В. И. Коржик, А. И. Кочкарев

ОСНОВЫ СТЕГАНОГРАФИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
К ЛАБОРАТОРНЫМ РАБОТАМ

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2013

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М.А. БОНЧ-БРУЕВИЧА»

В. И. Коржик
А. И. Кочкарев

ОСНОВЫ СТЕГАНОГРАФИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2013

УДК 004.9
ББК 3973я73????
К 66??????????????????

Рецензент
Р.Р. Биккенин доктор технических наук, профессор

Рекомендовано к печати
редакционно-издательским советом университета

Коржик, В.И.
К66 Основы стеганографии: методические указания к лабораторным работам. / *В.И. Коржик, А.И. Кочкарев.* – СПб. : Издательство «Теледом» ГОУВПО СПбГУТ, 2013. – 40 с.

Предназначены для подготовки и проведения лабораторных работ для специальностей 210403 «Защищенные системы связи», 210700 «Инфокоммуникационные технологии и системы связи», 090900 «Информационная безопасность» при изучении дисциплин «Основы стеганографии», «Технологии стеганографии», «Технологии стеганографии в системах инфокоммуникаций».

В процессе выполнения лабораторных работ студенты закрепляют полученные на лекциях знания по построению и свойствам различных стегосистем (СГ) и систем с цифровыми «водяными» знаками (ЦВЗ).

В частности отрабатываются СГ с вложением в наименее значащие биты (НЗБ), известные СГ F5 и Outguess, СГ с вложением в шумы сканера, лингвистические СГ, системы ЦВЗ, устойчивые к различным преобразованиям и коалиционным атакам, система ЦВЗ для аутентификации изображений. Текст полностью согласован с электронной версией курса „Основы стеганографии” – http://ibts.sut.ru/materialy/

Оглавление

Введение

Дисциплина «Основы стеганографии» читается в одном семестре для студентов специальностей 210403 «Защищенные системы связи», 210700 «Инфокоммуникационные технологии и системы связи» (направление подготовки бакалавров, профиль 1). Дисциплина «Технологии стеганографии в системах инфокоммуникаций» читается в одном семестре для студентов специальностей 210700 «Инфокоммуникационные технологии и системы связи» (направление подготовки бакалавров, профиль 2), 090900 «Информационная безопасность» (направление подготовки бакалавров). Дисциплина «Технологии стеганографии» читается в одном семестре для студентов специальности 090900 «Информационная безопасность» (направление подготовки магистров).

Это достаточно новый курс, поскольку данное направление начало активно развиваться в работах зарубежных учёных под названием «Steganography» или «Information Hiding» лишь в течении последних 20 лет. Поэтому, как при разработке лекций, так и циклов лабораторных работ, требуется постоянное обновление материала. Успешному решению данной проблемы способствовало то обстоятельство, что один из авторов данных методических указаний активно занимался научными исследованиями в этом направлении, участвуя с докладами на многих международных конференциях, публикуя научные работы в различных международных журналах и периодически читая аналогические курсы в зарубежных университетах (Республика Корея, Польша и др.).

Лекционный курс состоит из двух основных частей: собственно стеганографии (СГ) и цифровых «водяных знаков» (ЦВЗ).Подобным же образом выполняются и лабораторные работы по курсу. В первой части курса целью СГ является такое вложение дополнительной информации в основное (покрывающее сообщение - ПС), которое трудно обнаруживается нелегальными пользователями. Поэтому важным является рассмотрение методов «стегоанализа». Эта особенность представлена также и в лабораторных работах. Во второй части курса целью ЦВЗ является устойчивость вложенной информации к попыткам нелегитимных пользователей выполнить такие преобразования ПС, которые, не нарушая его высокое качество, делают невозможным надежное выделение вложенной информации легитимными пользователями. Эта особенность также учитывается при выборе тематики лабораторных работ.

В качестве ПС в лабораторных работах используются неподвижные изображения и текстовые документы, поскольку они позволяют наиболее наглядно показать методы вложения информации и оценить качество ПС после вложения.

Для успешного выполнения всех лабораторных работ необходимо умение обращения с ПК на уровне пользователя, а также предварительное

усвоение материала лекционного курса. Программы для выполнения всех лабораторных работ имеются на сайте кафедры ИБТС (http://ibts.sut.ru/materialy).

Результаты исследований, полученные при выполнении каждой лабораторной работы, должны быть представлены в виде отчёта (можно в одном экземпляре на бригаду). Зачёт по каждой лабораторной работе принимается по результатам индивидуальных ответов на контрольные вопросы, с учётом самостоятельного участия в работе каждого студента и представления отчёта, отвечающего требованиям, сформулированных в методических указаниях.

Лабораторная работа 1.
СГ с вложением в наименьшие значащие биты

Цель работы

Понять технику вложения и извлечения информации методом наименьших значащих бит. Проанализировать эффективность различных атак по выявлению вложения.

Задание

1.Произвести вложение и извлечение информации при различных скоростях вложения.

2. Оценить эффективность обнаружения факта вложения при использовании различных атак (визуальное обнаружение без преобразований, визуальное обнаружение после преобразования к двоичному изображению, атака по критерию χ^2, атака 2-го порядка с учетом корреляции яркостей пикселей).

Порядок выполнения

1.Для начала выполнения работы перейти в каталог, содержащий рабочие программы **ЛабСтег/LSB(1)**. Запустить программу **test.exe**. Рекомендуется скопировать папку ЛабСтег на рабочий стол учебного компьютера.

2.Нажать кнопку «Открыть файл» и выбрать один из предложенных файлов, содержащих изображения, с именем NN.bmp. Нажать кнопку «Вложить сообщение». В появившемся диалоговом окне выбрать вид вкладываемой информации – текст. Ввести сообщения, которое будет вложено. Выбрать вероятность вложения 100%.

3.Нажать кнопки «Визуальная атака». Сравнить покрывающее сообщение и стеганограмму, а так же визуальные атаки на эти изображения. Нажать кнопку «Статистические атаки», в появившемся диалоговом окне выбрать обе атаки. Нажать кнопку «Таблица» и записать результаты статистических атак.

4.Повторить пункты 1 и 2 для вероятностей вложения 50%, 10%, 5%, 2%. Перед каждым новым вложением нажимать кнопку «Очистить» и открывать файл NN.bmp заново. Сделать выводы об эффективности визуальной атаки при различных вероятностях вложения. По завершению записи всех данных статистических атак нажать кнопку «Очистить таблицу».

5.Открыть файл с вложением NN100%.bmp и нажать кнопку «Извлечь сообщение». Ничего не менять в появившемся диалоговом окне. Проверить, что выдается то сообщение, которое было вложено.

6.Нажать кнопку «Очистить».

7.По аналогии с пунктами 1 и 2 провести статистические атаки на стеганограммы с вероятностью вложения 1%, 0,1%, 0,05%, 0,01% и 1 двоичный символ для трех различных покрывающих сообщений. Проанализировать эффективность статистических атак.

8.Проведите процедуру удаления сообщения, вложенного в стеганограмму про 100% скорости вложения. Убедитесь, что при извлечении информации получается случайный набор символов.

Описание выполнения лабораторной работы

Программа работает с файлами формата BMP оттенки серого (8 разрядов) с параметрами изображения 300x200. Общее количество пикселей в таких изображениях равно 60000. Как уже говорилось выше, формат BMP представляет собой точечный рисунок. В данном формате один пиксель описывается одним байтом. Максимальное количество секретной информации, которое можно вложить в файл – 60000 бит, при этом каждый пиксель изображения будет содержать информацию. Программа позволяет вложить информацию в каждый пиксель с вероятность вложения 100% или с меньшей вероятностью, в случайные пиксели изображения.

Главное окно программы показано на рисунке 1.

Рассмотрим более подробно кнопки главного окна.

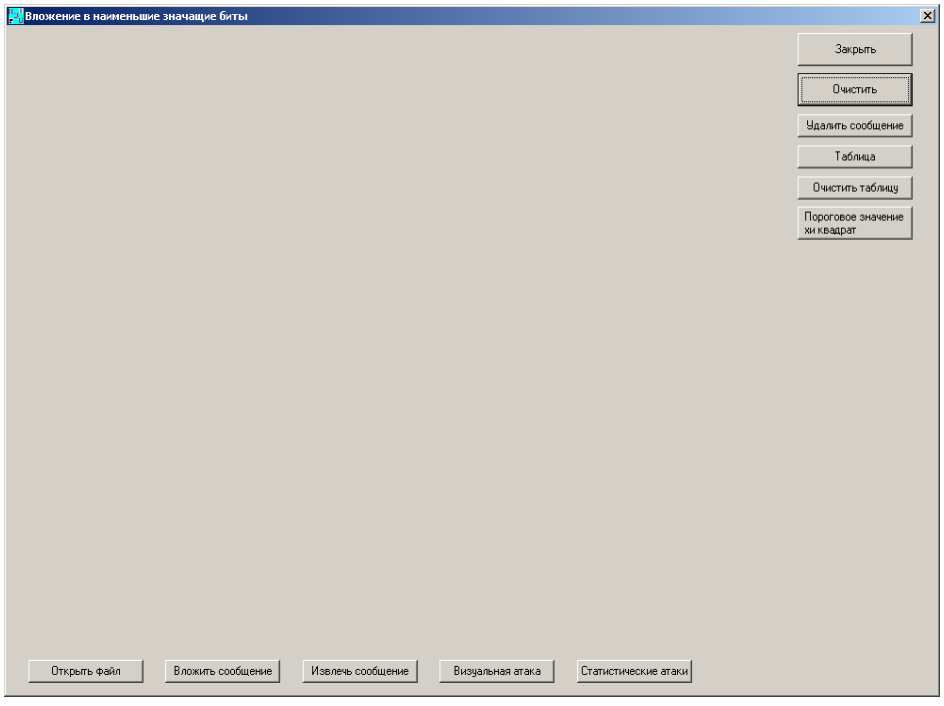

Рис.1. Главное окно лабораторной работы.

Кнопка «Открыть файл» позволяет открыть любой файл формата BMP оттенки серого (8 разрядов) размером 300x200 пикселей. Открываемый

файл может быть покрывающим сообщением, в которое нужно вложить информацию, возможной стеганограммой, которую нужно проверить на наличие вложения, или стеганограммой, полученной легальным пользователем, из которой надо извлечь секретное сообщение. Изображение открытого файла появляется в левом верхнем углу (рисунок4).

Кнопка «Вложить сообщение» позволяет вложить информацию в покрывающее сообщение. В качестве вкладываемого сообщения можно использовать как текст, так и двоичную последовательность, состоящую 0 и 1. Вероятность вложения можно выбрать из набора: 100%; 50%; 10%; 5%; 2%; 1%; 0,1%; 0,05%; 0,01%. Введенное сообщение повторяется, чтобы получилась выбранная вероятность вложения. Если при выбранной вероятности вложения количество бит, которое можно вложит, меньше бит сообщения, то последние биты сообщения не будут вложены. При желании можно зашифровать сообщение совершенным шифром. Диалоговое окно, появляющееся при нажатии кнопки «Вложить сообщение», показанно на рисунке 2. Полученная в результате вложения стеганограмма появится справа от покрывающего сообщения (рисунке 5).

Кнопка «Извлечь сообщение» позволяет легальному пользователю извлечь сообщение. До извлечения сообщения надо открыть файл со стеганограммой. Легальному получателю стеганограммы должно быть известно, было ли зашифровано сообщение совершенным шифром или нет. Так же получатель должен знать, в каком виде вкладывалось сообщение – в виде текста или двоичной последовательности. Выбор данных параметров производится с помощью диалогового окна, показанного на рисунке 3.

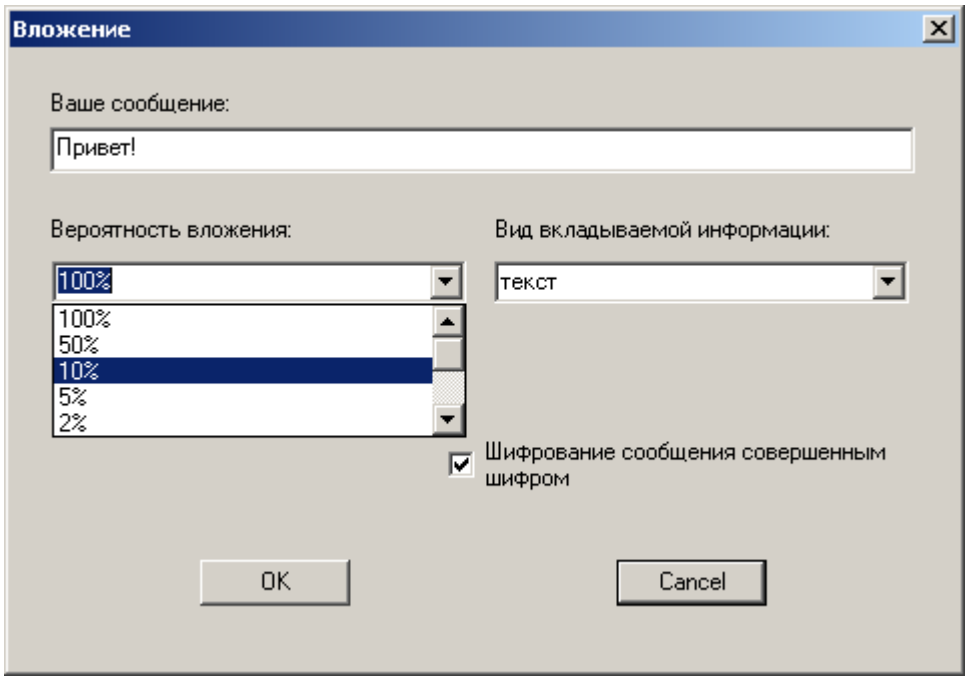

Рис. 2. Окно вложения сообщения.

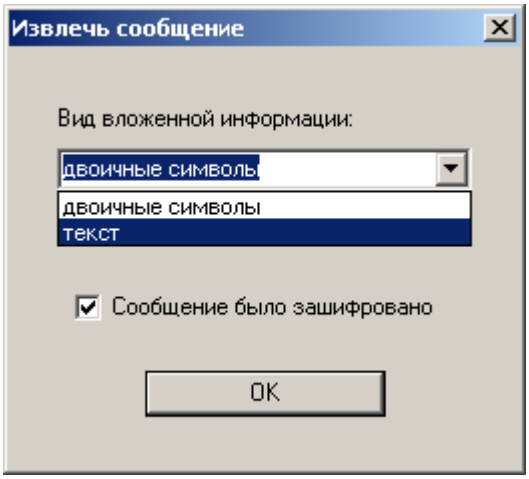

Рис. 3. Окно извлечения сообщения.

Сообщение, извлеченное из стеганограммы, появится справа от изображения, как показано на рисунке 4.

Если вложенное сообщение повторялось несколько раз, при извлечение сообщения получится периодически повторяющийся текст или периодически повторяющаяся двоичная последовательность. Если количество символов в извлеченном тексте или двоичной последовательности более пятидесяти, то появится только пятьдесят

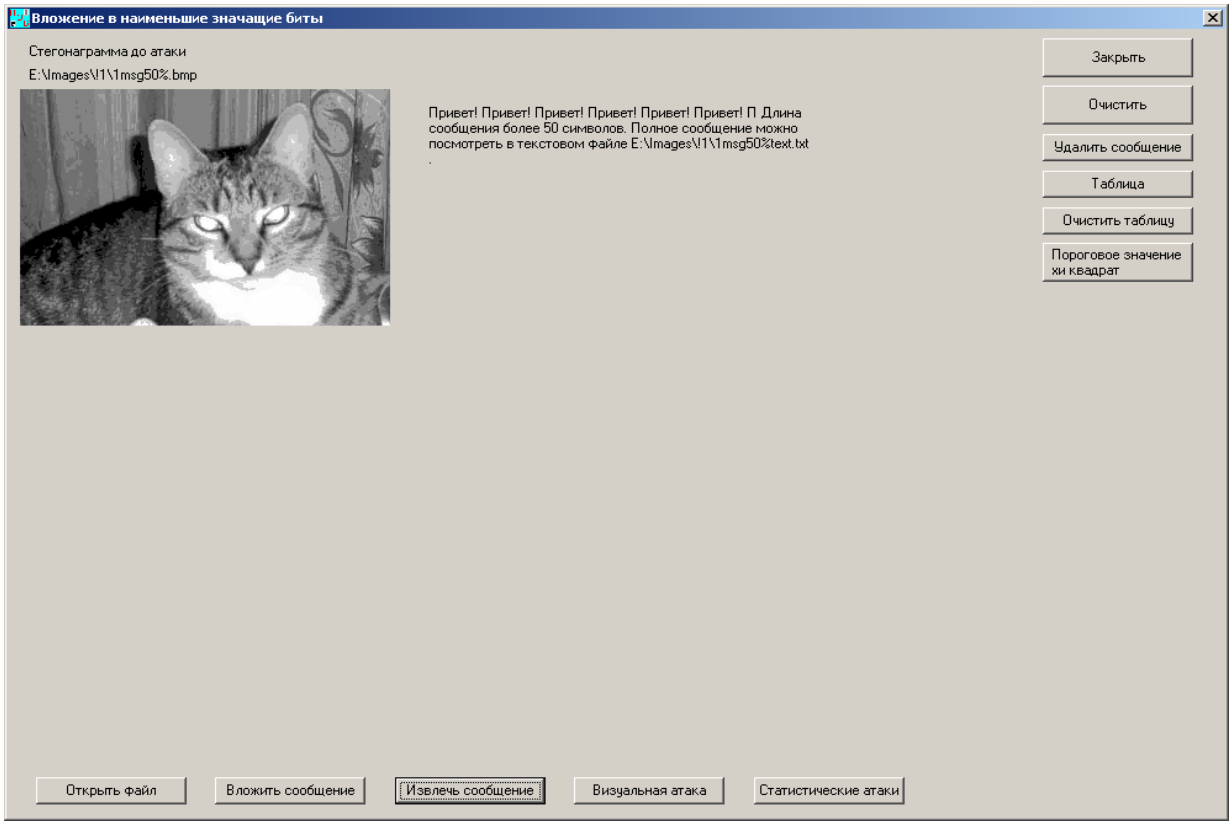

Рис. 4. Извлечение сообщения.

