УДК 681.3

А.В. Питолин, Ю.П. Преображенский, О.Н. Чопоров

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ

Воронежский государственный технический университет, Воронеж, Россия

Стеганографические методы применяют для того, чтобы скрыть сам факт существования определенных сообщений. В работе проведен анализ ключевых понятий, которые используются в стеганографических методах преобразования информации. Рассмотрены особенности стеганографических методов сокрытия информации в графических файлах. Разработана модель угроз несанкционированной передачи информации с применением методов стеганографического преобразования информации, использующих графические контейнеры. В статье приведена классификационная схема угроз несанкционированной передачи информации с применением методов стеганографического преобразования. Проведен эксперимент по выявлению наиболее эффективных способов противодействия несанкционированному доступу к информации. Было установлено, что почти все способы противодействия несанкционированному доступу по времени воздействия не превышают двух секунд. Выделены способы противодействия по времени воздействия, которые не превышают 0,7 секунды. Эксперимент проводился среди 10 человек при помощи программы S-tools и разработанного программного продукта AntiStego. В работе приведен алгоритм работы программы «AntiStego» вместе с описанием программных модулей, реализующих противодействие несанкционированному доступу. Предложена обобщенная схема проведения эксперимента по противодействию несанкционированной скрытой передачи информации.

Ключевые слова: защита информации, стеганографический подход, несанкционированный доступ.

Введение

Задача защиты информации решалась во все времена на протяжении истории человечества. Уже в Древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. В отличие от криптографии, целью которой является сокрытие смысла сообщения путём шифрования, стеганографические методы используются для сокрытия самого факта существования такого сообщения.

Первые следы применения стеганографических методов защиты информации теряются в глубокой древности [1]. Известны примеры, когда в качестве методов сокрытия сообщений использовались покрытые воском дощечки, спичечные коробки и даже головы рабов. Хорошо известны различные способы скрытого письма между строк обычного не защищаемого письма: от применения молока до использования сложных химических реакций с последующей обработкой при чтении. Другие методы стеганографии включают использование микрофотоснимков,

незначительные различия в написании рукописных символов, маленькие проколы определенных напечатанных символов и множество других способов по скрытию истинного смысла тайного сообщения в открытой переписке.

В настоящее время развитие стеганографии вызвано, прежде всего, распространением персональных компьютеров, всевозможных мультимедийных приложений и развитием информационно-телекоммуникационных систем, а также сетей общего пользования. Современную стеганографию правильно было бы называть компьютерной или цифровой стеганографией, так как скрытые сообщения обычно встраиваются в данные, представленные в некотором цифровом (электронном) формате.

Анализ основных понятий в стеганографических методах преобразования информации

Основными стеганографическими понятиями являются сообщение и контейнер. Термин "контейнер" употребляется в отечественной литературе большинством авторов, поскольку является дословным переводом устоявшегося английского термина "container", обозначающего несекретную информацию, которую используют для сокрытия сообщений [2].

Контейнером b (где $b \in B$ - множеству всех контейнеров) называют несекретную информацию, которую используют для сокрытия сообщений. В компьютерной стеганографии в качестве контейнеров могут быть использованы различные оцифрованные данные: растровые графические изображения, цифровой звук, цифровое видео, всевозможные носители цифровой информации, текстовые и другие электронные документы.

Сообщением m называют секретную информацию, наличие которой необходимо скрыть в контейнере. Всевозможные сообщения объединяются в пространство сообщений M.

Ключ k представляет собой некоторую секретную информацию, известную только законному пользователю. Через K обозначается множество всех допустимых секретных ключей.

В общем случае в качестве сообщений, контейнеров и ключей могут быть использованы объекты произвольной природы. В наиболее развивающейся в последнее время компьютерной стеганографии в качестве сообщений, контейнеров и секретных ключей используют двоичные последовательности, т.е. $M=Z_2^n$ для некоторого фиксированного целого n, $B=Z_2^q$ и $K=Z_2^p$, при этом $q>>n$ [3].

Пустой контейнер (или, еще говорят, немодифицированный контейнер) – это некоторый контейнер b, не содержащий сообщения. Заполненный контейнер (или соответственно модифицированный

контейнер) – это контейнер b, содержащий сообщение m, в дальнейшем $b_{m,k}$ (или b_m для случая бесключевой системы).

Стеганографическим преобразованием над ними принято называть два преобразования: прямое стеганографическое преобразование $F{:}M{\times}B{\times}K{\to}B$ и обратное стеганографическое преобразование $F^{-1}{:}B{\times}K{\to}M$, сопоставляющие соответственно тройке (сообщение, пустой контейнер, ключ) контейнер результат и паре (заполненный контейнер, ключ) - исходное сообщение, причем

$$F(m,b,k)=b_{m,k},\ F^{-1}(b_{m,k},k)=m, \text{ где } m\in M;\ b,\ b_{m,k}\in B;\ k\in K.$$

Стеганографической системой называют $S = (F,\ F^{-1},\ M,\ B,\ K)$ совокупность сообщений, секретных ключей, контейнеров и связывающих их преобразований. Отметим, что приведенное определение стеганографической системы принято считать современным. Существует более ранняя – классическая схема [4], являющаяся частным случаем данной схемы. Ее отличительной особенностью является отсутствие зависимости от секретного ключа, т.е.:

$$F(m,b)=b_m,\ F^{-1}(b_m)=m, \text{ где } m\in M;\ b,\ b_m\in B.$$

Под внедрением (сокрытием) сообщения с помощью системы S в контейнер b понимают применение прямого стеганографического преобразования F к конкретным m, b и k. Тогда извлечение сообщения есть ничто иное, как применение обратного стеганографического преобразования с теми же значениями аргументов [5].

