end;
```

На даному етапі у нас вже є інформація про «забрудненість» блоків зображення вбудовуванням. Для зручності користувача покажемо дані блоки на зображенні.

У циклі перебираються всі аналізовані блоки для кожної компоненти. Якщо аналізований блок чистий, виводимо його «рідним» (червоним, зеленим або синім) для компоненти кольором. Якщо блок з вбудовуванням, виводимо його сірим кольором

```
for Y = 1:step1Y:Pheight
for X = 1:step1X:Pwidth
red1_out(Y:Y+stepY-1,X:X+stepX-1,1) = brdrdd_Red1(Y:Y+step1Y-
1,X:X+step1X-1);
red1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Red1Y:Y+step1Y-
1,X:X+step1X-1).*red_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
red1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Red1(Y:Y+step1Y-
1,X:X+step1X-1).*red1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
green1_out(Y:Y+step1Y-1,X:X+step1X-1,1) = brdrdd_Green(Y:Y+step1Y-
1,X:X+step1X-1).*green1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
green1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Green1(Y:Y+step1Y-
1,X:X+stepX-1);
green1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Green1(Y:Y+step1Y-
1,X:X+step1X-1).*green1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
blue1_out(Y:Y+step1Y-1,X:X+step1X-1,1) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1).*blue1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
blue1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1).*blue1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
blue1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1);
 end;
 end;
```

Позбавляємося від широкої межі, доданої для роботи з крайніми блоками.

```
red1_out = red1_out(1:Pheight,1:Pwidth,:);
green1_out = green1_out(1:Pheight,1:Pwidth,:);
blue1_out = blue1_out(1:Pheight,1:Pwidth,:);
```

На даному етапі функція вже сформувала змінні-зображення, на яких видно результати аналізу. Для зручності додамо висновок результатів на екран. За бажанням наступні три рядки можна закомментировать або видалити.

```
% figure;imagesc(red1_out);
%figure;imagesc(green1_out);
%figure;imagesc(blue1_out);
end;
```

3.2. Практичне використання функції для стегоаналіза послідовного вкладення

Коротко подивимося, як працює наша функція.

Для аналізу візьмемо зображення 'stego_murzik3.bmp', ширину і висоту блоку візьмемо в чверть розміру зображення, рівень значущості задамо 0.8:

```
[red1_out,green1_out,blue1_out] =
histogr_chit2_steganalys('stego_murzik3.bmp',512,512,0.8);
```

В результаті отримуємо такі (рис. 3.1.):

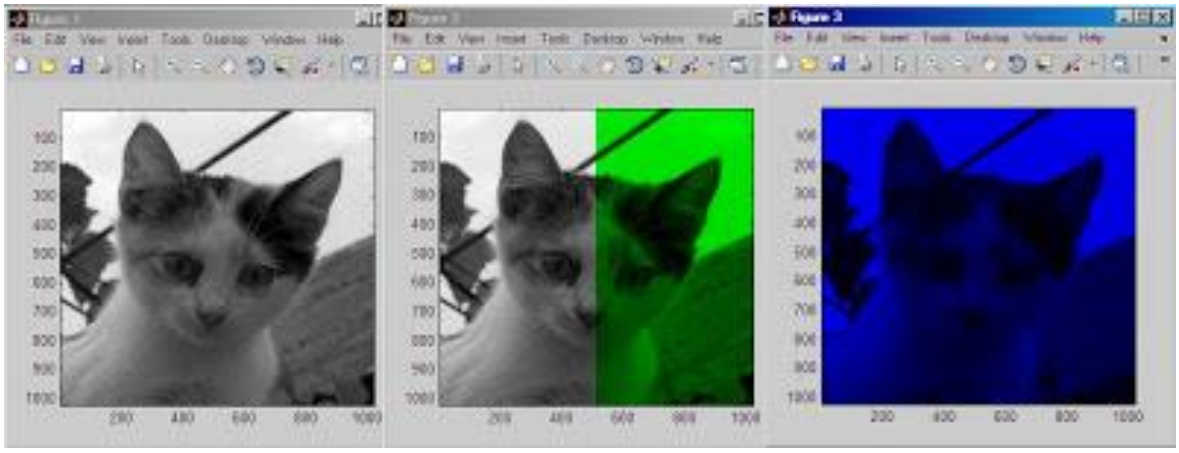


Рис. 3.1. Зображення заповнення зеленим і синім кольором

Червона компонента вся затемнена, що означає повне вбудовування в червону компоненту. Зелена компонента - зелена лише наполовину, що проявляє

області з вбудовуванням (сіра) і без вбудовування (зелена). Синя компонента показує відсутність вбудовування по всій площі.

Однак спробуємо зменшити розмір блоків, на які зображення розбивається для аналізу. Використовуємо блоки розміром 200x200 пікселів(рис.3.2.):