первых символов (чтобы не загружать экран), и будет указан путь к файлу, в котором можно прочитать полное извлеченное сообщение

Кнопка «Визуальная атака» позволяет провести визуальную атаку. Изображения, полученное в результате атаки появятся под атакованным изображением. Главное окно с результатами проведения визуальной атаки показано на рисунке 5.

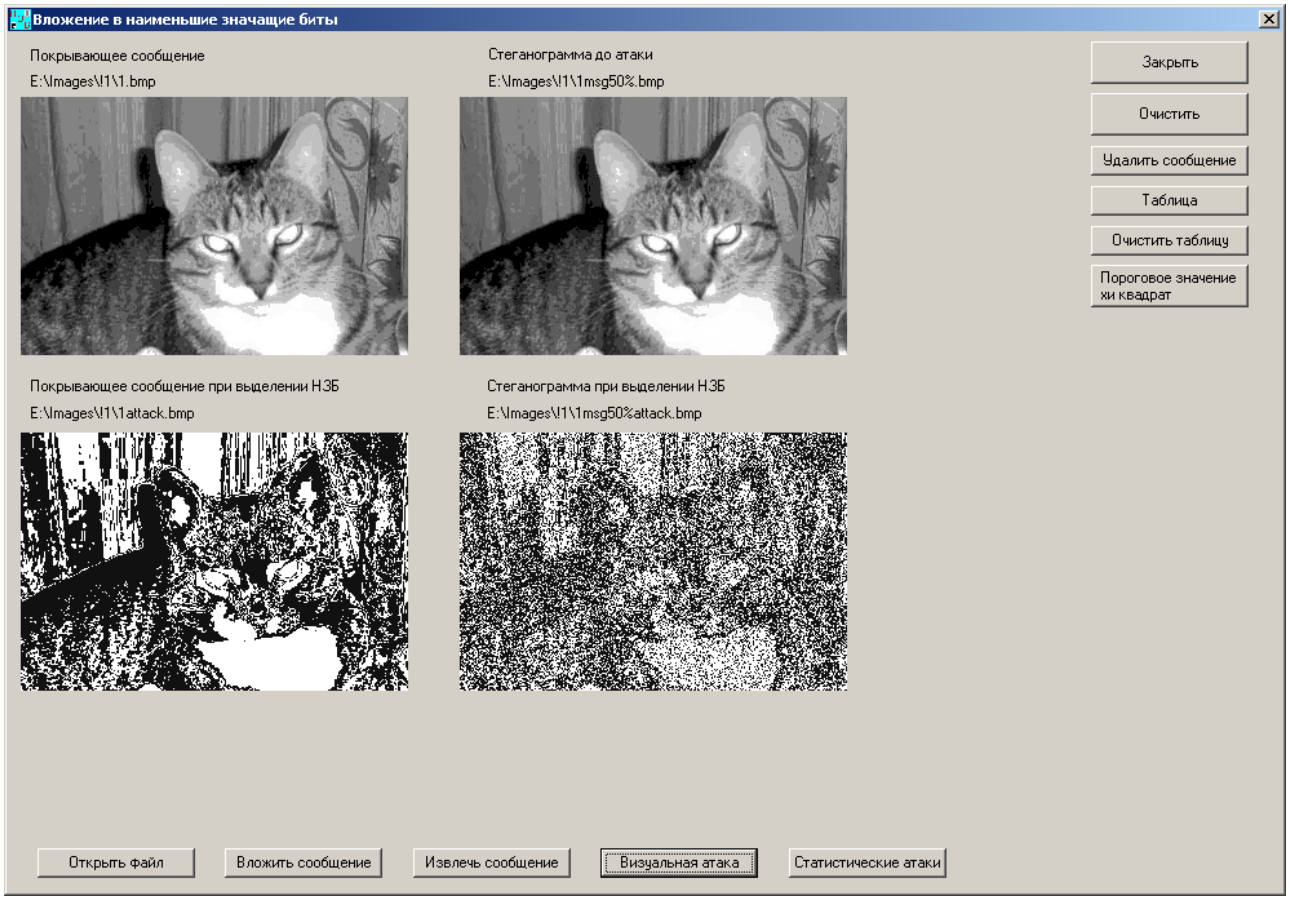

Рис. 5. Главное окно с результатами визуальной атаки.

Атаку можно произвести на покрывающее сообщение или стеганограмму, в зависимости от того, какой файл был открыт. Если вначале открыть покрывающее сообщение, а потов вложить сообщение, то в главном окне будет отображаться изображения покрывающего сообщения (слева) и стеганограммы (справа). Тогда визуальную атаку можно провести на оба изображения сразу, что позволяет сравнит результаты атаки для покрывающего сообщения и стеганограммы.

Конечно, у атакующего нет покрывающего сообщения, а значит нет возможности сравнения результаты атак. Но для студентов сравнение дает возможность понять, на какие особенности изображения предполагаемой стеганограммы после визуальной атаки стоит обратить особое внимание. Так же сравнение помогает выявить насыщенность возможного шума при

различных вероятностях вложения, понять, при какой вероятности после визуальной атаки можно уверенно сказать, что в изображении есть вложение, а при какой стоит провести другие, более эффективные атаки, например одну из статистических атак или обе сразу.

Кнопка «Статистические атаки» позволяет провести статистическую атаку без учета корреляции пикселей, основанную на гистограммах изображений, и статистическую атаку с учетом корреляции пикселей. Можно провести одну из атак, поставив галочку напротив выбранной атаки, а можно обе атаки одновременно, поставив две галочки напротив двух атак сразу.

Диалоговое окно для выбора атаки показано на рисунке 6.

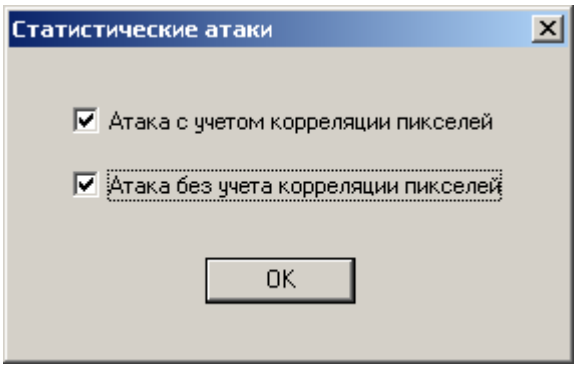

Рис. 6 Статистические атаки.

Атаковать можно одно изображение (покрывающее сообщение) или стеганограмму. Атака на покрывающее сообщение позволяет набрать статистику для выбора порогового значение χ_α^2. Можно провести атаку на оба изображения сразу и сравнить полученные результаты.

Результаты статистических атак заносятся в таблицу. Таблица вызывается нажатием кнопки «Таблица». В таблице 10 строк. Если две атаки проводились одновременно, то в строке будут заполнены оба столбца, если проводилась только одна атака, то результат атаки появится в столбце, соответствующем этой атаке. Слева, напротив результатов атак, появится полное имя атакуемого файла.

Таблица появляется в отдельном окне, поверх главного окна. Внешний вид таблицы с результатами двух атак на покрывающее изображение и стеганограмму показан на рисунке 7.

С помощью таблицы можно сравнить эффективность статистической атаки, основанной на гистограммах изображений, и статистической атаки с учетом корреляции пикселей. В таблице можно накопить данные, например, по значению χ^2 покрывающих сообщений, для выбора порогового значения χ_α^2.

Так же можно сравнивать различные результаты атак на различные предполагаемые стеганограммы, или сравнить результаты атак на покрывающее сообщение и стеганограмму.

В нижней строчке таблицы выведено пороговое значение для атаки, основанной на гистограммах изображений, – χ_α^2. Его можно выбрать, проанализировав χ^2 различных покрывающих сообщений.

Пороговое значение вводится с помощью кнопки «Пороговое значение хи квадрат», находящейся в главном окне программы. При нажатии кнопки

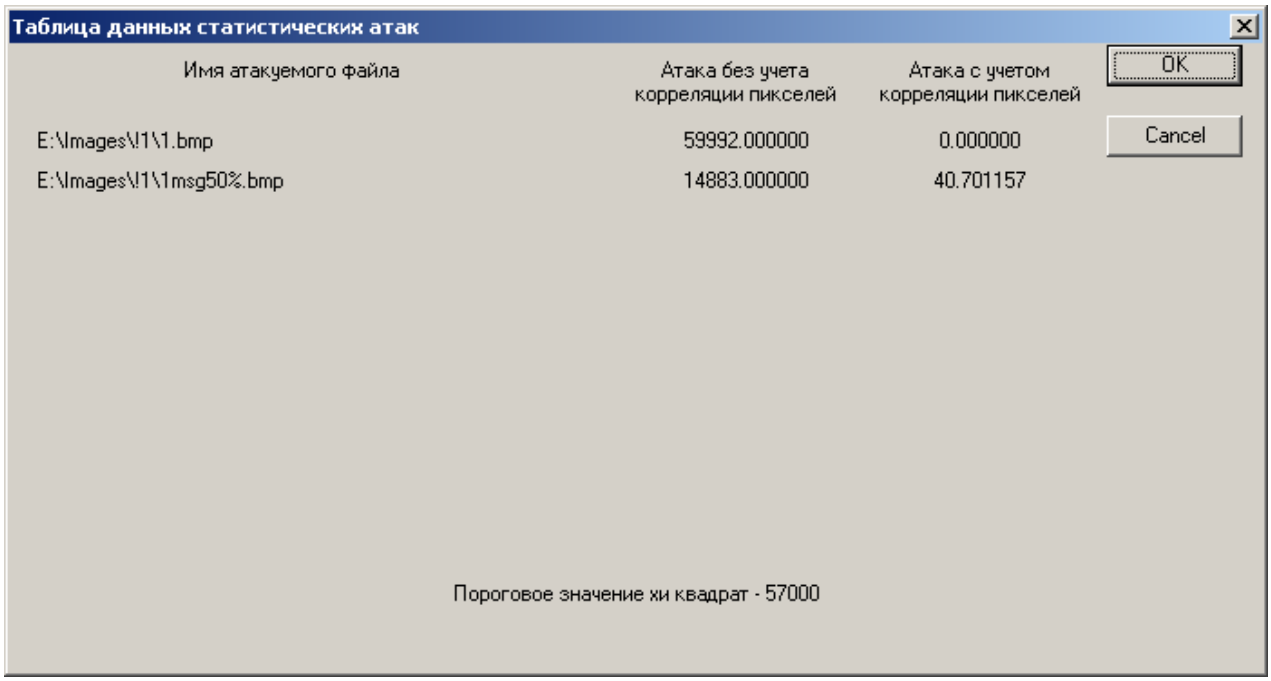

Рис. 7. Таблица данных статистических атак.

появляется диалоговое окно, показанное на рисунке 8.

До введения порогового значения нижняя строчка в таблице будет пустая. Введенное значение χ_α^2 будет отражаться в нижней строчке таблицы. Результаты, полученные после статистической атаки, основанной на гистограммах изображений, можно сравнить с пороговым значением и сделать вывод о наличие или отсутствии вложения.

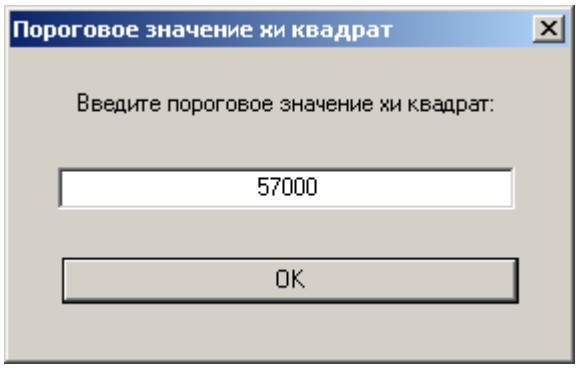

Рис. 8. Пороговое значение хи квадрат.

В любой момент пороговое значение можно изменить, для этого надо вновь нажать кнопку «Пороговое значение хи квадрат» и в появившемся диалоговом окне ввести новое значение χ_α^2. Потом в нижней строчке таблицы будет отображаться новое пороговое значение.

С помощью кнопки «Очистить таблицу» можно удалить из таблицы все ранее занесенные в нее данные, что позволяет начать накапливать статистические данные заново. При этом нижняя строчка, содержащая пороговое значение χ_α^2, не исчезнет, что позволяет проверить много изображений на наличие вложения с одним и тем же пороговым значение χ_α^2.

Кнопка «Удалить сообщение» позволяет удалить сообщение из стеганограммы. Атаку по удалению сообщения можно применить для любого файла с изображением. При этом не обязательно быть уверенным, что это стеганограмма.

При атаке по удалению сообщения все наименьшие значащие биты атакованного файла заполняются случайным образом 0 и 1, при этом не важно, в каких именно битах было вложено сообщение, поскольку изменяются все без исключения пиксели. Из стеганограммы после проведения атаки по удалению сообщения извлечь первоначальный текст или двоичную последовательность уже нельзя.

Результат проведения атаки по удалению показан на рисунке 9.

На рисунке 9 изображено главное окно с стеганограммой, после

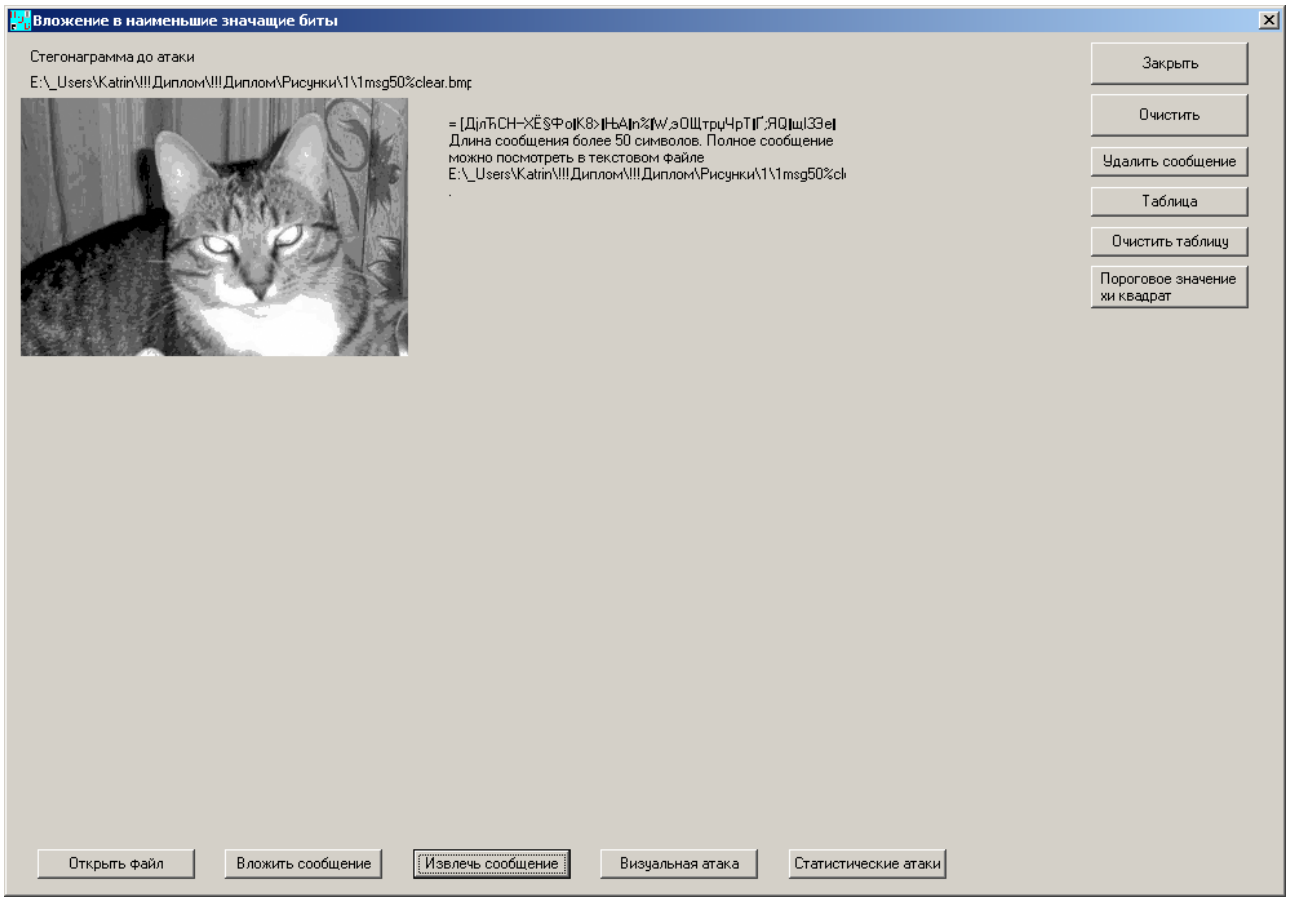

Рис. 9. Результат атаки по удалению сообщения.