Скрытость (undetectability, stegosecurity) встроенной информации – это основополагающее свойство стегосистемы, которое характеризует незаметность и невыявляемость факта скрытной передачи информации.

Анализ стеганографических методов сокрытия информации в графических файлах

Современные стеганографические методы сокрытия информации в графических файлах базируются на модификации цифрового представления графических изображений, выступающих в роли контейнеров.

По способу происхождения графические изображения принято делить на оцифрованные и неоцифрованные (полученные при помощи компьютерных программ). В современных стеганографических системах в качестве контейнеров выступают, прежде всего, оцифрованные изображения, так как они обладают свойствами, которые могут позволить произвести незаметное внедрение данных [6-8].

Интенсивное развитие стеганографических методов для изображений связано со следующими факторами:

- актуальностью задачи защиты высококачественных цифровых изображений от незаконного копирования и распространения, роста роли цифровых технологий в области развлечений;
- требованием относительно большого объёма информации для цифровых изображений в интересах представления цветного изображения с хорошим качеством и разрешением;
- наличием априорных сведений о размерах контейнера;
- существованием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации;
- слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображений, его яркости, контрастности, содержанию в нём шума, искажениям вблизи контуров;
- проработанность методов цифровой обработки изображений и цифровых форматов представления изображений.

Стеганографические методы сокрытия данных в изображении могут быть разделены на три класса [9, 10]:

- методы преобразования в пространственно-временной области;
- методы распределения по спектру;
- методы использования матриц промежуточных вычислений процесса сжатия графической информации.

Далее эти методы рассматриваются более подробно.

Основой методов сокрытия информации в пространственно-временной области являются преобразования, осуществляемые в матричном представлении оцифрованной аналоговой информации.

Первые открытые публикации результатов исследований и методов преобразования в пространственно-временной области относятся к 1989 году.

В настоящее время известны следующие методы данного класса:

- сокрытия в наименьших значащих битах (НЗБ-метод);
- сокрытие информации на основе стеганографического метода модификации индексного формата представления (сортировка и редукция палитры);
- сокрытие информации на основе автокорреляционных методов.

Стеганографические методы распределения по спектру (расширение спектра) [11] для маскирования сигнала-носителя используют широкополосный шум.

Адекватной моделью шума, присутствующего в изображениях, оцифрованных при помощи фотоэлектронных систем (таких как сканеры, цифровые фотоаппараты и видеокамеры и др.), является аддитивный белый гауссовский шум. При использовании в качестве стегоконтейнеров изображений, полученных в когерентном излучении, шум может быть

смоделирован в виде гранулированного шума [11], который характерен для когерентного излучения в интервале от микроволн до видимой области спектра. При необходимости, при помощи изменения модели шума, стеганографические методы расширения спектра могут применяться к другим типам стегоконтейнеров.

Модель угроз несанкционированной передачи информации с применением методов стеганографического преобразования информации использующих графические контейнеры

Модель угроз несанкционированной передачи информации с применением методов стеганографического преобразования данных разрабатывалась в интересах упорядочения представлений о составе и характеристиках таких угроз в КС и учета характеристик таких угроз в последующем при разработке предложений по способам противодействия несанкционированной передаче с использованием методов СПИ. Разработка модели проведена на основе результатов анализа состояния и перспектив развития современных методов стеганографии и характеристик существующего программного обеспечения, предназначенного для стеганографического сокрытия данных в графических и аудиофайлах [2].

Под угрозой несанкционированной передачи информации (НПИ) с применением методов стеганографического преобразования данных понимается определенная совокупность условий и факторов, при реализации которых возникает возможность несанкционированной передачи информации в КС. В описание угрозы НПИ входит наименование источника угрозы (нарушителя), описание используемого метода СПИ и возможного канала передачи информации, содержание или характеристика информации, несанкционированно передаваемой в КС, оценку последствий реализации угрозы НПИ.

Модель угроз включает в себя модель нарушителя, описание каналов передачи и ситуаций, в которых возможна НПИ с применением СПИ, краткую обобщенную характеристику последствий.

Структура модели угроз несанкционированной передачи информации с применением методов стеганографического преобразования данных, использующих графические контейнеры приведена на Рисунке 1.

Классификационная схема угроз НПИ представлена на Рисунке 2. Проведение машинного эксперимента по противодействию несанкционированной скрытой передачи информации в компьютерных сетях.

С целью определения наиболее эффективных и перспективных способов противодействия несанкционированной передачи информации в компьютерных сетях с помощью стеганографии, необходимо провести эксперимент. Для его проведения необходимо следующее:

Рисунок 1 – Структура модели угроз несанкционированной передачи информации с применением методов стеганографического преобразования данных, использующих графические контейнеры