```
[red1_out,green1_out,blue1_out] =
histogr_chit2_steganalys('stego_murzik3.bmp',200,200,0.8);
```

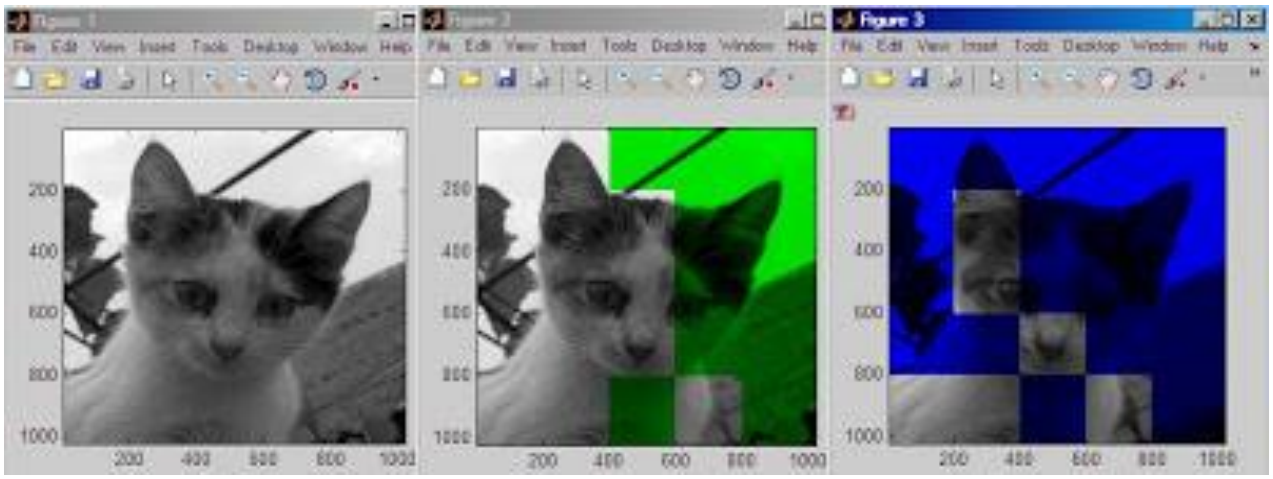


Рис. 3.2. Заповнення компонентами на зменшенні блоки

Як бачимо, в місцях визначених попереднім аналізом як чисті від вбудовування воно "з'явилося". Це говорить про важливість вибору розміру і форми блоків, на які розбивається для аналізу зображення.

Результат проходу вузькими вертикальними смужками 30x1023 на (рис. 3.3.):