удаления из нее сообщения. Изначально в стеганограмме было вложено сообщение «Привет! » с вероятностью вложения 50% и зашифровано совершенным шифром.

Если бы стеганограмма не подверглась атаке по удалению сообщения, то при извлечении легальный пользователь получил бы периодически повторяющийся текст «Привет! Привет! Привет!…». Но так как сообщение было удалено, вместо осмысленного текста легальный пользователь получает набор случайных символов «= [ДjлЋCH—ХЁ§ФоК8>ЊА…».

Данная атака очень удобна, если основной задачей атакующего является не допустить передачу вложенного сообщения. Ее можно применять ко всем изображениям, и быть уверенным, что даже если какой-то файл и содержал секретное сообщения, после атаки легальный пользователь все равно не сможет его причитать.

При нажатии кнопки «Очистить» очищается главный экран программы, при этом таблица не меняется, и данные из нее не удаляются.

При нажатии кнопки «Закрыть» закрывается главное окно, программа прекращает работу. Все статистические данные, находящиеся в таблице и

пороговое значение χ_α^2 после завершения работы программы удаляются, их уже не восстановить. Но все ключи (стегоключ и, если он был, ключ для совершенного шифра) и созданные изображения, такие как стеганограммы с вложенной информацией, изображения после визуальных атак и так далее, сохраняются на диске. При желании их можно посмотреть любыми программными средствами, которые соответствуют их форматам.

Отчет

1.Вкладываемый текст и текст, полученным при извлечении.

2.Данные по всем проведенным статистическим атакам.

3.Выводы об эффективности различных атак.

Контрольные вопросы

1.Что такое вложение в наименьшие значащие биты (НЗБ)?

2. Как регулируется скорость вложения при методе НЗБ?

3.На каком свойстве изображений основана атака с преобразованием тестируемых изображений к двоичному виду?

4.На каких свойствах СГ-НЗБ основана атака по методу χ^2?

5.Какую характеристику вложения позволяет определить атака, основанная на корреляции пикселей?

6.Как выполняется атака по удалению вложенного сообщения без обнаружения присутствия СГ?

Лабораторная работа 2.
Изучение СГ F5 и Outguess

Цель работы

Изучить работу СГ F5 и Outguess, имеющихся в открытом доступе.

Задание

Для системы F5:

1.Произвести вложение текстовых файлов, набранных латинским шрифтом, в тестовое изображение cover.jpg.

2.Проверить визуально отличаются ли файлы с вложением от чистого покрывающего сообщения.

3.Извлечь текстовый файл из стегосообщения и сравнить его с оригиналом.

4.Опытным путем определить максимальные размеры вкладываемых сообщений при не менее чем 3-х показателях качества «Quality» (Q).

5.Определить размер покрывающего сообщения и размеры стеганограмм. Рассчитать скорость вложения информации.

6.Отослать СГ по алгоритму F5 по своему электронному адресу для последующего извлечения и проверки приемлемости выполнения вложения сообщения.

Для системы Outguess:

1.Повторить пункты 1-5 применительно к СГ Outguess.

Порядок выполнения

Для начала выполнения работы перейти в каталог, содержащий рабочие программы **ЛабСтег/ F5_and_Outguess(2)**.

Для работы используются программы **Outguess/outguess.exe** и **F5/fronted.bat**. Необходимо также иметь установленную программу Java.

Для начала работы перейти в каталог, содержащий рабочие программы. Ознакомиться с описанием алгоритмов и их программных реализаций в файле OutguessF5.doc.

1.Создать текстовый файл с произвольной смысловой информацией.

2.Вложить его в тестовое покрывающее сообщение cover.jpg с помощью алгоритма F5 при Q=100.

3.Извлечь текстовое сообщение и сравнить его с оригиналом.

4.Постепенно увеличивать количество вкладываемой информации до достижения максимума.

5.Сравнить визуально стегосообщение с максимальным вложением и покрывающее сообщение.

6.Проделать п.1-5 для других значений показателя качества (Q).

7.Проделать п. 1-6 для алгоритма Outguess.

8. Отправить СГ, созданное в п.2, на свой электронный адрес. Проверить скрытность и корректное извлечение сообщения.

Отчет

1.Титульный лист.

2.Таблицу , содержащую : размеры покрывающего сообщения , показатель качества Q , максимальные размеры вложенного сообщения , размеры файла стеганограммы и скорость вложения для обоих алгоритмов .

3.Выводы об эффективности алгоритмов.

4.Выводы о визуальном восприятии вносимых искажений и возможности визуального обнаружения стеганограммы.

Контрольные вопросы

1.Каковы основные принципы вложения информации в СГ F5 и Outguess?

2.Можно ли обнаружить факт вложения информации в F5 и Outguess при использовании статистических методов?

3.Будет ли искажаться вложенное сообщение при передаче СГ по сети Интернет?

Лабораторная работа 3. Изучение лингвистической СГ на основе использования синонимов

Цель работы

Ознакомиться с одним из методов лингвистической стеганографии, основанном на использовании синонимов.

Задание

1.Ознакомиться со словарем синонимов русского языка.

2.Наблюдать изменение коротких (специально подобранных) фраз, в зависимости от изменения короткой двоичной цепочки вкладываемой в них секретной информации.

3.Произвести вложение заранее выбранной 10-битовой последовательности в один из текстов, используя специальную программу, оперирующую с лингвистической базой данных (словарем синонимов).

4.Произвести извлечение 10-битовой последовательности из полученной в п.3 стеганограммы.

5.Оценить скрытность секретной информации и скорость ее вложения.

Порядок выполнения

Для начала работы перейти в каталог, содержащий рабочие программы: **ЛабСтег/LingvLab(3)**. Для работы используются программы: *Information Processor, Information Retriever*.

1.Для знакомства со словарем синонимов перейти в подкаталог «TestTexts» и открыть файл «_SynonymDictionary» для чтения.

2.Для демонстрации метода вложения короткой цепочки бит в четыре, заранее подобранные фразы:

- Запустить программу «*Information Processor*». (Для работы программы необходимо после запуска загрузить Текстовый файл – контейнер и словарь синонимов).
- Произвести вложение различных битовых последовательностей в текстовый файл «TestSentence».
- Наблюдать изменения слов во фразах при сохранении основного содержания последних.

Сделать пометки, если, на ваш взгляд, содержание фраз хотя бы незначительно изменится или произойдут нарушения грамматики языка.

3.Для демонстрации автоматического вложения скрытной информации в смысловые тексты значительного объема на основе использования словаря синонимов:

- Запустить программу «*Information Processor*».

- Создать произвольную двоичную цепочку длиной 10 бит для погружения в выбранный смысловой текст.

- Произвести вложение битовой последовательности в текстовый файл «Text_n_Author» (где n – номер бригады).

4.Произвести сравнение текста, полученного в ходе вложения, с оригиналом (Compare).

Сделать выводы о сохранении (или нет) основного содержания и грамматики текста. Рассчитать скорость вложения секретной информации в битах на байт текста.

5.Сохранить полученную стеганограмму в некотором файле.

6.Извлечь стеганограмму из файла и произвести декодирование скрытой в ней информации, запустив программу *Information Retriever.*

(Для работы программы необходимо после запуска загрузить Текстовый файл – стеганограмму и словарь синонимов).

Сравнить выделенную информацию с той, которая была вложена соседней бригадой.

7.Сделать выводы о незаметности (или заметности) вложения секретной информации.

Отчет

1.Титульный лист.

2.Исходные короткие фразы, вложенная в них секретная информация и соответствующие ей стеганограммы.

Выводы по секретности вложения и сохранения основного содержания и грамматики коротких фраз.

3.10-битовая цепочка Выводы по секретности вложения и сохранения основного содержания и грамматики текстов.

4.Расчет скорости вложения в бит/байт покрывающего текста.

5.10-битовая цепочка, выделенная из стеганограммы. Её совпадение (или нет) с вложенной цепочкой.

Контрольные вопросы

1.В чем состоит основной принцип лингвистической стеганографии (СГ-Л)?

2.Как производится вложение информации с использованием лингвистической базы в виде синонимов?

3.В чем состоят преимущества и недостатки СГ-Л?

Лабораторная работа 4.
Изучение лингвистической СГ на основе редактирования текста

Цель работы

Изучить методы вложения и извлечения скрытой информации в текстовые документы на основе использования их незначительного редактирования.

Задание

Для работы используется программа **LingvSteg.exe** в каталоге **ЛабСтег/ДемоЛСГ(4)** и дополнительное матобеспечение NetFramework 4.0.

1.Выбрать текстовый документ для вложения.

2.Установить основные параметры, используемые при вложении.

3.Задать короткое сообщение и произвести его вложение в текстовый документ.

4.Произвести извлечение информации из стеганограммы.

5.Оценить секретность СГ и скорость вложения информации оператором.

Обзор элементов управления программы

Панель установки параметров

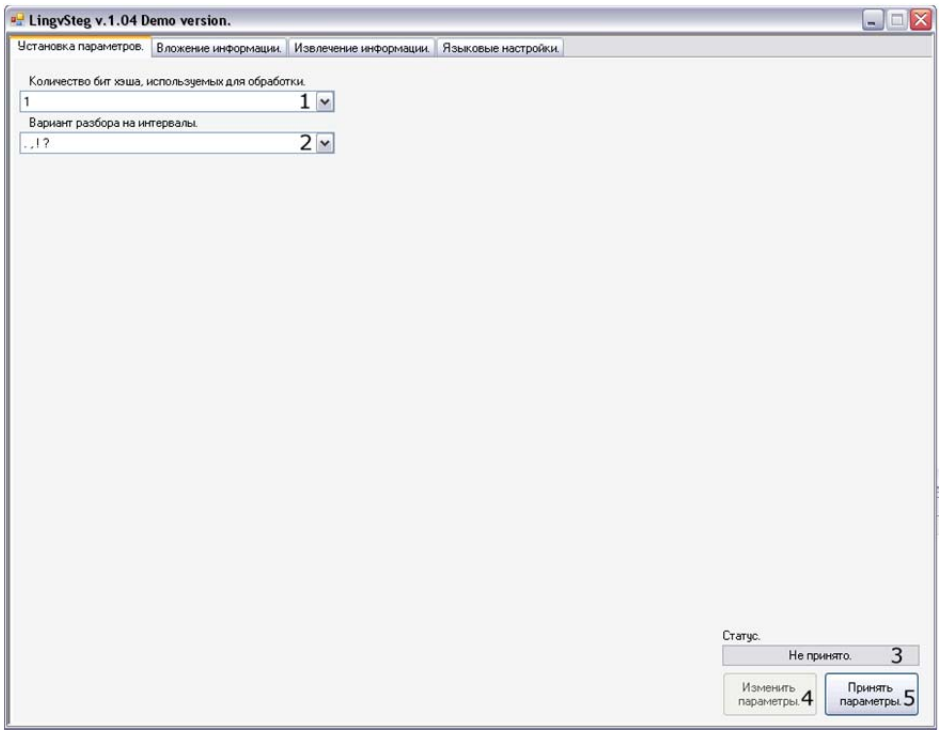

Рис. 10. Панель установки параметров.

1 - поле для выбора количества бит хэша, используемых для вложения. Используются первые биты хэша в указанном количестве.
2 - поле для выбора варианта разбора покрывающего сообщения на интервалы для хеширования.
3 - поле, показывающее успешно ли параметры были применены.
4 - кнопка для изменения уже принятых параметров.
5 – кнопка для принятия введенных параметров.

Вложение информации

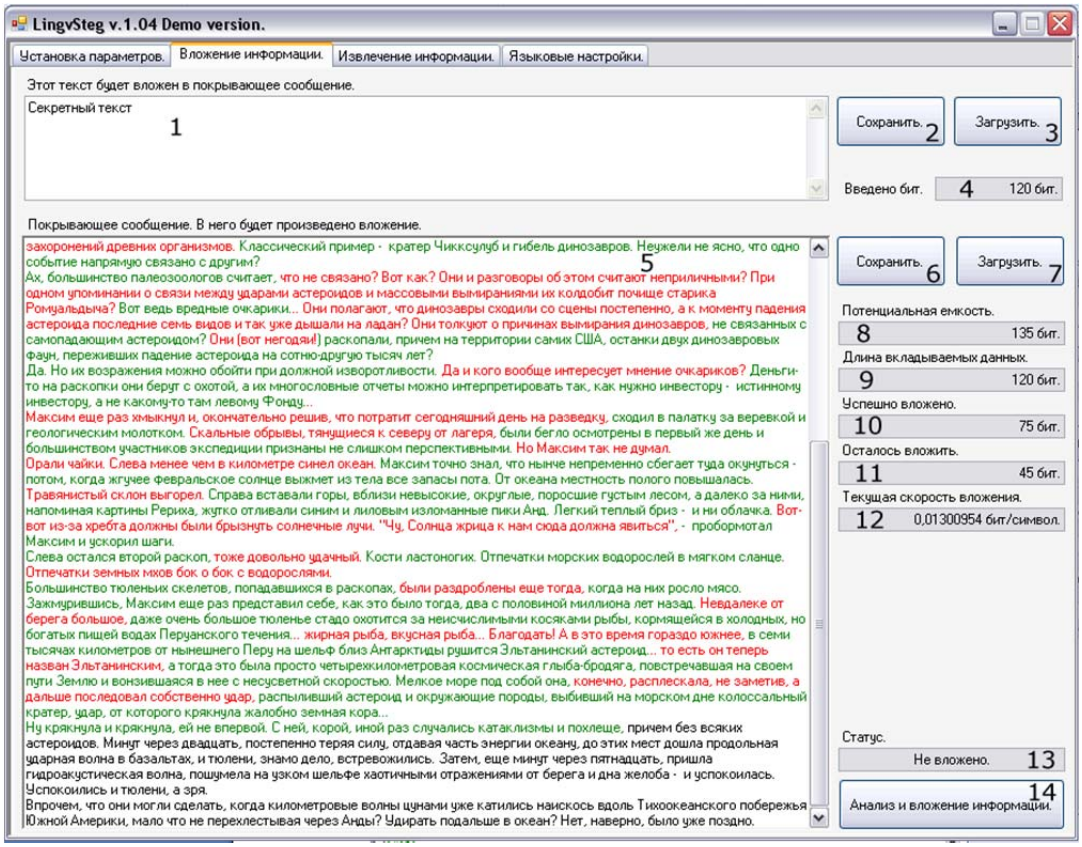

Рис. 11. Панель вложения информации.

1 - поле для ввода секретного сообщения, оно будет вложено в покрывающее сообщение.
2 - кнопка, позволяющая сохранить секретное сообщение в файл.
3 - кнопка, позволяющая загрузить секретное сообщение из файла.
4 - поле, показывающее сколько бит данных введено в поле для ввода секретного сообщения.
5 - поле для ввода и редактирования покрывающего сообщения. Цвета указывают на совпадение или несовпадение хэшей интервалов с подблоками секретного сообщения. Красный текст - текст, нуждающийся в дальнейшем редактировании, зеленый текст- текст, который уже успешно отредактирован. Черный текст - текст, в который

вложение не производится, потому, что все данные уже могут быть вложены в предшествующий ему текст.

6 - кнопка, позволяющая сохранить покрывающее сообщение в файл.

7 - кнопка, позволяющая загрузить покрывающее сообщение из файла.

8 - поле, показывающее сколько максимально можно вложить бит в текст введенного покрывающего сообщения.

9 - поле, показывающее длину секретного сообщения в битах.

10 - поле, показывающее сколько бит уже успешно вложено в покрывающее сообщение.

11 - поле, показывающее сколько бит еще не совпадает с битами интервалов.

12 - поле, показывающее текущую скорость вложения информации.

13 - поле, указывающее, успешно ли осуществлено вложение секретного сообщения в покрывающее.

14 - кнопка, по нажатию которой проверяется успешность вложения секретного сообщения в покрывающее и происходит обновление цветовой индикации в поле редактирования покрывающего сообщения.