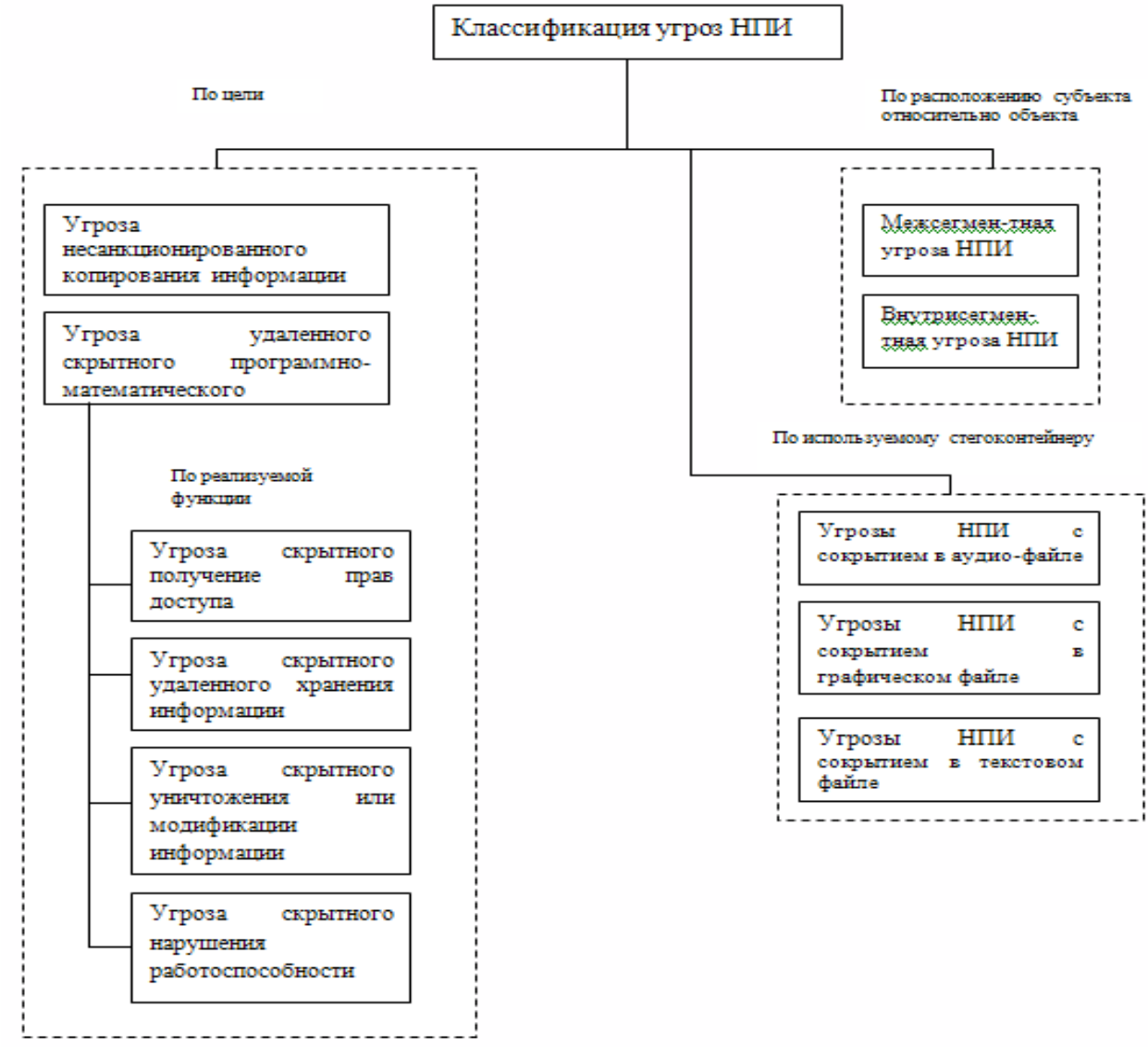

Рисунок 2 – Классификационная схема угроз несанкционированной передачи информации с применением методов ее стеганографического преобразования

- выбрать несколько наиболее перспективных программных продуктов (ПП), которые реализуют сокрытие информации в графических контейнерах;
- определить одинаковые, для всех выбранных ПП, стегоконтейнер и информацию, подлежащую сокрытию;
- провести сокрытие информации в стегоконтейнер;
- осуществить противодействия НПИ с наименьшими демаскирующими признаками (СКО разности стегоконтейнеров) при наилучшем результате противодействия;
- сформировать сводную таблицу, содержащую сравнительные характеристики способов НПИ.
- сделать вывод о наиболее эффективных и перспективных способах противодействия НПИ.

В качестве средств, реализующих методы стеганографии в графических файлах, выбраны MagicEncoder и S-tools. Средством, реализующим способы противодействия НПИ, был программный продукт AntiStego. Макет стенда, на котором проводился эксперимент приведен на Рисунке 3. Результаты эксперимента сведены в Таблице 1 для MagicEncoder и таблице 2 для S-tools.

В качестве графического стегоконтейнера был взят файл формата *.bmp с разрешением 10024x768 и размером в 2359350 байт.