```
[red1_out,green1_out,blue_out] =
histogr_chit2_steganalys('stego_murzik3.bmp',30,1023,0.8);
```

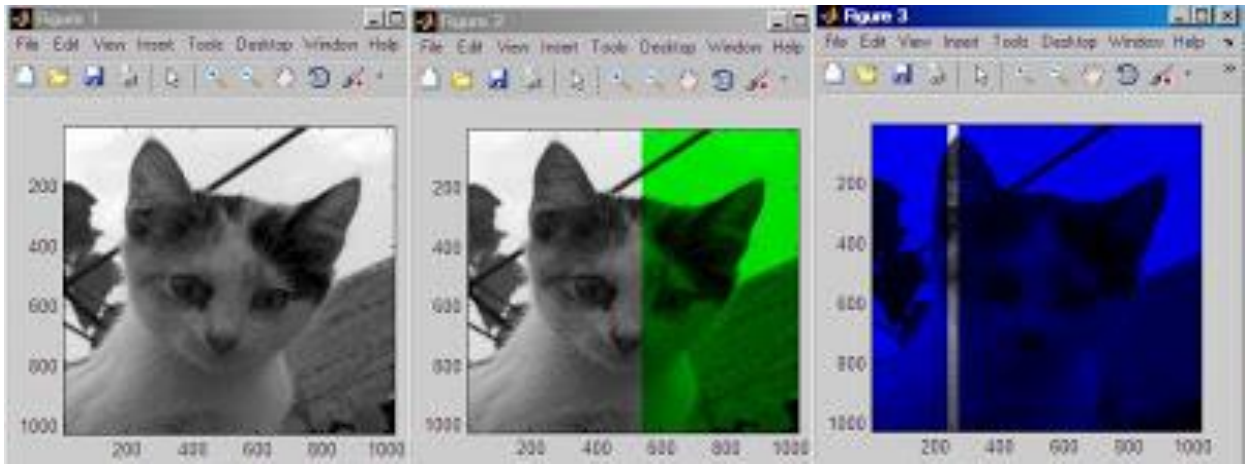


Рис. 3.3. Заповнення компонентами вузькими вертикальними смужками

Аналіз квадратиками 30x30 на (рис. 3.4.):