Извлечение информации

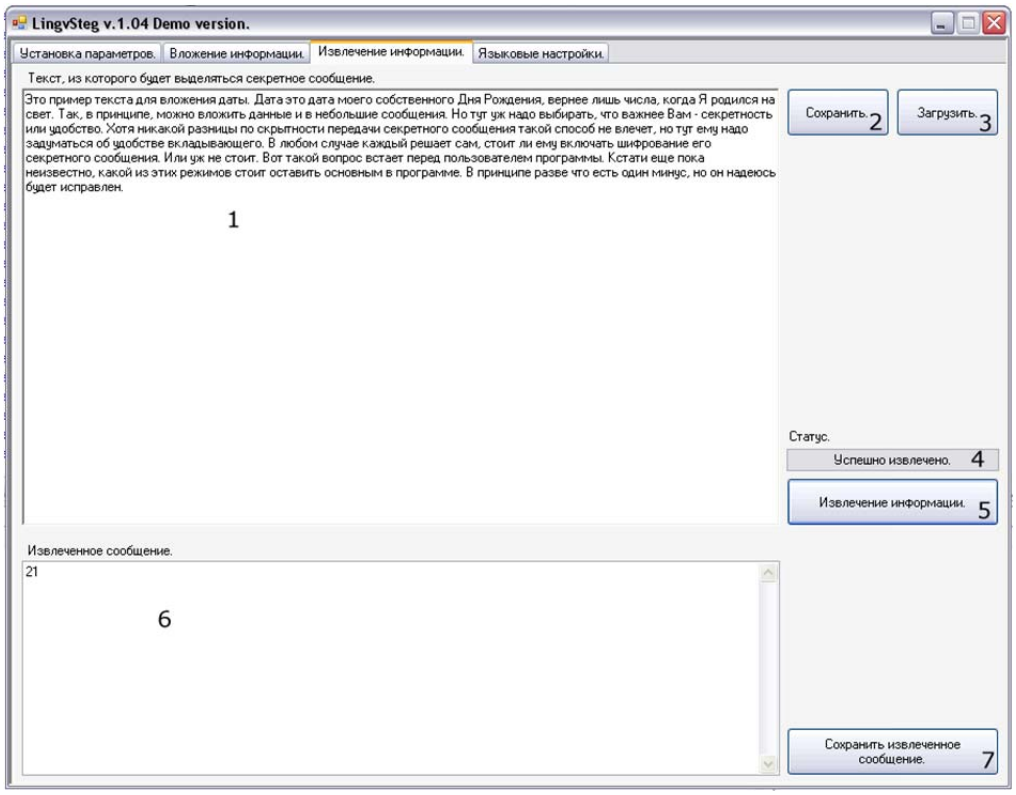

Рис. 12. Панель извлечения информации.

1 - поле для ввода сообщения, из которого будет проходить извлечение информации.

2 - кнопка, позволяющая сохранить стеготекст в файл.

3 - кнопка, позволяющая загрузить стеготекст из файла.
4 - поле, указывающее успешно ли осуществлена попытка извлечения информации из введенного сообщения.
5 - кнопка, по нажатию которой будет произведена попытка извлечь информацию из введенного сообщения.
6 - поле, в котором будет отображено секретное сообщение в случае успешного извлечения.
7 - кнопка, позволяющая сохранить секретное сообщение в файл.

Языковые настройки

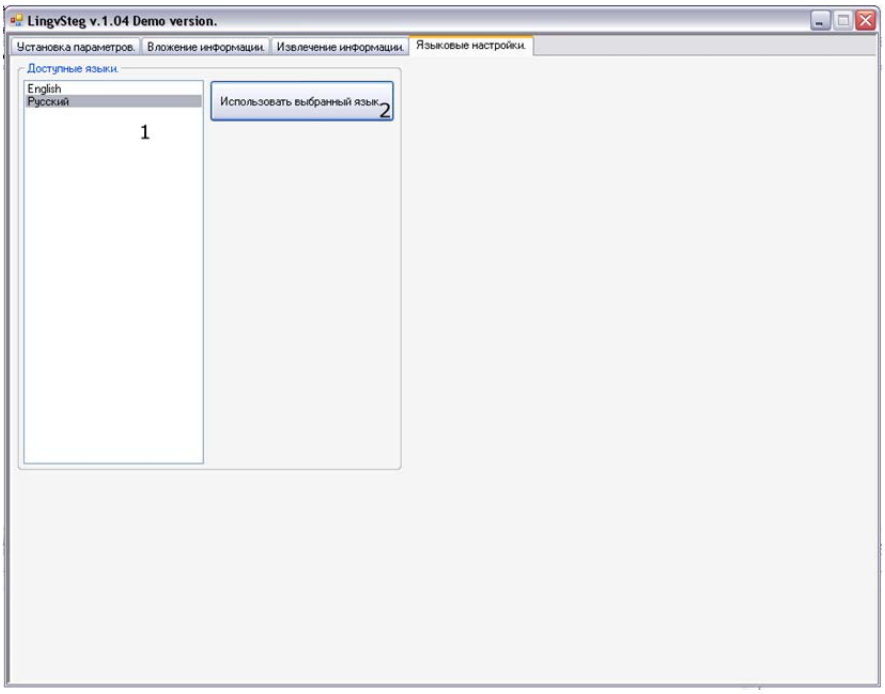

Рис. 13. Панель языковых настроек.

1 - список, в котором отображены те языки, на которых может быть представлен интерфейс программы.
2 - кнопка, по нажатию которой будет установлен выбранный язык интерфейса.

Порядок выполнения работы

Вложение информации

1. Задайте требуемые параметры во вкладке «Установка параметров».
2. Нажмите кнопку «Принять параметры» (5). После этого в случае корректно указанных параметров ввод в поля будет заблокирован, и указанные параметры будут применяться для дальнейшей работы. Поле «Статус» (3) отобразит информацию о том, что параметры успешно приняты. В случае же некорректно указанных параметров будет выведено сообщение том, какой из параметров нуждается в

корректировке, а поле «Статус» (3) отобразит информацию о том, что параметры не приняты.

3. После того, как параметры будут успешно заданы, перейдите на вкладку «Вложение информации».
4. Введите в поле для ввода секретного сообщения (1) сообщение, которое хотите вложить, или загрузите его из файла, используя кнопку «Загрузить»(3). Поле «Введено бит.»(4) будет отображать его длину в битах
5. Начинайте вводить в поле для покрывающего сообщения (5) текст в который будет производиться вложение, или загрузите этот текст из файла, используя кнопку «Загрузить»(7).
6. Нажмите кнопку «Анализ и вложение информации» (14). Программа произведет попытку вложения в текст покрывающего сообщения. Поля справа (8-12) отобразят различную информацию о ходе вложения. Текст покрывающего сообщения станет окрашен в несколько цветов. Цвета указывают на совпадение или несовпадение битов хэшей интервалов с битами секретного сообщения. Красный текст - текст, нуждающийся в дальнейшем редактировании, зеленый текст - текст, который уже успешно отредактирован. Черный текст - текст, в который вложение не производится, потому, что все данные уже могут быть вложены в предшествующий ему текст. Длина черного текста ограничена, не стоит вводить текста более чем в такой, в который потенциально можно вложить 8 бит, иначе из этого участка тоже будут извлекаться данные.
7. Редактирование покрывающего сообщения и последующее нажатие кнопки «Анализ и вложение информации» (14) необходимо производить до тех пор, пока поле «Статус» (13) не отобразит информацию о том, что секретное сообщение было успешно вложено.
8. Готовое покрывающее сообщение можно или скопировать прямо из поля редактирования (5), или сохранить в файл, используя кнопку «Сохранить» (6).

Извлечение информации

9. Задайте требуемые параметры во вкладке «Установка параметров».
10. Нажмите кнопку «Принять параметры» (5). После этого в случае корректно указанных параметров ввод в поля будет заблокирован, и указанные параметры будут применяться для дальнейшей работы.

Поле «Статус» (3) отобразит информацию о том, что параметры успешно приняты. В случае же некорректно указанных параметров будет выведено сообщение том, какой из параметров нуждается в корректировке, а поле «Статус» (3) отобразит информацию о том, что параметры не приняты.

11. После того, как параметры будут успешно заданы, перейдите на вкладку «Извлечение информации».
12. В поле для ввода стеготекста (1) введите текст сообщения, из которого планируется извлечение информации, или загрузите текст из файла, используя кнопку «Загрузить» (3).
13. Нажать кнопку «Извлечение информации» (5). Результат попытки извлечения будет указан в поле «Статус» (4). В случае успешного извлечения извлеченное сообщение появится в поле для извлеченного сообщения (6).
14. Извлеченное сообщение можно или скопировать прямо из этого поля извлеченного сообщения (6), или сохранить в файл, используя кнопку «Сохранить извлеченное сообщение» (7).

Примечание

В данной программе вкладываемое сообщение предварительно не шифруется (для упрощения) и поэтому обнаружение данной лингвистической СГ оказывается тривиальным при известном алгоритме вложения и извлечения. Однако, при использовании стойкого шифрования такая СГ будет необнаруживаемой.

Отчет

1. Титульный лист.
2. Текст вкладываемого сообщения.
3. Текст извлеченного сообщения.
4. Объём покрывающего сообщения.
5. Время вложения информации (затраченное оператором) и скорость вложения по отношению к объёму покрывающего сообщения.

Контрольные вопросы

1. Что такое лингвистические СГ?
2. Каков алгоритм вложения и извлечения информации для лингвистических СГ с редактированием текста?
3. Чем обуславливается секретность (необнаруживаемость) таких СГ?
4. Можно ли удалить вложенную информацию без её обнаружения и без нарушения содержания покрывающего текста?

Лабораторная работа 5.
Исследование СГ, использующую погружение информации в шумы сканирования

Цель работы

Изучить метод погружения скрытой информации в шумы сканера и возможности обнаружения данной СГ в зависимости от выбора её параметров.

Задание

1. Выбрать параметры вложения скрытой информации.
2. Произвести вложение информации с различными скоростями. Проверить корректность её извлечения
3. Произвести стегоанализ для различных скоростей вложения и сделать выводы о его эффективности.
4. Сравнить текстовые документы до и после вложения. Сделать вывод о заметности (или незаметности) изменений после вложения.

Порядок выполнения

Для начала выполнения работы перейти в каталог, содержащий рабочие программы **ЛабСтег/ScannerStego(5)**. Запустить программу **stego-image1.3.jar**.

1. Ознакомиться с описанием полей и кнопок программы, используемых при выполнении работы.

1.1. Вкладка «Insert Bits»

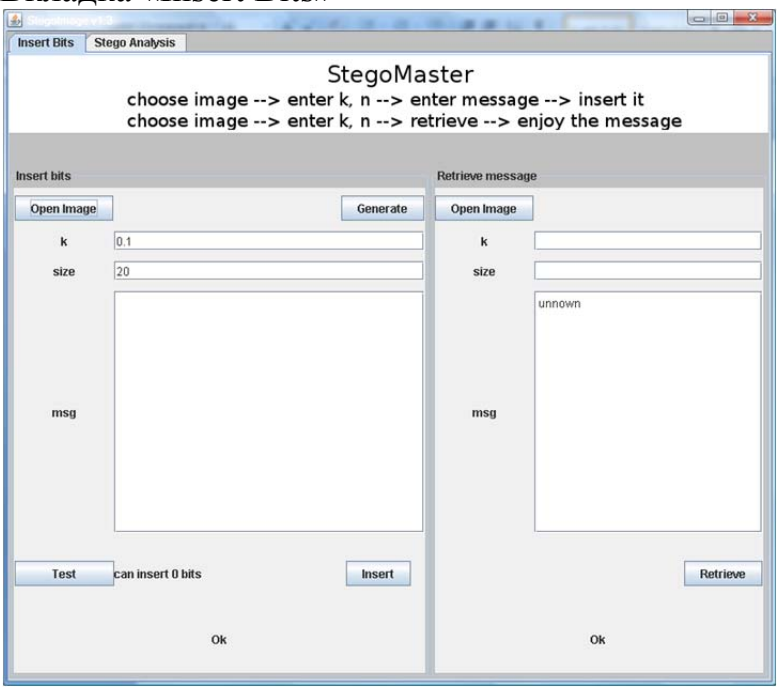

Рис. 14. Вкладка «Insert Bits».

Поле «**Insert bits**»

- Кнопка «**Open Image**» открывает проводник, позволяющий выбрать изображения форматов *.bmp и *.jpg.
- Поле «**k**» позволяет ввести значение параметра k;
- Поле «**Size**» позволяет выбрать размер области;
- Кнопка «**Test**» производит подсчёт количества бит, которые можно будет вложить в выбранное изображение с выбранными параметрами «**k**» и «**size**»;
- Кнопка «**Generate**» генерирует ПСП, состоящую из 0 и 1, длиной равной результату «**Test**»;
- Поле «**Msg**» позволяет ввести секретную информацию;
- Кнопка «**Insert**» производит вложение секретной информации, изображение со вложением будет создано в той же директории откуда был выбран файл, к имени файла добавится «**_st**».

Поле «**Retrieve message**»

- Кнопка «**Open Image**» открывает проводник, позволяющий выбрать изображение;
- Поле «**k**» позволяет ввести значение параметра k;
- Поле «**Size**» позволяет выбрать размер области;
- Кнопка «**Retrieve**»производит извлечение секретного сообщения с выбранными параметрами «**k**» и «**size**»;

1.2. Вкладка «Stego Analysis»

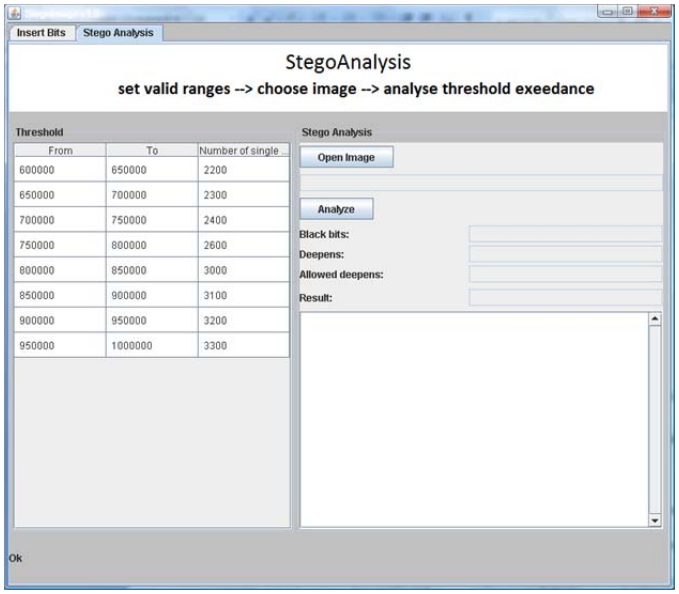

Рис. 15. Вкладка «Stego Analysis».

Поле «**Threshold**»

- В таблице содержатся количества черных пикселей изображения текстового документа формата А4 и максимальное количество единичных углубление соответствующее каждому диапазону, если количество черных пикселей выбранного изображения не попадает ни в один из диапазонов следует заменить одну из строк таблицы;

Поле «**Stego Analysis**»

- Кнопка «**Open Image**» позволяет выбрать изображение для стегоанализа;
- Кнопка «**Analysis**» производит подсчёт количества черных пикселей и единичных углублений, затем производит сравнение с заранее выбранными порогами и выводит результат сравнения.

2. Выбрать изображение (отсканированный текст) для вложения. Для этого нажать кнопку «**Open Image**» и найти папку «**изображения**» с текстовыми изображениями. Выбрать определённое изображение без вложения (без расширения «–st…»). В результате появится запись «file open»
3. Выбрать параметры вложения (k, size).
4. Проверить доступный объём вложения (показывается количество вкладываемых бит).
5. Задать или случайно сгенерировать вкладываемые биты (Ввести в поле или нажать кнопку «**Generate**»).
6. Вложить выбранное сообщение в текстовый документ.
7. Извлечь вложенную последовательность бит. Для этого ввести те же параметры, которые были выбраны при вложении. ??? текст с вложением (имеющий расширение «–st…»). Нажать кнопку «**Retrieve**». Проверить правильность извлечённого сообщения.

8. Перейти на вкладку «Stego Analysis». Видна таблица выбора порогов для принятия решения по количеству углублений. Открыть текст (изображение) без вложения и с вложением. Провести обнаружение вложения, нажав кнопку «**Analysis**». Появятся таблицы с результатом стегоанализа. Убедиться в правильности (или неправильности) обнаружения вложения.
9. Повторить пп. 1-8 для других (не менее двух) наборов параметров вложения и для других изображений.
10. Посмотреть текст без вложения и сделать вывод о заметности (или незаметности) вложения.

11. Определить места вложения при увеличении масштаба изображения. Для этого посмотреть копию стеганограммы с вложением, где отличия отмечены красными точками.

Отчет

1. Титульный лист.
2. Выбранные параметры.
3. Вкладываемая информация. Допустимый объём вложения.
4. Результаты извлечения информации.
5. Результаты стегоанализа.

Контрольные вопросы

1. В чем состоит основное преимущество СГ с вложением секретной информации в шумы сканера по сравнению с другими видами СГ?
2. Как проводится вложение и извлечение секретной информации для данного метода?
3. Какими параметрами определяется скорость и секретность вложения при данном методе?
4. На чём основан стегоанализ данного метода? Является ли он эффективным?

Лабораторная работа 6. Исследование системы «0-битовой» ЦВЗ при преобразованиях изображения

Цель работы

Исследование возможности детектирования ЦВЗ при выборе различных параметров системы и выполнении различных преобразований изображений.

Задание

Для начала работы перейти в каталог, содержащий рабочую программы **ЛабСтег/NullBitWM(6)**. Запустить программу **nullBitWM.jar**

1. Изучить метод вложения 0-битового ЦВЗ в области, инвариантные к преобразованиям, и метод детектирования 0-битового ЦВЗ.

2. Выбрать изображение для вложения.

3. Выбрать параметры для генерации ключа и получить ключ в виде изображения.

4. Наблюдать промежуточные этапы формирования ключа. Пояснить значение параметров ключа.

5. Задать параметры вложения 0-битового ЦВЗ (выбрать ключ, указать размер области вложения согласно выбранному ключу, указать значение коэффициента глубины вложения).

6. Произвести вложение ЦВЗ в выбранное изображение.

7. Наблюдать изображение до и после вложения.

8. Выполнить поиск оптимального порога детектирования.