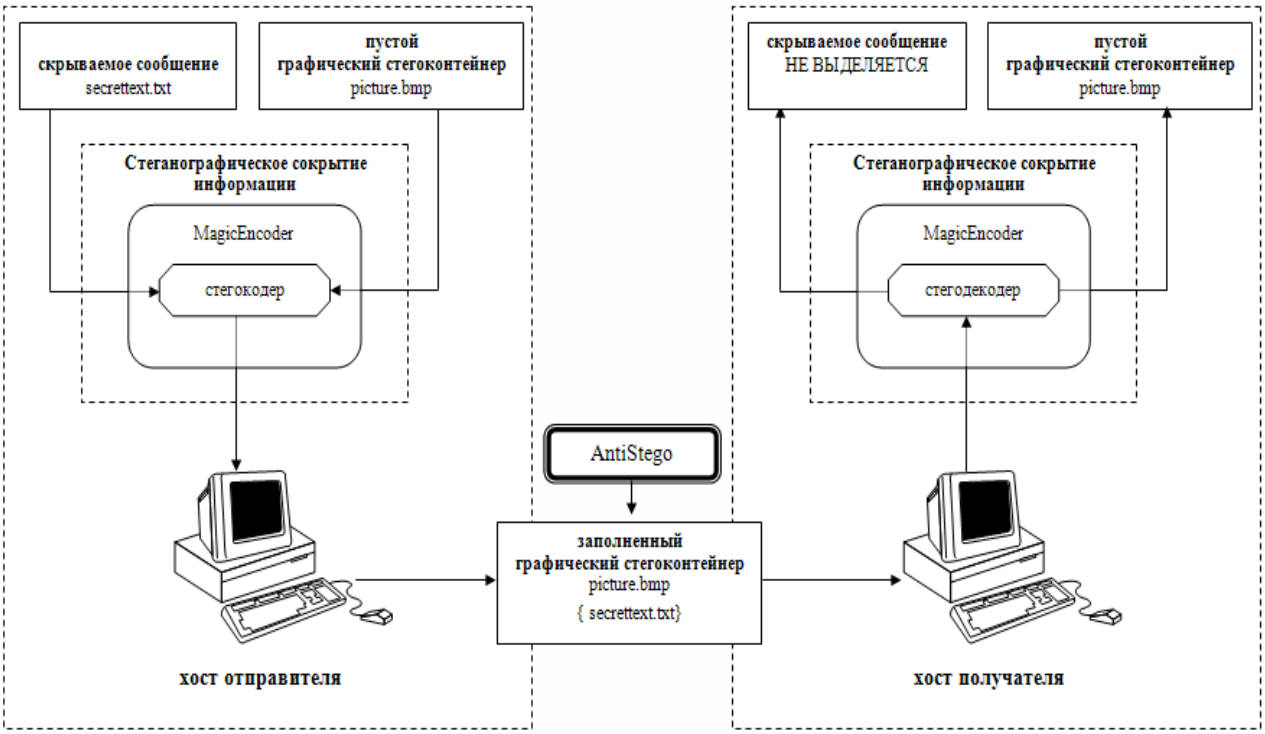

Рисунок 3 – Макет стенда для проведения эксперимента по выявлению наиболее эффективных способов противодействия НСПИ

Таблица 1 – Сводная таблица характеристик способов противодействия НПИ с помощью MagicEncoder

Способы противодействия НПИ	Факт противодействия (+ - полное уничтожение скр инф.)	Степень искажения информации (P – вероятность искажения)	Время воздействия (сек)	Демаскирующие признаки		
				Визуальное изменение стегоконтейнера. (СКО)	Объем стегоконтейнера (байт)	Разрешение (+ - прежнее)
Волновая компрессия (1 итерация)	+	P=0,015	0,42849328	0,48	2359350	+
JPEG компрессия (качество 100)	+	P=0,389	0,25721819	0,79	2359350	+
Верт. отобр.	+	P=0,501	0,00577461	35,16	2359350	+
Гор. отобр.	+	P=0,002	0,08018659	37,87	2359350	+
Маштабирование (+7,+7) 101,783%	+	P=0,0002	0,06079458	4,77	2402634	1033x 775
Поворот -0,01град	+	P=0,001	0,10806598	2,8	2359350	+
Смещение (0;-1)	+	P=0,001	0,02609116	11,06	2359350	+
Гаусовское размытие	97% - искажения скр. Инф.	P=0,283	0,55453216	3,11	2359350	+
Двумерный рекуррентный фильтр (α=0,5, q=10)	+	P=0,251	0,56175378	0,02	2359350	+
Медианный фильтр (порог 10, окрест-ность 3*3)	+	P=0,221	1,14793916	4,71	2359350	+
Равномерная масочная фильтрация	+	P=0,358	0,52818569	6,87	2359350	+
Равномерное размытие	98% - искажения скр. инф.	P=0,399	0,57614215	6,92	2359350	+
Равномерный шум	+	P=0,313	0,30598487	0,5	2359350	+
Гаусовский шум	+	P=0,196	1,75350216	0,45	2359350	+

Таблица 2 – Сводная таблица характеристик способов противодействия НПИ с помощью S-tools

Способы противодействия НПИ	Факт противодействия (+ - полное уничтожение скр инф.)	Степень искажения информации (P – вероятность искажения)	Время воздействия (сек)	Демаскирующие признаки		
				Визуальное изменение стегоконтейнера. (СКО)	Объем стегоконтейнера (байт)	Разрешение (+ - прежнее)
Волновая компрессия (1 итерация)	+	P=0,015	0,42849328	0,48	2359350	+
JPEG компрессия (качество 100)	+	P=0,389	0,25721819	0,79	2359350	+
Верт. отобр.	+	P=0,501	0,00577461	35,16	2359350	+
Гор. отобр.	+	P=0,002	0,08018659	37,87	2359350	+
Маштабирование (+1,+1) 100,228%	+	P=0,0002	0,03437682	4,7	2365578	1025X769
Поворот -0,01град	+	P=0,001	0,10806598	2,8	2359350	+
Смещение (0;-1)	+	P=0,001	0,02609116	11,06	2359350	+
Гаусовское размытие	+	P=0,283	0,55453216	3,11	2359350	+
Двумерный рекуррентный фильтр (α=0,5, q=10)	+	P=0,251	0,56175378	0,02	2359350	+
Медианный фильтр (порог 10, окрестность 3*3)	+	P=0,221	1,14793916	4,71	2359350	+
Равномерная масочная ф.	+	P=0,358	0,52818569	6,87	2359350	+
Равномерное размытие	+	P=0,399	0,57614215	6,92	2359350	+
Равномерный шум	+	P=0,313	0,30598487	0,5	2359350	+
Гаусовский шум	+	P=0,196	1,75350216	0,45	2359350	+

Таким образом, из Таблицы 1 и 2 видно, что почти все способы противодействия НПИ по времени воздействия не превышают 2 секунд.