```
[red1_out,green1_out,blue1_out] =
histogr_chit2_steganalys('stego_murzik3.bmp',30,30,0.8);
```

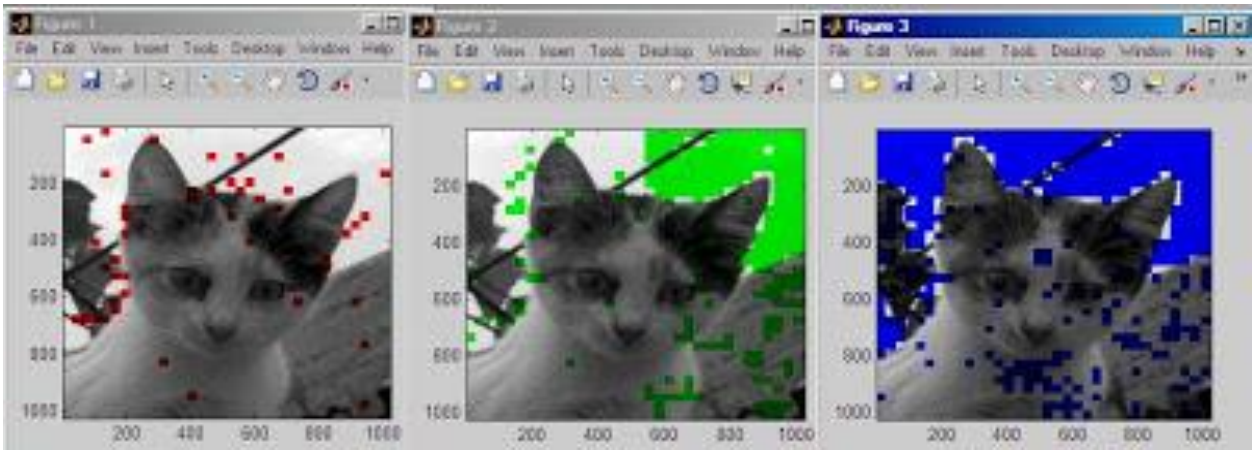


Рис. 3.4. Заповнення компонентами квадратиками 30x30

ВИСНОВОК

У результаті виконання дипломної роботи вирішена актуальна науково-практична задача - пошук стеганографічних вкладень за допомогою гістограмного стегоаналізу.

Була виконана задача розробки імовірнісного методу гістограмного стегоаналізу, який в просторовій формі подання зображення за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом, який реалізується за допомогою програми «MATLAB». Для досягнення поставленої мети вирішили наступні задачі:

1) Ознайомилися з роботою програми «MATLAB» та методами реалізацій програмного продукту;
2) Було написано програму, яка за допомогою статистичного критерію Хі-квадрат шукає стеганографічні вкладення, зроблені певним алгоритмом
3) Практично використали функції для стегоаналіза послідовного вкладення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Є.І. Хомяков, В.М. Федоров, Стеганографія даних за допомогою мовних повідомлень, - Таганрог, Збірник праць науково-практичної семінару «Інформаційна безпека-Південь Росії», 1999.
2. Федоров В.М. Рубльов Д.П. Використання методу зсуву фази для приховування даних в мовному сигналі Праці VI Всеросійській науковій конференції студентів і аспірантів "Технічна кібернетика, радіоелектроніка та системи управління", Таганрог, 2002.
3. Рубльов Д.П. Метод аналізу стеганосообщеній, заснований на кореляції точок зображення. печ. Зб. "Известия ТРТУ" Таганрог, 2003.
4. Рубльов Д.П. Метод приховування даних в аудіопотоки на основі фазового кодування. VII Всеросійська науково-технічна конференція «Підвищення ефективності засобів обробки інформації на базі математичного і машинного моделювання», Тамбов, 2004.
5. Рубльов Д.П. Макаревич О.Б., Федоров В.М. Метод вбудовування даних в аудиопоток на основі перетворення фазових складових. VII Міжнародна науково-практична конференція "Інформаційна безпека" -2005.
6. Хомяков Є.І., Федоров В.М., Макаревич О.Б. Стеганографія: застосування та виявлення. Збірник праць другого регіонального науково-практичної семінару "Інформаційна безпека Південь Росії", Таганрог, 28-30 червня 2000 р
7. Грібунін В.Г., кайдани І.М., туринці І.В. Цифрова стеганографія, М .: Солон-Прес, 2002.
8. Барсуков В.С., Романцов А.П. Оцінка рівня скритностімультімедійних стеганографічних каналів зберігання і передачі інформації .// Спеціальна техніка, 1999, № 6.
9. Макаревич О.Б., Федоров В.М. Рубльов Д.П. Виявлення прихованих повідомлень в зображеннях на основі вейвлет-декомпозиції Праці VII Міжнародної науково-практичної конференції "Інформаційна безпека" -2005.

10. Д.П.Рублёв, В.М Федоров, О.Б.Макаревіч Метод приховування даних в аудіофайл, інваріантний до стиснення сигналів VII Міжнародний симпозіум Інтелектуальні системи-2006.
11. Федоров В.М., Макаревич О.Б., Рубльов Д.П. Виявлення прихованих повідомлень в зображеннях на основі статистичних моделей вищих порядків. Праці VI Міжнародної науково-практичної конференції «Інформаційна безпека», Таганрог, 2004.
12. Рубльов Д.П. Федоров В.М., Макаревич О.Б. Виявлення прихованих закономірностей у бінарних послідовностей за допомогою нейронних мереж Матеріали другої міжнародної науково-практичної конференції
13. Інфокомунікаційні технології в науці і техніці "(Інфоком 2) Ставрополь-2006.
14. Метод стеганографії в зображеннях на основі біортогональних вейвлетов. Матеріали Третьої міжнародної конференції "Інформаційні системи і технології" (IST'2006), частина 1.
15. Воробйов В.І., Грібунін В.Г. Теорія і практика вейвлет-перетворення. ВУС, 1999. з 66-67.
16. Воробйов В.І., Грібунін В.Г. Теорія і практика вейвлет-перетворення. ВУС, 1999. с. 1-204.
17. Єжов А.А., Шумський С.А. Нейрокомпьютинг і його застосування в економіці і бізнесі. М .: МІФІ, 1998..
18. Д.П. Рубльов, В.М. Федоров, О.Б. Макаревич, Застосування нейронних мереж для стегоаналіза прихованих повідомлень в зображеннях. Інтелектуальні системи. Праці Сьомого міжнародного симпозіуму. -М .: русака, 2006.
19. Рубльов Д.П. Метод очищення мовних сигналів від імпульсних перешкод на основі адаптивного вирішального правила. Матеріали LI науково-технічної конференції, "Известия ТРТУ", Таганрог, 2005В
20. B. Pfitzmann, "Information Hiding Terminology". In R. Anderson, Information Hiding: first international workshop, Proceedings (Lecture notes in computer science; Vol. 1147), Berlin: Springer, 1996.

21. Ross J. Anderson, Fabien A.P. Petitcolas On The Limits of Steganography IEEE Journal of Selected Areas in Communications, May 1998, Special Issue on Copyright & Privacy Protection. ISSN 07338716.
22. Christian Cachin An Information-TFheoretic Model for Steganography In Proceedings of 2nd Workshop on Information Hiding (D. Aucsmith, ed.), Lecture Notes in Computer Science, Springer, 1998.
23. Frans M.J. Willems, Universal data compression and repetition times, IEEE Transactions on Information Theory 35 (1989), № 1.
24. J.Zollner, H.Federrath, H.Klimant, A.Pfitzmann, R.Piotraschke, A.Westfeld, G.Wicke, G.Wolf Modeling the security of steganographic systems, Proc. 2nd Workshop on Information Hiding, Apr 1998.
25. Sviatoslav Voloshynovskiy, Alexander Herrigel, Yuriy Rytsar and Thierry Pun Stego Wall: Blind statistical detection of hidden data. Proc. SPIE Vol. 4675.
26. Bender W. et al. "Techniques for data hiding", IBM Systems Journal, Vol. 35, 1996.
27. Aucsmith D., Ed. Information Hiding: Second InternationalWorkshop, vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.
28. Kuen Lee, Ling-Hwei Chen An Adaptive Image Steganographic Model Based on Minimum-Error НЗБ Replacement. International Conference on Parallel Processing, 1999, pp 363-370.
29. Jain A.K. Fundamentals of Digital Image Processing Prentice-Hall, Inc., Englewood Cliffs, NJ, 1989.
30. Marvel Lisa M. , Boncelet Charles G. Jr., and Retter Charles T. "Spread Spectrum Image Steganography", IEEE Transactions on Image Processing, 1999.
31. A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Lecture Notes in Computer Science, vol.1768, Springer-Verlag, Berlin, 2000.
32. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images State of the Art", Security and Watermarking of Multimedia Contents, 2002, vol. SPIE-4675.
33. S. Trivedi and R.Chandramouli Active Steganalysis of Sequential Steganography Multimedia Systems, SPIE conference California 5020 (2003), no. 13.

34.J. Fridrich, R. Du, M. Long Steganalysis of LSB encoding in color images // Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY, 2000.

35.J. Fridrich Reliable Detection of LSB Steganography in Grayscale and Color Images, with M. Goljan and R. Du, Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5,2001.

ДОДАТОК А