9.Произвести детектирование ЦВЗ при выбранном ключе и оптимальном пороге детектирования.

10.Выполнить поочерёдно преобразования выбранного изображения (удаление строк и столбцов, дублирование срок и столбцов, циклический сдвиг, вырезание окна, выделение окна, поворот, добавление Гауссовского шума, преобразование JPEG с показателем качества Q) с различными параметрами.

11.Наблюдать изменение изображения после всех преобразований, количество вложенных максимумов, количество распознанных максимумов и возможность детектирования ЦВЗ.

12. Повторить пункты 2-11 при другом значении коэффициента глубины вложения и для другого изображения.

13. Попытаться обнаружить ЦВЗ в изображении без вложения.

14. Сгенерировать ложный ключ с указанием других параметров генерации.

15. Попытаться обнаружить вложение ЦВЗ при выборе ложного ключа.

Порядок выполнения

1. На вкладке «Настройки» ввести необходимые данные в соответствующие поля ввода. Нажать кнопку «Создать структуру папок для сохранения результатов». На рис. 16 представлен внешний вид панели настроек.

Рис. 16. Внешний вид вкладки «Настройки».

2. Перейти на вкладку «Вложение ЦВЗ».

3. Выбрать из базы изображений одно изображение для вложения, нажав кнопку «Открыть» в верхней части окна. База изображений находится в папке **/nullBitWM(6)/01images**.На рис. 17 представлен внешний вид вкладки «Вложение ЦВЗ» при выборе изображения из базы.

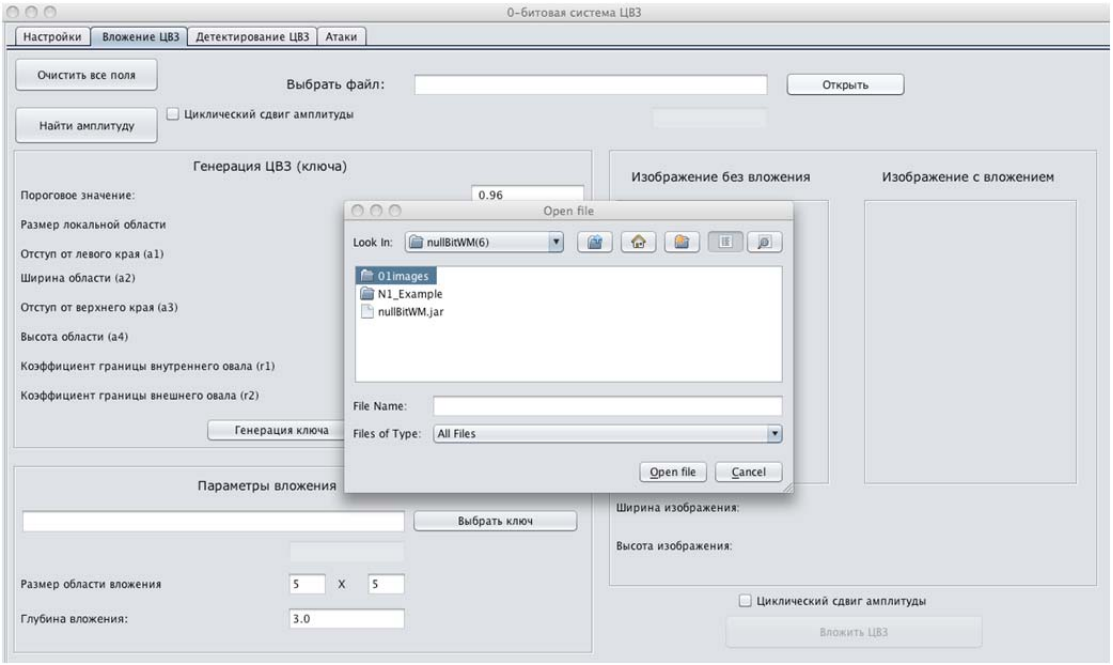

Рис. 17. Вид вкладки «Вложение ЦВЗ» при выборе изображения для вложения.

4.Получить частотное распределение амплитуды изображения с центрированием и без него, нажав на кнопку «Найти амплитуду». Для центрирования матрицы амплитуды необходимо установить «Циклический сдвиг амплитуды».

На рис. 18 представлен внешний вид вкладки «Вложение ЦВЗ» с окном отображения частотного распределения амплитуды без центрирования. Внешний вид вкладки «Вложение ЦВЗ» с окном отображения частотного распределения амплитуды с центрированием представлен на рис.19.

Изображения матрицы амплитуд с центрированием и без него автоматически сохраняются в папке **nullBitWM(6)/N<номер бригады>_<Фамилия студента>/ 02images/ Amplitude.**

5. Сформировать ключ для вложения ЦВЗ (параметры формирования ключа предустановлены, в дальнейшем необходимо будет их изменить), нажав на кнопку «Генерировать ключ».

Полученное изображение ключа автоматически сохраняется в папке **nullBitWM(6)/N<номер бригады>_<Фамилия студента>/02images/Key**.

Полученные изображения всех матриц ключа автоматически сохраняются в папке **nullBitWM(6)/N<номер бригады>_<Фамилия студента>/02images/Key_matrix**.

Внешний вид вкладки «Вложение ЦВЗ» при установке параметров формирования ключа представлен на рис. 20.

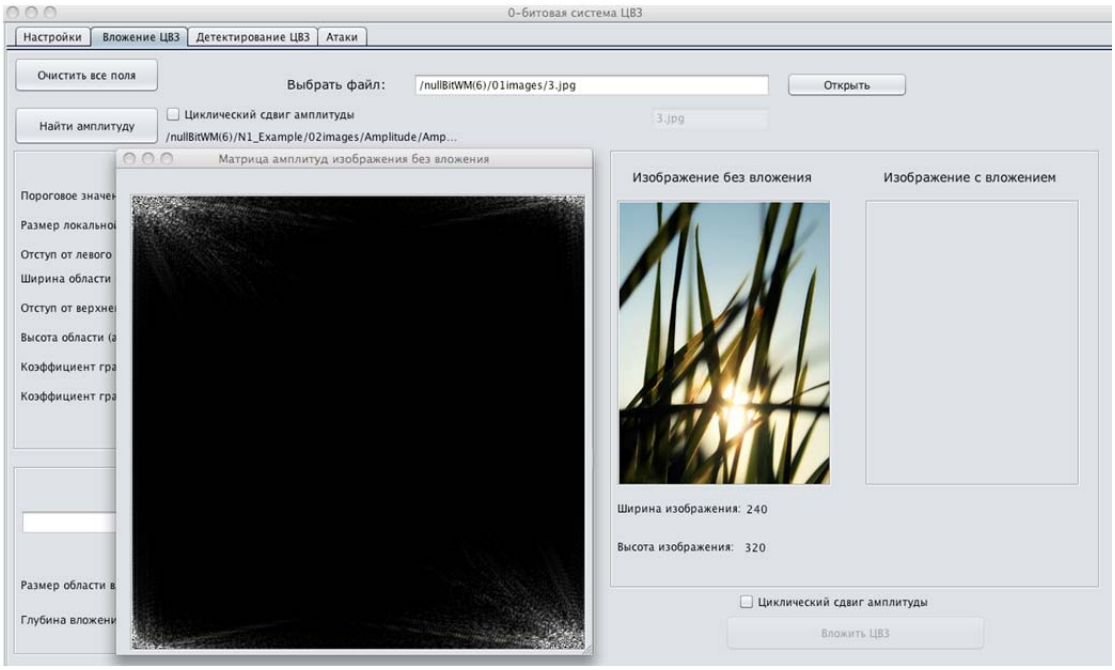

Рис. 18. Внешний вид вкладки «Вложение ЦВЗ» с окном отображения частотного распределения амплитуды без центрирования.

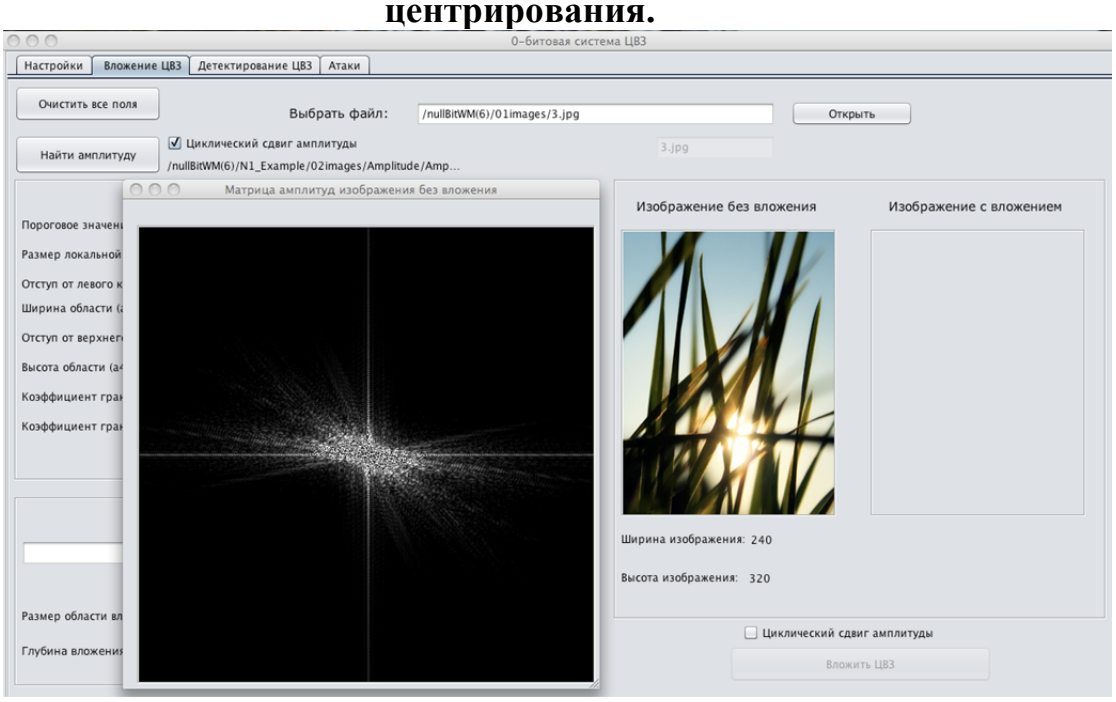

Рис. 19. Внешний вид вкладки «Вложения ЦВЗ» с окном отображения частотного распределения амплитуды с центрированием.

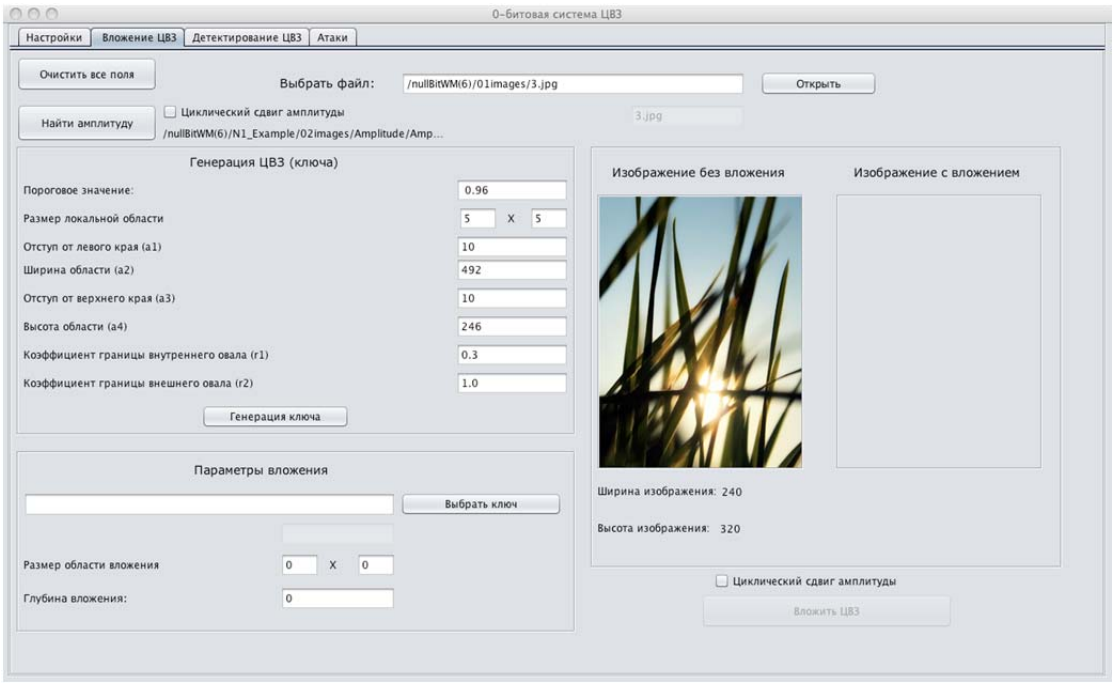

Рис. 20. Вид вкладки вложения ЦВЗ рабочей программы при установке необходимых параметров генерации ключа.

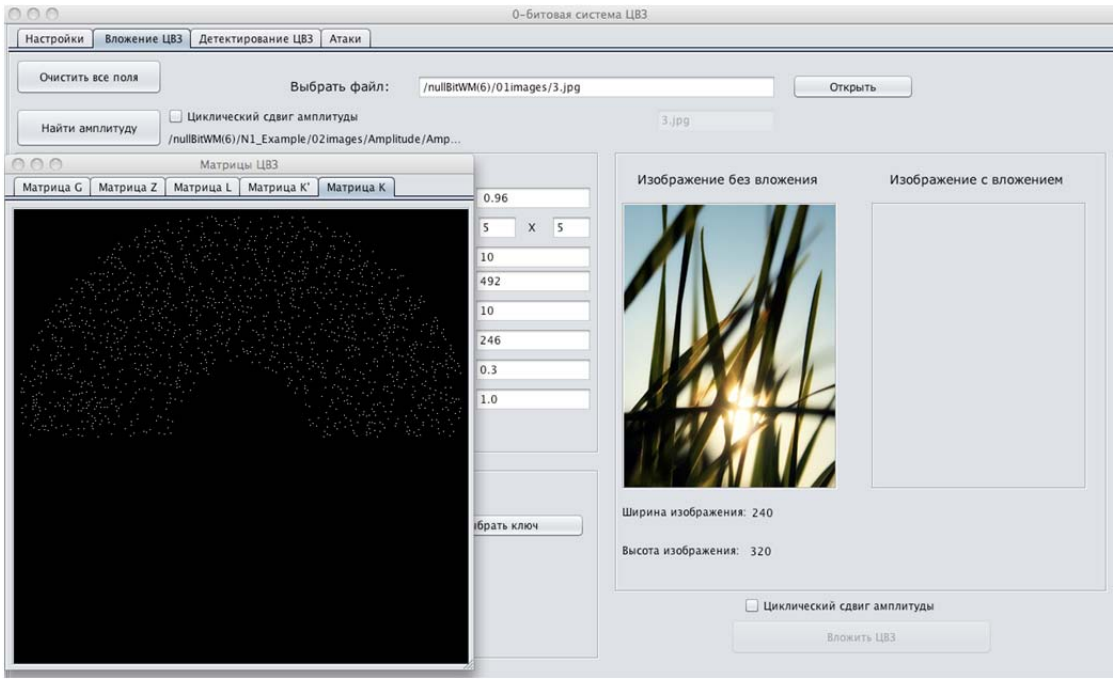

Рис. 21. Внешний вид вкладки «Вложение ЦВЗ» с окном отображения результата генерации матрицы ключа и промежуточных матриц.

6. Указать параметры вложения ЦВЗ (выбрать ключ из папки **nullBitWM(6)/N<номер бригады>_<Фамилия студента>/02images/Key**, указать размеры локальной области согласно ключу, указать коэффициент

глубины вложения). Вид вкладки «Вложение ЦВЗ» при установке параметров вложения ЦВЗ представлен на рис. 22.

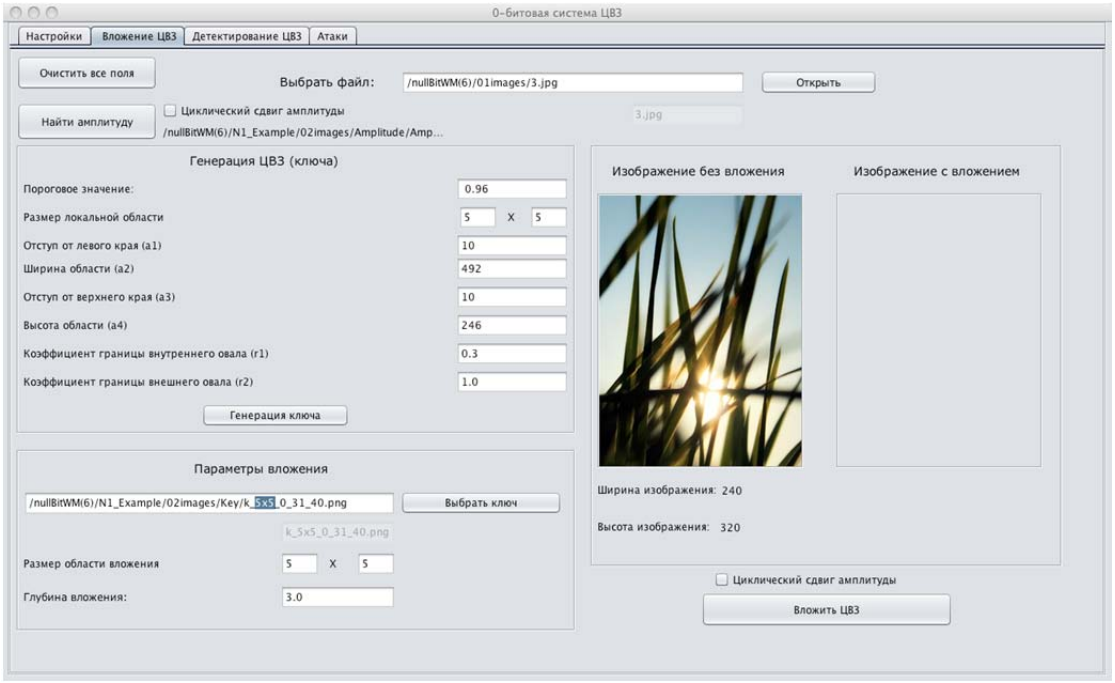

Рис. 22. Внешний вид вкладки «Вложение ЦВЗ» при установке параметров вложения.