Однако если речь идет об обработке нескольких картинок, то 2 секунды на обработку одной пусть даже с разрешением 1024x768 это много. В связи с этим выделим способы противодействия НПИ по времени воздействия, которые не превышают 0,7 секунды:

- волновая компрессия (1 итерация) – 0,42849328 с;
- JPEG компрессия (качество 100) – 0,25721819 с;
- вертикальное отображение – 0,00577461 с;
- горизонтальное отображение – 0,08018659 с;
- масштабирование (+1,+1) 100.228% - 0,03437682 с;
- поворот 0,01град – 0,10806598 с;
- смещение (0;-1) – 0,02609116 с;
- гаусовское размытие – 0,55453216 с;
- двумерный рекуррентный (α=0,5, q=10) – 0,56175378 с;
- равномерная масочная – 0,52818569 с;
- равномерное размытие – 0,57614215 с;
- равномерный шум – 0,30598487 с.

Далее необходимо выделить те способы противодействия СПИ, которые привносят наименьшее искажения стегоконтейнеру. Для этого был введен параметр СКО разности изображений до противодействия и после него. В нашем эксперименте он колеблется от 0,02 до 37,87. Как определить границы, которые будут говорить о том, насколько легко выявить факт противодействия способам СПИ. Для этого был проведен следующий эксперимент.

Был сформирован ряд изображений, отличающихся от оригинала определенным значением СКО. Чем выше СКО, тем более искаженной была картинка. В эксперименте участвовало 10 человек, задача которых была определить из двух предложенных картинок факт различия между собой. Как только человек увидел картинки разными это фиксировалось. Таким образом, была сформирована следующая шкала демаскировки (Рисунок 4) на базе СКО разности изображений.

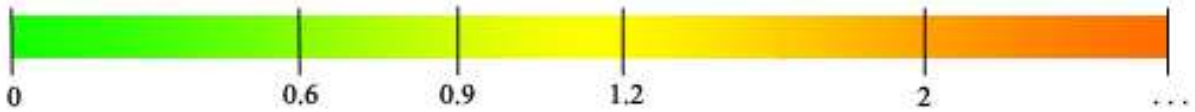

Рисунок 4 – Шкала демаскировки

где (0;0,6) – 1-й уровень скрытности, когда 0 – человек из 10 увидели, что предложенная пара изображений содержит разные картинки;
[0,6;0,9) – 2-й уровень скрытности, когда 1 – человек из 10 увидел, что предложенная пара изображений содержит разные картинки;
[0,9;1,2) – 3-й уровень скрытности, когда 3 – человека из 10 увидели, что предложенная пара изображений содержит разные картинки;

[1,2;2) – 4-й уровень скрытности, когда 5 – человек из 10 увидели, что предложенная пара изображений содержит разные картинки;
[2;∞) –5-й уровень скрытности, когда 6 – человек из 10 увидели, что предложенная пара изображений содержит разные картинки.

Выберем способы противодействия НПИ СКО разности изображений, которых удовлетворяет первому уровню скрытности:

- волновая компрессия (1 итерация) – 0,48;
- двумерный рекурентный фильтр (α=0,5, q=10) – 0,25;
- равномерный шум – 0,5.

Таким образом, определилась тройка наиболее эффективных способов противодействия НПИ в компьютерных сетях. Но наибольшего внимания с точки зрения перспективных способов НПИ заслуживает двумерный рекурентный фильтр, так как обладает самым низким СКО разности стегоконтейнеров.

С целью значительного понижения времени осуществления противодействия НПИ можно прибегнуть к следующим подходам:

- распараллелить вычисления (распоточить - создать по одному потоку на процессор и пусть каждый поток выполняет обработку своей части картинки, в этом случае получим выигрыш на многопроцессорной машине);
- аппаратная реализация алгоритма.

Далее проведен эксперимент (Рисунок 5) по предотвращению несанкционированной скрытой передачи информации нарушителем нулевого уровня с ограниченным ресурсом времени, использующим в качестве средства, реализующего методы стеганографии, программу S-tools.

Предположим, нарушитель хочет передать в глобальную компьютерную сеть [12, 13], некоторую информацию, имеющую ограниченное пользование.

С целью недопущения несанкционированной передачи информации, произведем воздействие двумерной рекуррентной фильтрацией как наиболее эффективного способа противодействия НПИ реализуемого программой AntiStego.

Скрытый текст, передаваемый нарушителем после воздействия двумерной рекуррентной фильтрации реализуемой программой AntiStego невозможно распознать.

Таким образом, было успешно реализовано противодействие несанкционированной скрытой передачи информации нарушителем нулевого уровня с ограниченным ресурсом времени, использующим в качестве средства, реализующего методы стеганографии, программу S-tools (Рисунок 5).

Основные характеристики программного продукта AntiStego, реализующего противодействие несанкционированной скрытной передаче информации с использованием стеганографических методов.

С помощью программного продукта можно:

Проводить исследования стеганографических методов преобразования информации в графических файлах *.bmp, *.gif, *.jpg форматов на устойчивость к способам противодействия стеганографического сокрытия информации.

1) Использовать в качестве стегоконтейнеров наиболее распространенные форматы графических файлов, таких как: *.bmp, *.gif, *.jpg.
2) Реализовывать различные способы противодействия НСПИ.
3) Производить сбор статистики обработки стегоконтейнеров: подсчет среднеквадратичного отклонения модифицированного или уничтоженного скрытого сообщения, подсчет вероятности ошибок модифицированной информации, времени реализации способа противодействия, размера файла и полотна изображения до и после наложения заданного способа противодействия.
4) Проводить удобный визуальный анализа стегоконтейнеров, через возможность одновременного их сравнения с увеличением и уменьшением холста изображения.
5) Определять (тестировать) эффективность программных продуктов, реализующих способы, СПИ.

В процессе работы с программой можно:

1) При сокрытии информации задавать параметры позволяющие регулировать пропускную способность стегоконтейнера.
2) Воздействовать серией способов противодействия НСПИ.
3) Перед сокрытием информации, существует возможность задавать количества байт составляющей цвета, которые используются при скрытии информации.