```
function [red1_out,green1_out,blue1_out] =
histogr_chit2_steganalys(IMG_in,step1X,step1Y,Probb);
% pirson_Xi_2_Analiz
Image = imread(IMG_in,'bmp');
  Red1 = Image (:,:,1);
  Green1= Image (:,:,2);
  Blue1 = Image (:,:,3);
  [Pheight,Pwidth] = size(Red1);
a_ind_X = 1:step1X:Pwidth;
  a_ind_Y = 1:step1Y:Pheight;
countX = size(a_ind_X,2);
  countY = size(a_ind_Y,2);
 brdrdd_Red1 = [Red1;Red1((count1Y-1)*step1Y:-1:(count1Y-2)*step1Y+1,:)];
   brdrdd_Red1 = [brdrdd_Red1,brdrdd_Red1(:,(count1X-1)*step1X:-1:(count1X-
 2)*step1X+1)];
 brdrdd_Green1 = [Green1; Green1((count1Y-1)*step1Y:-1:(count1Y-
 2)*step1Y+1,:)];
   brdrdd_Green1 = [brdrdd_Green1, brdrdd_Green1(:,(count1X-1)*step1X:-
 1:(count1X-2)*step1X+1)];
brdrdd_Blue1 = [Blue1;Blue1((count1Y-1)*step1Y:-1:(count1Y-2)*step1Y+1,:)];
  brdrdd_Blue1 = [brdrdd_Blue1,brdrdd_Blue1(:,(count1X-1)*step1X:-1:(count1X-
2)*step1X+1)];
brdrdd_ Image (:,:,1) = brdrdd_Red1(:,:);
  brdrdd_ Image (:,:,2) = brdrdd_Green1(:,:);
  brdrdd_ Image (:,:,3) = brdrdd_Blue1(:,:);
HistogrTheor=zeros(1,256);
  ArrayRealn = zeros(size(a_ind_Y,2),size(a_ind_X,2));
  ArrayTheor = zeros(size(a_ind_Y,2),size(a_ind_X,2));
for Z = 1:3
```