7. Произвести вложение, нажав на кнопку «Вложить ЦВЗ».
8. Наблюдать изображение до и после вложения и амплитуду изображения с вложением, которая отобразится в новом окне программы. Внешний вид вкладки «Вложение ЦВЗ» с результатом вложения и с окном отображения амплитуды с вложением представлен на рисунке 40.

Изображение с вложением ЦВЗ автоматически сохраняется в папке **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Embedded_image**.

Амплитуда с вложением ЦВЗ автоматически сохраняется в папке **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Amplitude**.

9. Амплитуда с вложением ЦВЗ с измененной синей составляющей автоматически сохраняется в папке **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Embedded_amplitude.** Перейти на вкладку «Детектирование ЦВЗ».
10. Выбрать изображение для детектирования ЦВЗ из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Embedded_image**, нажав на кнопку «Открыть» в верхней части окна.

На рис. 24 представлен внешний вид вкладки «Детектирование ЦВЗ» при выборе изображения для детектирования.

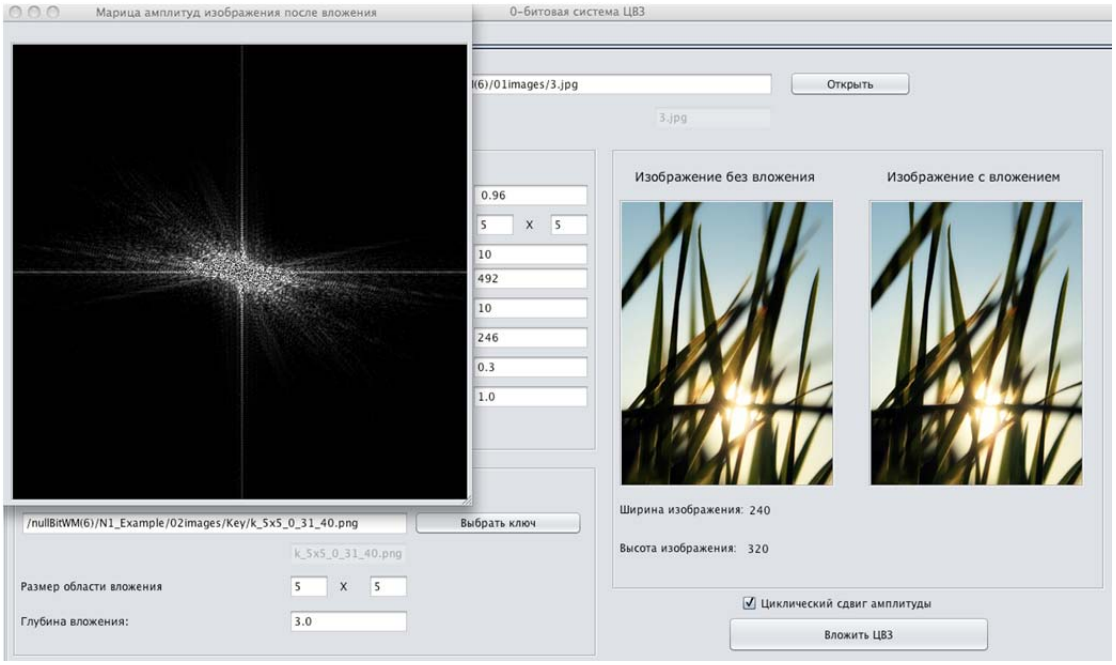

Рис. 23 – Вид вкладки «Вложения ЦВЗ» с результатом вложения и с окном отображения амплитуды с вложением.

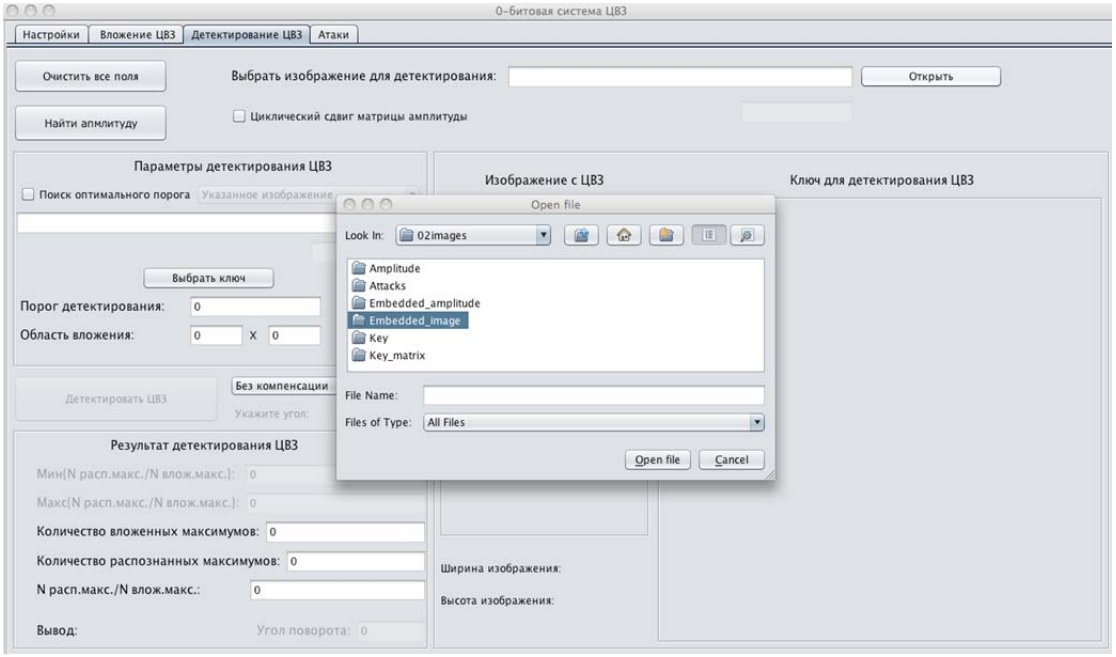

Рис. 24. Внешний вид вкладки «Детектирование ЦВЗ» при выборе изображения для детектирования.

11. Установить «Поиск оптимального порога» и выбрать в выпадающем списке «По базе изображений» в поле «Параметры детектирования».

12. Выбрать ключ из для детектирования из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Key** и указать размер локальной области вложения согласно имени ключа.

Внешний вид вкладки «Детектирование ЦВЗ» при поиске оптимального порога для детектирования представлен на рис. 25.

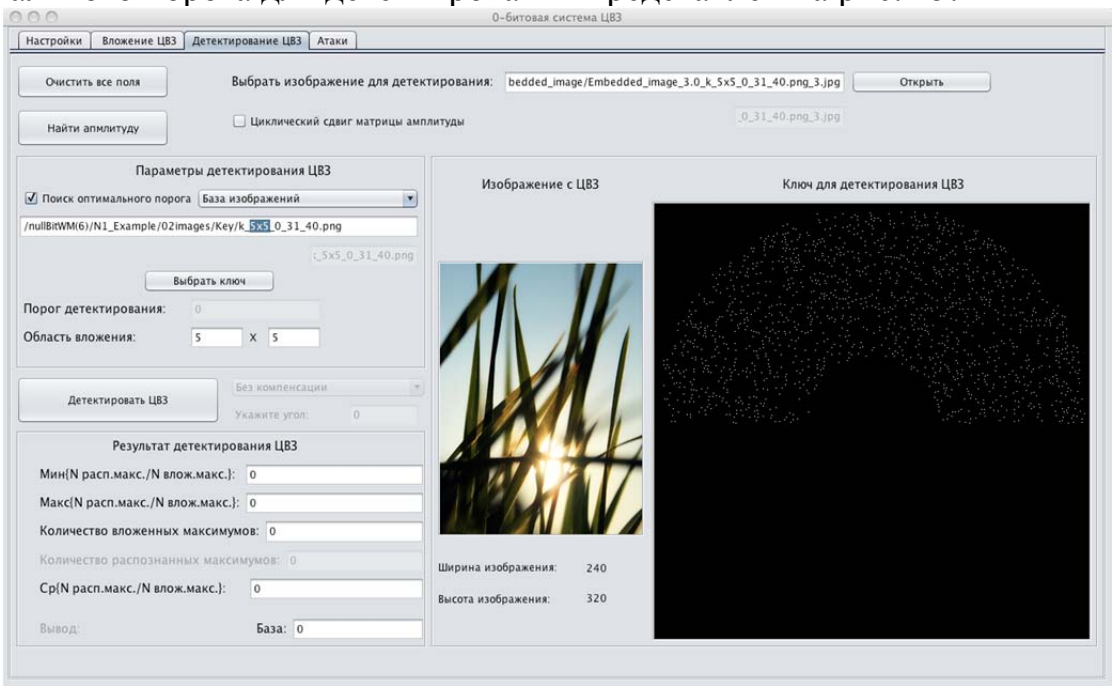

Рис. 25. Внешний вид вкладки «Детектирование ЦВЗ» при поиске оптимального порога для детектирования.

13. Найти оптимальный порог, нажав на кнопку «Детектировать ЦВЗ». Результат поиска оптимального порога представлен на рис. 26.

Оптимальный порог выбирается немного большим, чем максимальное отношение количества распознанных максимумов к количеству вложенных. Необходимые значения отображаются в поле «Результат детектирования ЦВЗ» в нижней части окна.

14. Снять выделение «Поиск оптимального порога» и указать оптимальный порог детектирования, полученный в пункте 13.

15. Произвести обнаружение водяного знака для выбранного в пункте 10 изображения (без преобразований), выбрав в выпадающем списке «Без компенсации» и нажав кнопку «Детектировать ЦВЗ».

Результаты детектирования отобразятся в поле «Результаты детектирования ЦВЗ».

Результат детектирования ЦВЗ представлен на рис. 27.

16. Перейти на вкладку «Атаки».

17. Выбрать изображение для преобразования из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Embedded_image**, нажав кнопку «Открыть» в верхней части окна.

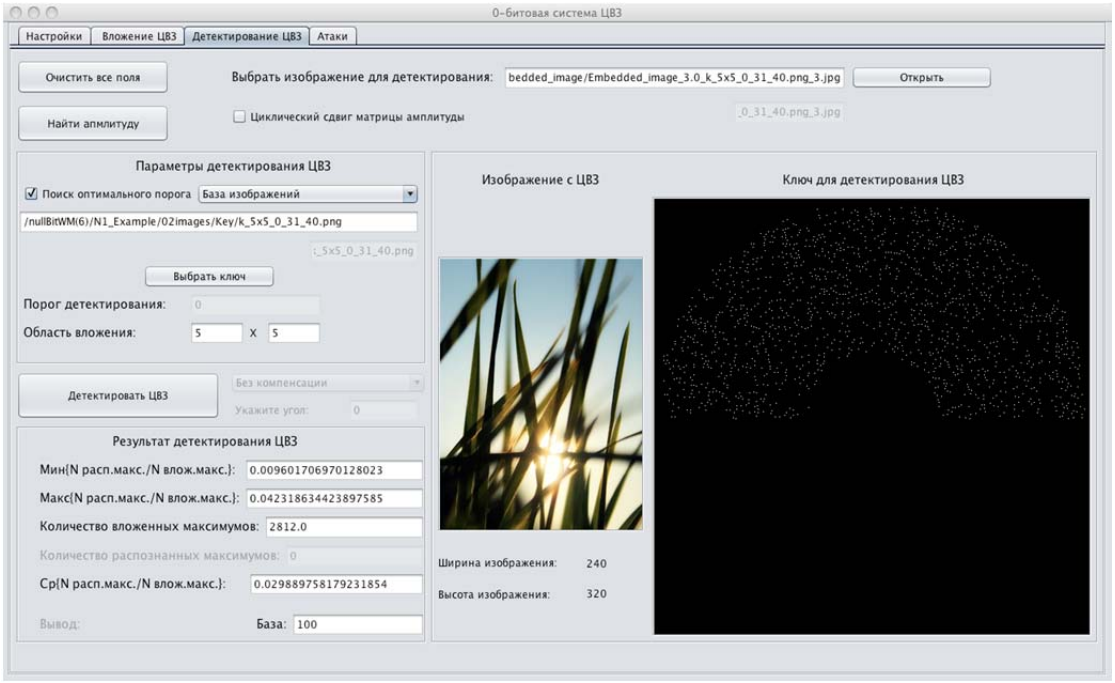

Рис. 26. Результат поиска оптимального порога.

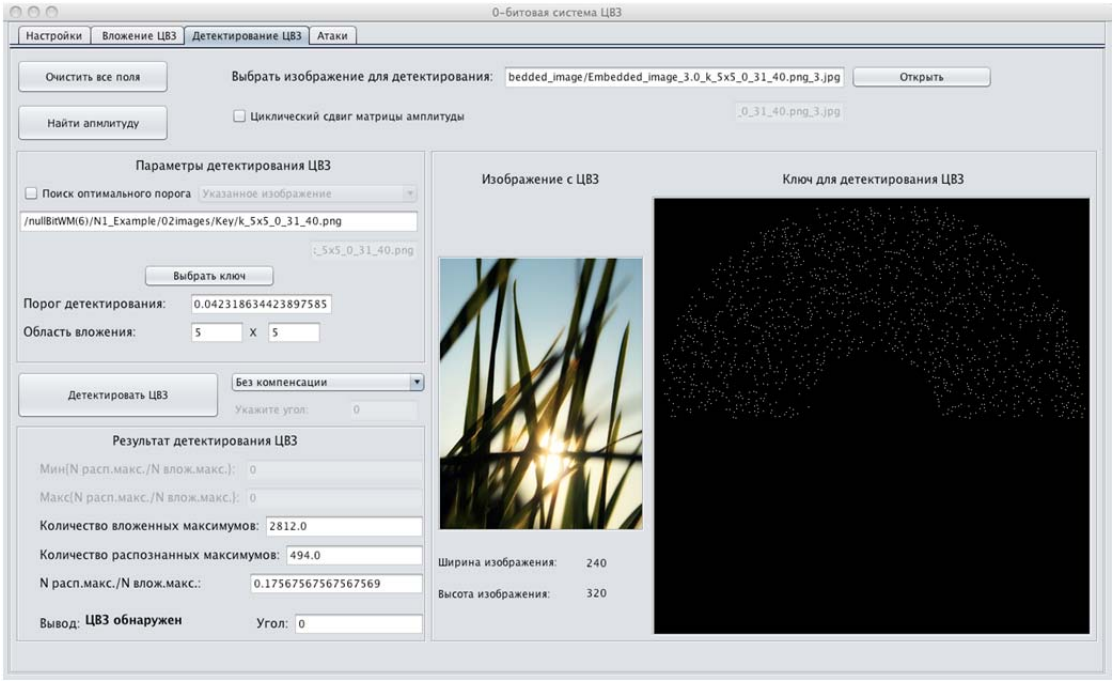

Рис. 27. Результат детектирования ЦВЗ в изображении с вложением (без преобразований) без компенсации поворота.

18. Выполнить поочерёдно преобразования изображений (удаление строк и столбцов, дублирование строк и столбцов, циклический сдвиг, вырезание

окна, выделение окна, поворот, зашумление, преобразование JPEG с показателем качества Q).

Внешний вид вкладки «Атаки» с результатом выполнения циклического сдвига по горизонтали и вертикали изображения с вложением представлен на рис 28; с результатом выполнения поворота изображения с вложением представлен на рис. 29.

Результаты всех преобразований автоматически сохраняются в папку **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Attacks**.