На Рисунке 6 приведен алгоритм программы «AntiStego» вместе с описанием программных модулей, реализующих противодействие НСПИ.

Компрессия стегоконтейнера:

WaveletCompressionUnit - Описание класса реализующего волновое сжатие изображения с целью модификации или уничтожения скрытой информации.

JPEGCompressionUnit - Описание класса, реализующего JPEG-компрессию изображения с целью модификации или уничтожения скрытой информации.

Зашумление стегоконтейнера:

UnifromDistrUnit - Описание класса, реализующего зашумление изображения с равномерным распределением случайной величины с целью модификации или уничтожения скрытой информации.

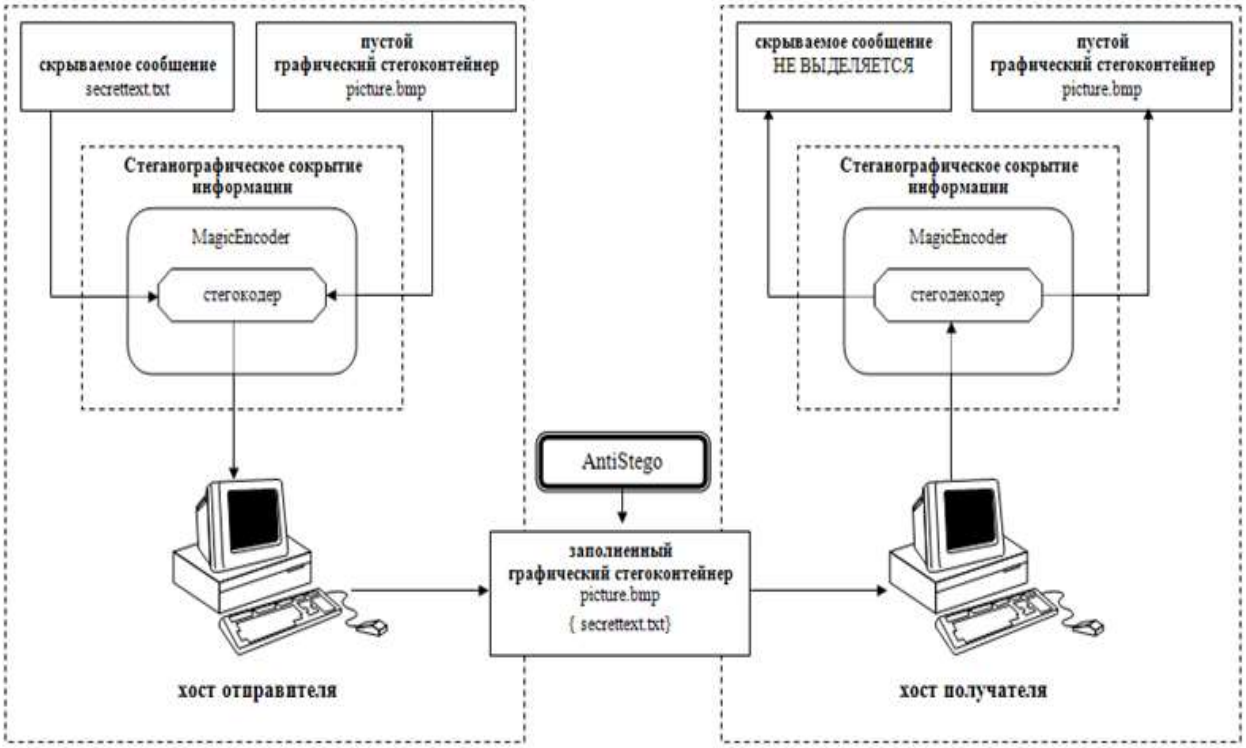

Рисунок 5 - Обобщенная схема проведения эксперимента по противодействию несанкционированной скрытой передачи информации

GaussDistrUnit - Описание класса, реализующего зашумление изображения с нормальным распределением случайной величины с целью модификации или уничтожения скрытой информации.

Аффинные преобразования стегоконтейнера:

ScaleFormUnit - Описание класса реализующего масштабирования изображения с целью модификации или уничтожения скрытой информации

RotateFormUnit - Описание класса реализующего вращение изображения с целью модификации или уничтожения скрытой информации.

MoveFormUnit - Описание класса реализующего смещение изображения с целью модификации или уничтожения скрытой информации.

Фильтрация стегоконтейнеров:

ReccurenceFilterUnit - Описание класса реализующего двумерную рекуррентную фильтрацию изображения с целью модификации или уничтожения скрытой информации.

MedianFilterUnit - Описание класса реализующего медианную фильтрацию изображения с целью модификации или уничтожения скрытой информации.

MaskFilterFormUnit - Описание класса реализующего фильтрацию изображения с произвольной КИХ с целью модификации или уничтожения скрытой информации.