```
  IMG = brdrdd_ Image (:,:,Z);
for Y = 1:step1Y:Pheight
    for X = 1:step1X:Pwidth
areaXY = IMG(Y:Y+step1Y,X:X+step1X);
% побудова емпіричної гістограми
    % результат – горизонтальний вектор #HistogrEmpirich#
    HistogrEmpirich = imhist(areaXY);
% транспонування вектора #HistogrEmpirich#
    % результат – горизонтальний вектор #HistogrEmpirich#
    HistogrEmpirich = transpose(HistogrEmpirich);
% побудова теоретичної гістограми #HistogrTheor#
    % результат – горизонтальний вектор #HistogrTheor#
    k = 1:2:256;
    HistogrTheor(k) = (HistogrEmpirich (k)+HistogrEmpirich (k+1))/2;
    HistogrTheor(k+1) = (HistogrEmpirich (k)+HistogrEmpirich (k+1))/2;
%*************************************************************
% розрахунок вірогідностей емпіричної та теоретичної яркостей #VarTheor#
#VarEmpirich#
    % результат – горизонтальний #VarEmpirich# #VarTheor#
VarEmpirich = HistogrEmpirich;
    VarTheor = HistogrTheor;
zero_ind = find(VarTheor <=20);
     VarEmpirich (zero_ind) = [];
    VarTheor(zero_ind) = [];
% розрахунок массива-сировини для розрахунку реального значення #Xi2#
% результат – горизонтальний вектор  #Xi2#
    Xi2 = ((VarEmpirich-VarTheor).^2)./VarTheor;
% видалення помилкових значень ділення на нуль з #Xi2#
    Xi2 = Xi2(~isnan(Xi2));
```

```
%розрахунок реального значення #Xi2#
      Xi2Realn = sum(Xi2);
 % розрахунок табличного #Xi2#
      Xi2Theor = chi2inv(Probb,size(Xi2,2)-1);
      % формування наглядних массивів реального та табличного значення #Xi2#
 green1_ArrayRealn = ArrayRealn;
     green1_ArrayTheor = ArrayTheor;
     green1_ArrayCompare = uint8(green1_ArrayRealn
   end;
   if (Z == 3)
     blue1_ArrayRealn = ArrayRealn./ArrayTeor;
     blue1_ArrayTheor = ArrayTheor./ArrayTheor;
     blue1_ArrayCompare = uint8(blue1_ArrayRealn
   end;
  end;
 for Y = 1:step1Y:Pheight
   for X = 1:step1X:Pwidth
 red1_out(Y:Y+step1Y-1,X:X+step1X-1,1) = brdrdd_Red1(Y:Y+step1Y-
 1,X:X+step1X-1);
     red1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Red1Y:Y+step1Y-
 1,X:X+step1X-1).*red_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
     red1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Red1(Y:Y+step1Y-
 1,X:X+step1X-1).*red1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
```

```
green1_out(Y:Y+step1Y-1,X:X+step1X-1,1) = brdrdd_Green(Y:Y+step1Y-
1,X:X+step1X-1).*green1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
    green1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Green1(Y:Y+step1Y-
1,X:X+stepX-1);
green1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Green1(Y:Y+step1Y-
1,X:X+step1X-1).*green1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
 blue1_out(Y:Y+step1Y-1,X:X+step1X-1,1) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1).*blue1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
    blue1_out(Y:Y+step1Y-1,X:X+step1X-1,2) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1).*blue1_ArrayCompare((Y-1)/step1Y+1,(X-1)/step1X+1);
    blue1_out(Y:Y+step1Y-1,X:X+step1X-1,3) = brdrdd_Blue1(Y:Y+step1Y-
1,X:X+step1X-1);
  end;
 end;
red1_out = red1_out(1:Pheight,1:Pwidth,:);
 green1_out = green1_out(1:Pheight,1:Pwidth,:);
 blue1_out = blue1_out(1:Pheight,1:Pwidth,:);
% figure;imagesc(red1_out);
 %figure;imagesc(green1_out);
 %figure;imagesc(blue1_out);
end;
```