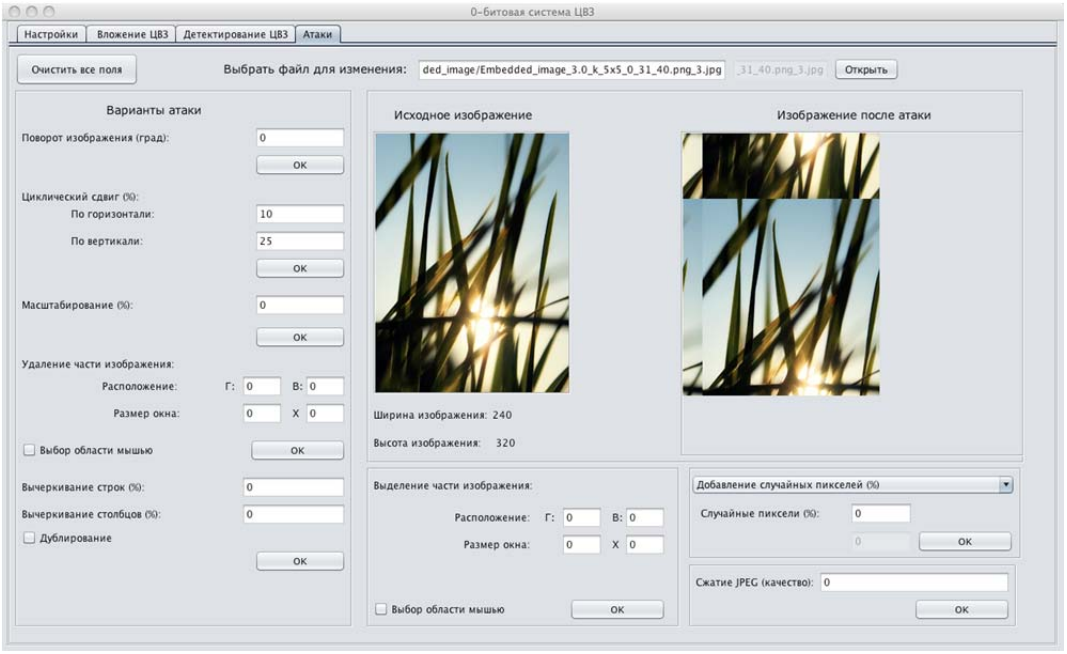

Рис. 28. Вид вкладки «Атаки» при выполнении циклического сдвига по горизонтали и вертикали изображения с вложением.

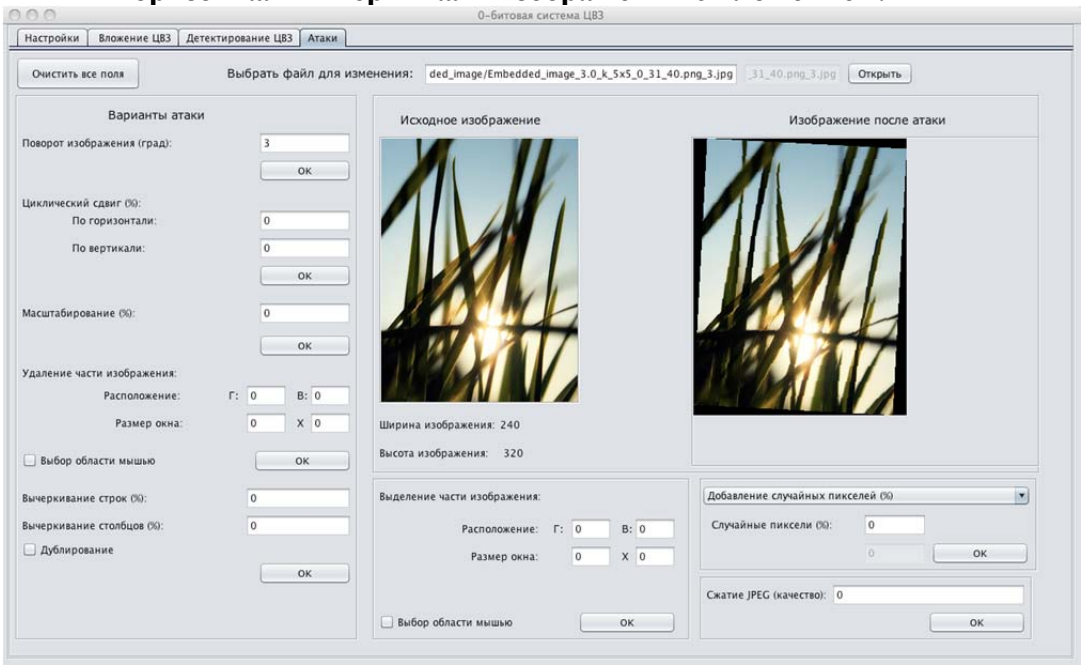

Рис. 29. Вид вкладки «Атаки» при выполнении поворота изображения с вложением.

19. Наблюдать изменение изображения после всех преобразований и возможность детектирования ЦВЗ при выборе истинного ключа из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Key**.

Для детектирования ЦВЗ в изображении после преобразования необходимо перейти на вкладку «Извлечение ЦВЗ» и повторить действия, описанные в пунктах 14-15, выбирая изображения для детектирования из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Attacks**.

Оптимальный порог для каждого ключа определяется только один раз (согласно пункту 13).

Результат детектирования ЦВЗ в изображении с вложением без компенсации поворота после циклического сдвига представлен на рис. 30; с компенсацией поворота в изображении с вложением после поворота представлен на рис. 31.

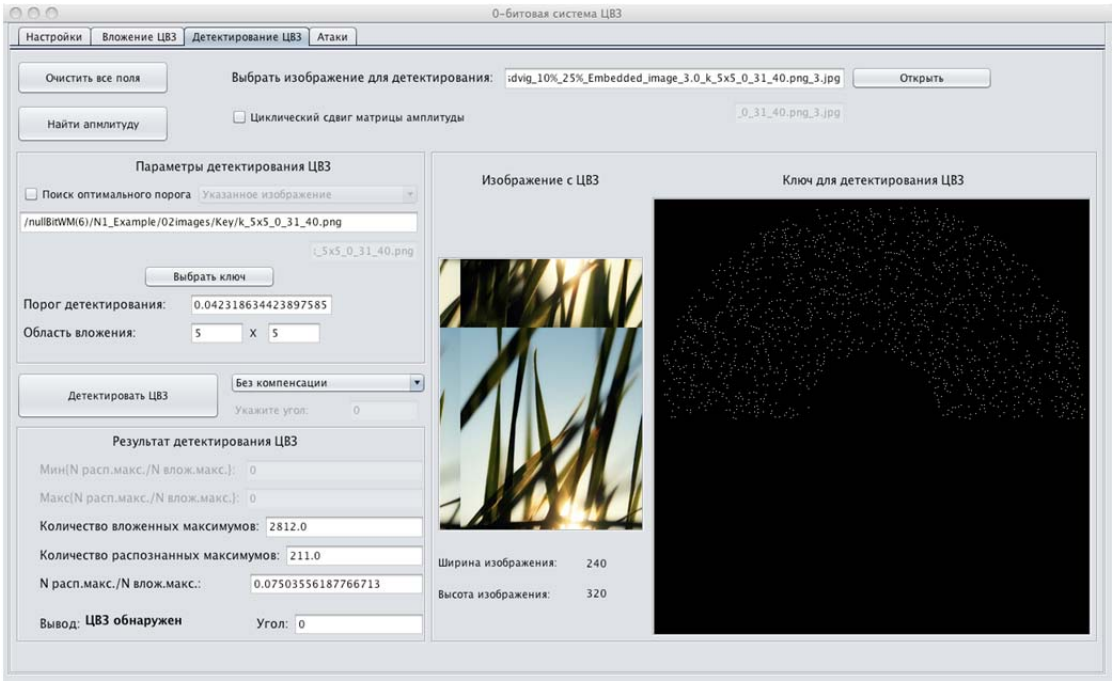

Рис. 30. Результат детектирования ЦВЗ без компенсации поворота при циклическом сдвиге изображения с вложением.

При детектировании ЦВЗ в изображении с поворотом необходимо выбрать в выпадающем списке «С компенсацией» и указать в поле ввода «Укажите угол» угол поворота, до которого будет проводиться проверка.

20. Повторить пункты 2-19 при других параметрах вложения и для другого изображения.

21. Попытаться обнаружить вложение ЦВЗ для изображения, в которое не проводилось вложение.

Для этого выбрать исходное изображение без вложения из папки **nullBitWM(6)/01images** и повторить пункты 11-15.

Результат детектирования ЦВЗ в изображении без вложения представлен на рис. 32.

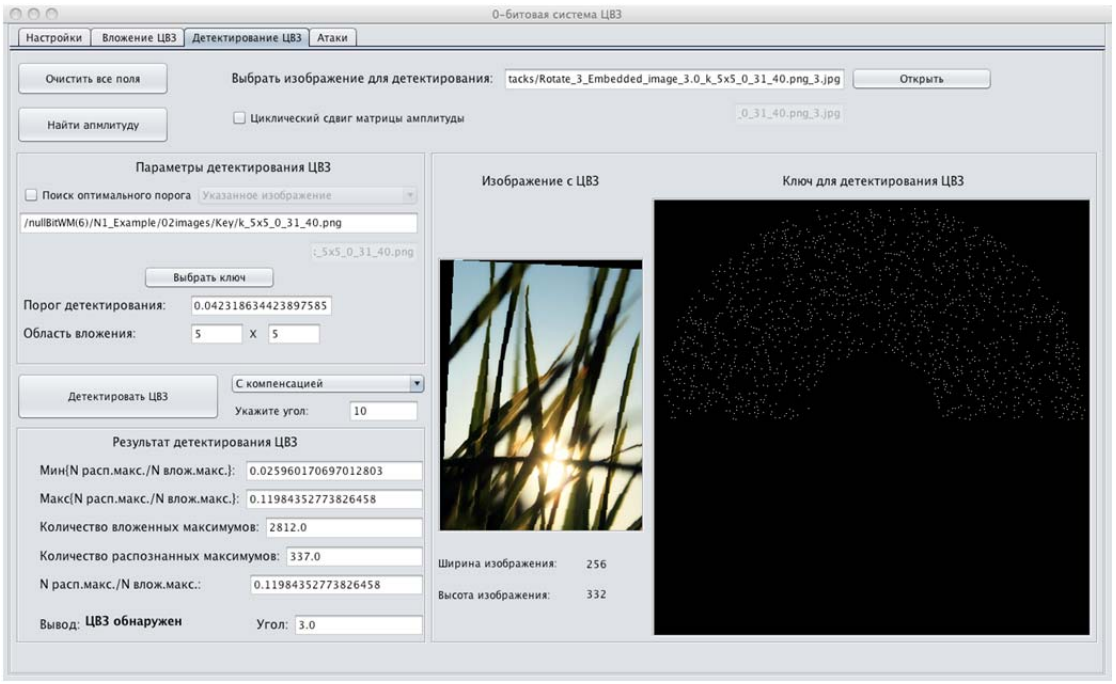

Рис. 31. Результат детектирования ЦВЗ с компенсацией поворота при повороте изображения с вложением.

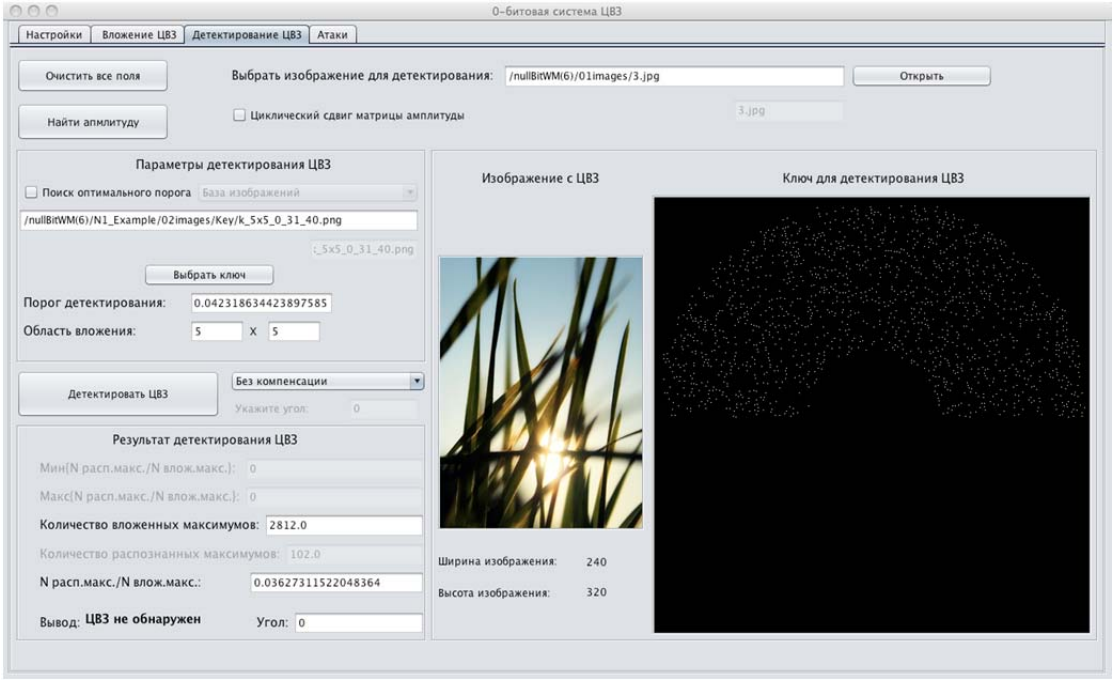

Рис. 32. Результат детектирования ЦВЗ в изображении без вложения.

22. Попытаться обнаружить вложение ЦВЗ при ложном ключе.

Для этого повторить пункт 5, изменив параметры генерации ключа и пп.10-15, выбрав ложный ключ из папки **nullBitWM(6)/N<номер бригады>_<Фамилия>/02images/Key**. Определить ложный ключ или нет можно по названию изображения с вложением, в котором указано название истинного ключа.

Внешний вид вкладки «Вложение ЦВЗ» с параметрами ложного ключа и окном графического отображения матрицы ключа и промежуточных матриц представлен на рис.33.

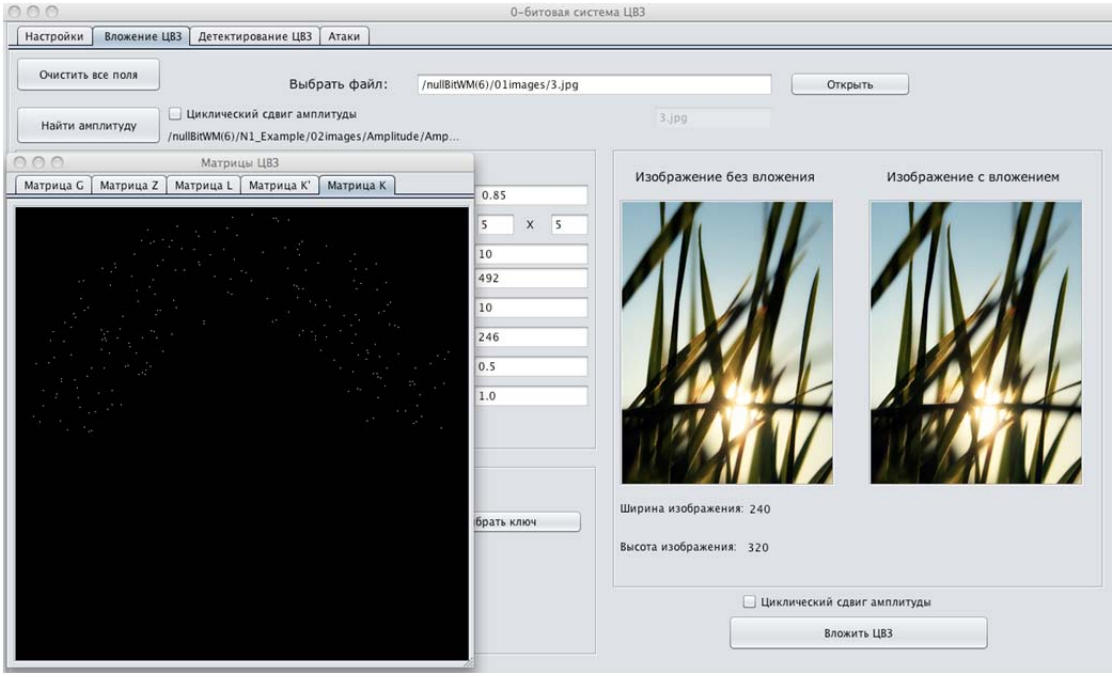

Рис. 33. Внешний вид вкладки «Вложение ЦВЗ» с параметрами ложного ключа и окном графического отображения матрицы ключа и промежуточных матриц.

Результат поиска оптимального порога для ложного ключа представлен на рис. 34.

Результат детектирования ЦВЗ в изображении с вложением при ложном ключе представлен на рис. 35.

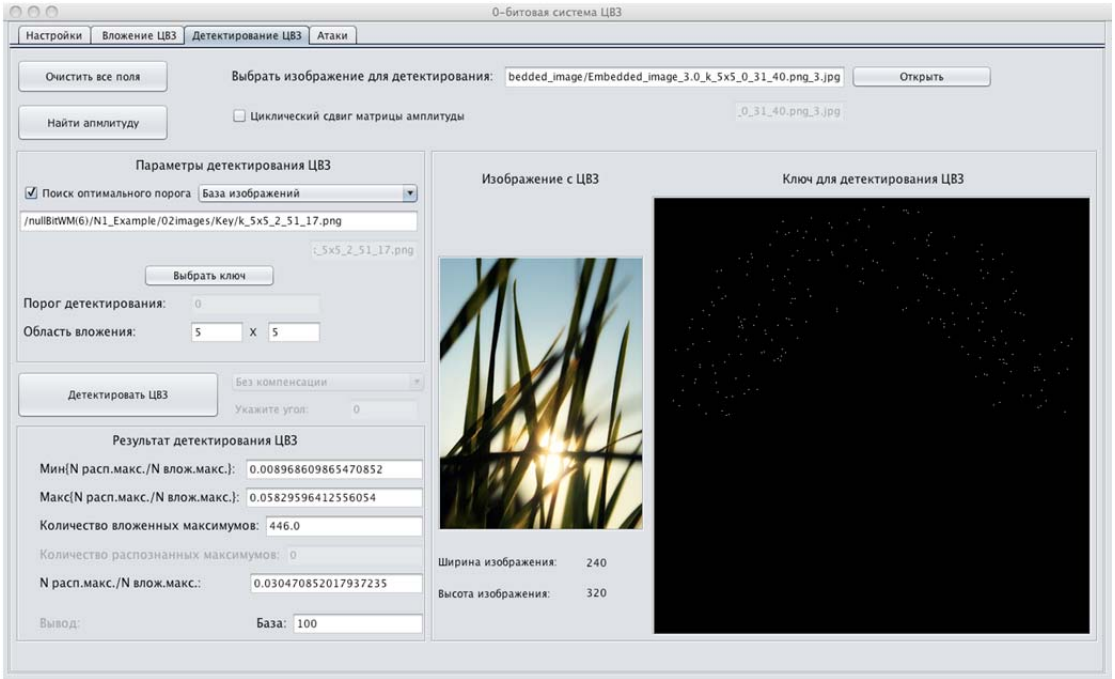

Рис. 34. Результат поиска оптимального порога для ложного ключа.