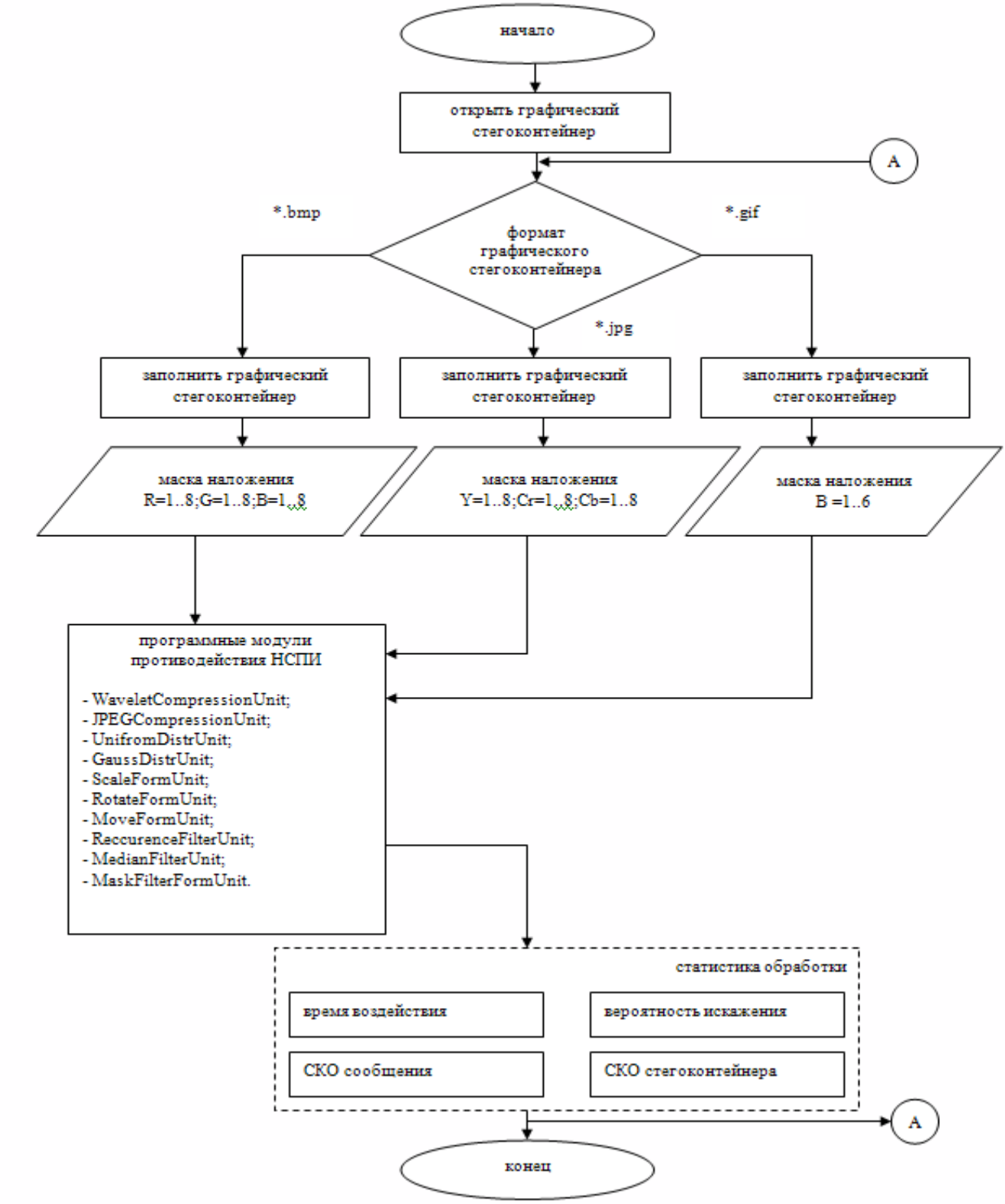

Рисунок 6 - Алгоритм программы «AntiStego»

Выводы

1. Проведен сравнительный анализ методов стеганографического преобразования информации, который показал, что наиболее эффективными являются методы, использующие графические стегоконтейнеры, обладающие следующими преимуществами:
   - обеспечивают пропускную способность до 48% от общего размера стегоконтейнера при достаточно высоком уровне скрытности, тогда как стеганографические методы, использующие аудио стегоконтейнеры - до 23%, а текстовые - до 12%;
   - позволяют заранее учитывать при стеганографическом преобразовании информации априорные сведения о размерах контейнера;
   - учитывают возможности контейнеров, связанных с существованием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации, а также с проработанностью методов цифровой обработки изображений и цифровых форматов представления изображений [14, 15].
2. С учетом результатов анализа состояния, перспектив развития современных методов стеганографии и характеристик существующего программного обеспечения, предназначенного для стеганографического сокрытия данных, разработана описательная модель угроз несанкционированной скрытой передачи информации (НСПИ). Модель угроз включает в себя модель нарушителя, описание каналов передачи и ситуаций, в которых возможна НСПИ с применением методов стеганографического преобразования информации (СПИ), краткую обобщенную характеристику последствий, таких как несанкционированное копирование (хищение) или изменение (уничтожение) данных или программ, нарушению работоспособности компьютерных систем (в том числе нарушение нормальной работоспособности стеганографического программного обеспечения).
3. Успешно проведен эксперимент по предотвращению несанкционированной скрытой передачи информации нарушителем, использующим в качестве средства, реализующего методы стеганографии, программу S-tools. Полное уничтожение скрытой информации происходило в течении 0,2 с.
4. Разработан программный продукт, реализующий рассмотренные в работе способы противодействия НСПИ в компьютерных системах.