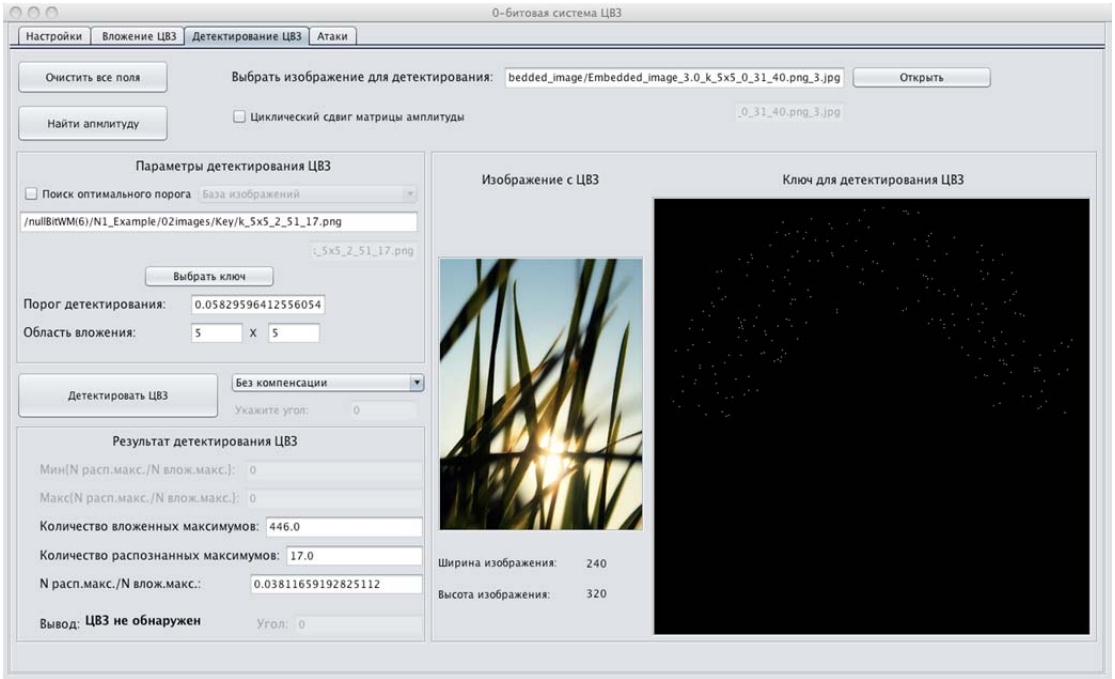

Рис. 35. Результат детектирования ЦВЗ в изображении с вложением при ложном ключе.

Отчет

1.Титульный лист.

2.Выбранные параметры вложения.

3.Результаты обнаружения идентификационного кода при различных преобразованиях и различном выборе параметров (в виде таблицы).

4.Изображения до и после вложения.

5.Результат обнаружения вложения на ложном ключе.

6.Выводы об устойчивости системы ЦВЗ к различным преобразованиям.

Контрольные вопросы

1.Что такое 0-битовый и многобитовый ЦВЗ?

2.Как выполняется вложение и извлечение ЦВЗ в исследуемой системе?

3.Какими характеристиками описывается эффективность системы 0 - битового ЦВЗ?

4.Почему система оказывается устойчивой к вырезанию фагмента изображения?

Лабораторная работа 7.
Исследование эффективности системы ЦВЗ - ШПС при атаке аддитивным шумом

Цель работы

Исследовать качество изображения после вложения ЦВЗ и возможности их извлечения после атаки аддитивным шумом.

Задание

1.Произвести вложение ЦВЗ в изображение с различными параметрами ШПС.

2.Выполнить атаку аддитивным шумом различного уровня .

3.Оценить визуально качество изображения после вложения ЦВЗ и после атаки.

4.Найти теоретическую и экспериментальную вероятности ошибок при извлечении ЦВЗ.

5.Рассчитать количество вкладываемых бит при различных параметрах ШПС.

Порядок выполнения

Для начала выполнения работы перейти в каталог, содержащий рабочую программу **ЛабСтег/AveragingSSS_light(7-8).** Запустить программу **AveragingSSS_light.exe**.

В первом столбце (Embedded FPs (PRSs)) показаны начальные символы ПСП, которые вкладываются в 10 копий изображения.

Второй столбец показывает результат обнаружения ЦВЗ при отсутствии атаки. В третьем столбце представлены результаты обнаружения ЦВЗ при коалиционной атаке C пользователей, причём предполагается, что в эту группу объединяются первые C пользователей.

В третьем столбце показаны ошибки в обнаружении ЦВЗ (1- есть ошибка, 0 – нет ошибки). Величина Pmi- означает частоту пропуска участника коалиции, а Pfa – частота ложного обнаружения участника коалиции из общего числа 10-ти пользователей. theor Pmi=Pfa даёт значение теоретических значений вероятностей пропуска, при выборе порога, обеспечивающее равенство её с вероятностью ложного обнаружения. «Steps» означает количество повторений тестирования при различных образцах аддитивного шума.

Pmean – показывает оценки вероятностей ошибок пропуска и ложного обнаружения при заданном пороге («Porog»).

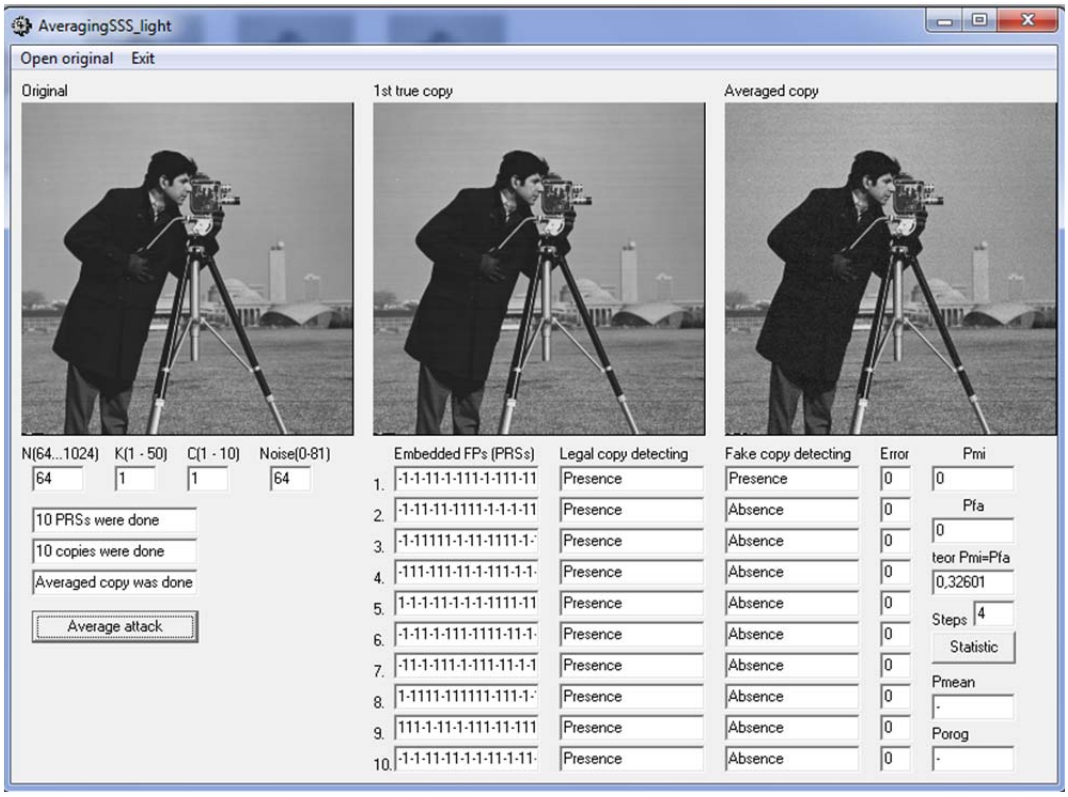

Рис. 36. Вид панели рабочей программы.

1.Ввести изображение (Cameraman), нажав кнопку “Open original”.

2.Установить параметр C=1(размер коалиции атакующих) на все время выполнения работы.

3.Установив N=256 (длина ШПС сигнала) и K=1 (амплитуда вложения ШПС), исследовать качество изображения после вложения и после атаки (визуально). а также вероятность ошибки извлечения ШПС по теории (theor Pmi=Pfa) и экспериментальную (Pmean) при изменении дисперсии (мощности) аддитивного шума атаки (Noise), изменяемой в пределах от 1 до 99 (5 значений). Рассчитать количество бит, вложенных в изображение.

4.Повторить п.3 при изменении K=5,10.

5.Повторить п.3 при K=1 и N=512 и 1024.

Отчет

1.Титульный лист.

2.Таблица значений теоретических и экспериментальных вероятностей ошибок по пп.3-5

3.Визуальная оценка качества изображения (по сравнению с оригиналом) после вложения ЦВЗ и после атаки (по 5-ти бальной шкале) для всех случаев.

4.Количество вложенных бит для всех случаев.

5.Выводы об эффективности (или нет) использования ЦВЗ ШПС с заданными параметрами.

Контрольные вопросы

1.Как выполняется вложение ЦВЗ-ШПС в область пикселей изображения?

2.Чем определяется качество изображения после вложения ЦВЗ и после атаки?

3.От каких параметров ШПС и атаки зависит вероятность ошибки при извлечении ЦВЗ?

4.Какими параметрами определяется количество вложенных бит (скорость вложения ЦВЗ)?

5.Какие атаки, кроме атаки аддитивным шумом , возможны на систему ЦВЗ-ШПС?

Лабораторная работа 8
Исследование эффективности системы ЦВЗ - ШПС при коалиционной атаке

Цель работы

Исследовать качество изображения после вложения ЦВЗ и возможности их извлечения после коалиционной атаки.

Задание

1. Произвести вложение ЦВЗ в изображение с различными параметрами ШПС .
2. Выполнить коалиционную атаку с различным числом участников.
3. Оценить визуально качество изображения после вложения ЦВЗ и после атаки.
4. Найти теоретическую и экспериментальную вероятности ошибок при извлечении ЦВЗ.
5. Рассчитать количество вкладываемых бит при различных параметрах ШПС.

Порядок выполнения

Для начала выполнения работы перейти в каталог, содержащий рабочую программу **ЛабСтег/AveragingSSS_light(7-8).** Запустить программу **AveragingSSS_light.exe**.

В первом столбце (Embedded FPs (PRSs)) показаны начальные символы ПСП, которые вкладываются в 10 копий изображения.

Второй столбец показывает результат обнаружения ЦВЗ без отсутствия атаки.В третьем столбце представлены результаты обнаружения ЦВЗ при коалиционной атаке С пользователей, причём предполагается, что в эту группу объединяются первые С пользователей.

В третьем столбце показаны ошибки в обнаружении ЦВЗ (1- есть ошибка, 0 – нет ошибки). Величина Pmi- означает частоту пропуска

участника коалиции, а Pfa – частота ложного обнаружения участника коалиции из общего числа 10-ти пользователей. theor Pmi=Pfa даёт значение теоретических значений вероятностей пропуска, при выборе порога, обеспечивающее равенство её с вероятностью ложного обнаружения. «Steps» означает количество повторений тестирования при различных образцах аддитивного шума.

Pmean – показывает оценки вероятностей ошибок пропуска и ложного обнаружения при заданном пороге («Porog»).

Рис. 37. Вид панели рабочей программы.

1.Ввести изображение (*Cameraman)* , нажав кнопку "*Open original*".

2.Используя параметры *N* (длина ШПС сигнала) , *K* (амплитуда вложения) и *Noise* (мощность аддитивного шума) , установленные по умолчанию , исследовать качество изображения после вложения и атаки (визуально) . а также вероятность ошибки извлечения ШПС по теории (*theor Pmi=Pfa*) и экспериментальную (*Pmean*) при различном количестве участников коалиции (*C*), изменяемом в пределах от 1 до 10 (5 значений). Рассчитать количество бит , вложенных в изображение.

3.Повторить п.3 при изменении K=5,10.

4.Повторить п.3 при K=1 и N=512 и 1024.

Отчет

1.Титульный лист.

2.Таблица значений теоретических и экспериментальных вероятностей ошибок по пп.2-4

3.Визуальная оценка качества изображения (по сравнению с оригиналом) после вложения ЦВЗ и после атаки для всех случаев (по 5-ти бальной шкале).

4.Количество вложенных бит для всех случаев.

5.Выводы об эффективности (или нет) использования ЦВЗ- ШПС с заданными параметрами.

Контрольные вопросы

1.Как выполняется вложение ЦВЗ-ШПС в область пикселей изображения?

2.Чем определяется качество изображения после вложения ЦВЗ и после коалиционной атаки?

3.От каких параметров ШПС и атаки зависит вероятность ошибки при извлечении ЦВЗ?

4.Какими параметрами определяется количество вложенных бит (скорость вложения ЦВЗ)?

5.Какие еще атаки, кроме атаки аддитивным шумом и коалиционной атаки , возможны на систему ЦВЗ-ШПС?

Лабораторная работа 9
Изучение системы аутентификации изображений, использующих ЦВЗ

Цель работы

Изучить процедуру аутентификации изображений с вложением аутентификатора, полученного как имитовставка для шифра DES.

Задание

1. Произвести вложение аутентификатора и дополнительной информации.
2. Проверить корректность извлечения информации и подтверждение подлинности изображения при отсутствии искажений.
3. Проверить отсутствие подтверждения подлинности изображения при наличии произвольно вносимых искажений.

Порядок выполнения

Для начала работы перейти в каталог, содержащий рабочие программы **ЛабСтег/Authentication(9)**, ознакомиться с описанием алгоритмов и их программных реализаций.

1.Запустить программу вложения аутентификатора и дополнительной информации (Вложение.exe).

2.Выбрать изображение для вложения (открыть файл), наблюдать изображение.

3.Произвести вложение (ввести дополнительное буквенное сообщение и 8-буквенный произвольный ключ аутентификатора). Наблюдать изображение с вложением. Сравнить его с оригиналом.

4.Выбрать опцию «не портить файл с вложением».

5. Произвести извлечение информации и проверить подлинность изображения (Извлечение.exe => Извлечение => ключ DES (прежний))

Убедиться в успешной аутентификации и правильном извлечении дополнительного сообщения. Наблюдать восстановленное покрывающее сообщение (изображение).

6.Произвести искажение изображения с вложением (Вложение.exe => Открыть файл => Вложение =>испортить файл с вложением =>произвести искажение файла с вложением).

7.Проверить, что искаженное сообщение не аутентифицируется.

8.Повторить пп.1-5 при неправильном выборе ключа.

9.Повторить пп.1-7 для другого дополнительного сообщения.

Отчет

1.Титульный лист.

2.Текст вложенного сообщения и ключа DES.

3.Визуальное сравнение исходного изображения и изображения с вложением.

4.Результаты проверки подлинности изображения и выводы.

Контрольные вопросы

1.В чём состоит преимущество аутентификации с использованием ЦВЗ?

2.Какова основная проблема при разработке систем аутентификации с использованием ЦВЗ?

3.Существуют ли атаки на рассматриваемую систему аутентификации?

4.Каковы основные показатели эффективности данной системы аутентификации?

Литература

1.В.И.Коржик, «Основы стеганографии», http://ibts.sut.ru/materialy.

2.Грибунин В.Г. Цифровая стеганография/В.Г. Грибунин, И.Н. Оков, И.В. Туринцев //— М.: Солон-Пресс, 2002.

3.Barni M.Watermarking system Engineering /M. Barni, F. Bartolini // Maral Dekker, 2004.

4. Cox I., et all, Digital Watermarking / MK, 2002.

Валерий Иванович Коржик
Александр Игоревич Кочкарев

ОСНОВЫ СТЕГАНОГРАФИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Ответственный редактор ***В.И. Коржик***

Редактор ***Л.А. Медведева***

План 2012 г., п. 7

Подписано к печати 24.10.2011
Объем 32усл. печ. л. Тираж?? экз. Зак. ??
Издательство СПбГУТ. 191186 СПб., наб. р. Мойки, 61
Отпечатано в СПбГУТ

В. И. Коржик
А. И. Кочкарев

ОСНОВЫ СТЕГАНОГРАФИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

САНКТ-ПЕТЕРБУРГ
2013