ЛИТЕРАТУРА

1. Petitcolas A.P. Information hiding - a survey, Proceedings of the IEEE, special issue on protection of multimedia content/ A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, July 1999.-vol.87(7). - P. 1062-1078.
2. Грибунин В.Г Компьютерная стеганография. / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев, В.Ю. Головачев, А.В. Коняев, - М: Солон-Р, 2002. - 240с.
3. Richard E. Blahut Principles and practice of information theory / E. Richard // Addison-Wesley, Reading, 1987. – pp. 76-90.
4. Gustavus J. Simmons The prisoners' problem and the subliminal channel / J.Gustavus // Advances in Cryptology: Proceedings of Crypto 83 (David Chaum, ed.), Plenum Press, 1984, - pp. 51-67.
5. Pfitzmann B. Information Hiding Terminology / B.Pfitzmann // Information hiding: first international workshop, vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, 1996. - pp. 347-350.
6. Львович И.Я. Применение методологического анализа в исследовании безопасности / И.Я.Львович, А. А. Воронов // Информация и безопасность. 2011. Т. 14. № 3. С. 469-470.
7. Львович И.Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. 2006. Т. 9. № 1. С. 36-39.
8. Грибунин В. Г. Цифровая стеганография. / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // М.: Солон-Пресс, 2009. – 272 с.
9. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ. Монография. – М.: Вузовская книга, 2009. – 220 с.
10. Преображенский Ю. П. Разработка методов формализации задач на основе семантической модели предметной области / Ю. П.Преображенский // Вестник Воронежского института высоких технологий. 2008. № 3. С. 075-077.
11. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
12. Максимов И.Б. Принципы формирования автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. 2014. № 12. С. 130-135.
13. Максимов И. Б. Классификация автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. 2014. № 12. С. 127-129.
14. Мерзлякова Е. Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-

информационных принципах. / Е. Ю.Мерзлякова //Дис. … канд. техн. наук: 05.13.19. – Новосибирск: СибГУТИ, 2011. – 161 с.
15. Слипенчук П. В. Стеганография в кодах, исправляющих ошибки / П. В. Слипенчук // Вестник МГТУ. – 2013. – № 5. – С. 1-12.

A.V. Pitolin, Y.P. Preobrazhensky, O.N. Choporov

A STUDY OF THE POSSIBILITIES OF USING STEGANOGRAPHIC METHODS OF INFORMATION PROTECTION

Voronezh state technical University, Voronezh, Russia

Steganographic methods are used to hide the very fact of the existence of certain messages. The paper analyzes the key concepts that are used in steganographic methods of information transformation. Describes the features of the steganographic methods hide information in graphic files. Developed the threat model unauthorized transfer of information by steganographic methods of information transformation using the graphical containers. The article Presents a classification scheme of threats of unauthorized information transfer using the methods of its steganographic transformation. An experiment was conducted to identify the most effective ways to counteract unauthorized access to information. The author has established that almost all methods of counteraction to unauthorized access on time of influence do not exceed 2 seconds. Highlighted ways to counter at the time of exposure that do not exceed 0.7 seconds. The experiment was conducted among 10 people with the help of the S-tools program and the created AntiStego software. The paper presents the algorithm of the program "AntiStego" together with the description of the software modules implementing counteraction to unauthorized access. A generalized scheme of the experiment for combating the unauthorized covert transfer of information.

Keywords: information security, steganographic approach, unauthorized access.

REFERENCES

1. Gribunin V.G Komp'yuternaya steganografiya. / V.G. Gribunin, I.N. Okov, I.V. Turintsev, V.Yu. Golovachev, A.V. Konyaev, - M: Solon-R, 2002. – 240p.
2. Richard E. Blahut Principles and practice of information theory / E. Richard // Addison-Wesley, Reading, 1987. – pp. 76-90.
3. Gustavus J. Simmons The prisoners' problem and the subliminal channel / J.Gustavus // Advances in Cryptology: Proceedings of Crypto 83 (David Chaum, ed.), Plenum Press, 1984, - pp. 51-67.
4. Pfitzmann B. Information Hiding Terminology / B.Pfitzmann // Information hiding: first international workshop, vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, 1996. - pp. 347-350.
5. L'vovich I.Ya. Primenenie metodologicheskogo analiza v issledovanii bezopasnosti / I.Ya.L'vovich, A. A. Voronov // Informatsiya i bezopasnost'. 2011. Vol. 14. No. 3. pp. 469-470.

6. L'vovich I.Ya. Faktory ugrozy ekonomicheskoy bezopasnosti gosudarstva / I. Ya. L'vovich, A. A. Voronov, Yu. P. Preobrazhenskiy // Informatsiya i bezopasnost'. 2006. Vol. 9. No. 1. pp. 36-39.
7. Gribunin V. G. Tsifrovaya steganografiya. / V. G. Gribunin, I. N. Okov, I. V. Turintsev // M.: Solon-Press, 2009. – 272 p.
8. Agranovskiy A. V., Balakin A. V., Gribunin V. G., Sapozhnikov S. A. Steganografiya, tsifrovye vodyanye znaki i stegoanaliz. Monografiya. – M.: Vuzovskaya kniga, 2009. – 220 p.
9. Preobrazhenskiy Yu. P. Razrabotka metodov formalizatsii zadach na osnove semanticheskoy modeli predmetnoy oblasti / Yu. P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No. 3. pp. 075-077.
10. Konakhovich G. F., Puzyrenko A. Yu. Komp'yuternaya steganografiya. Teoriya i praktika. – K.: MK-Press, 2006. – 288 p.
11. Maksimov I.B. Printsipy formirovaniya avtomatizirovannykh rabochikh mest / I. B. Maksimov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2014. No. 12. pp. 130-135.
12. Maksimov I. B. Klassifikatsiya avtomatizirovannykh rabochikh mest / I. B. Maksimov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2014. No.12. pp. 127-129.
13. Merzlyakova E. Yu. Postroenie steganograficheskikh sistem dlya rastrovykh izobrazheniy, baziruyushchikhsya na teoretiko-informatsionnykh printsipakh. / E. Yu.Merzlyakova //Dis. … kand. tekhn. nauk: 05.13.19. – Novosibirsk: SibGUTI, 2011. – 161 p.
14. Slipenchuk P. V. Steganografiya v kodakh, ispravlyayushchikh oshibki / P. V. Slipenchuk // Vestnik MGTU. – 2013. – No. 5. – pp. 1-12.