УДК681.3

ТЕХНОЛОГИЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ПРИ КОСВЕННОМ СТЕГАНОГРАФИЧЕСКОМ ВСТРАИВАНИИ

ЮДИН А.К., БАРАННИК В.В., ФРОЛОВ О.В.

Рассматривается возможность повышения безопасности информационных ресурсов на основе использования методов компьютерной стеганографии. Проводится сравнительный анализ методов непосредственного и косвенного стеганографического встраивания информации в изображение контейнер. Определяются основные показатели качества функционирования систем косвенного стеганографического встраивания. Проводится сравнительный анализ наиболее распространенных существующих стеганографических методов. Для устранения выявленных недостатков существующих стеганографических систем сформулирован подход, основанный на синтезировании функционала для использования при встраивании структурной избыточности изображения.

Введение

Одним из возможных способов повышения безопасности информационных ресурсов в инфокомунникационных каналах является использование методов компьютерной стеганографии. На сегодняшний день наибольшей популярностью пользуются методы, позволяющие встраивать скрываемую информацию в изображение-контейнер. Данный факт обусловлен широким распространением цифровых изображений различных форматов.

Существующие стеганографические методы встраивания информации в изображение-контейнер включают алгоритмы непосредственного стеганографического встраивания и алгоритмы косвенного стеганографического встраивания. Непосредственное встраивание информации в изображение реализуется путем замены бита контейнера на бит скрываемого сообщения. Алгоритмы, основанные на данном подходе, не обеспечивают в полной мере системных требований относительно стойкости встроенных данных к активным атакам злоумышленника. Это обосновано в первую очередь тем, что методы непосредственного стеганографического встраивания используют визуальную избыточность изображения для скрытия данных. При этом встроенные данные неустойчивы к атакам с пережатием, которые направлены на устранение потенциально опасной психовизуальной избыточности.

В отличие от методов непосредственного встраивания, стеганографическое встраивание бита скрываемого сообщения в косвенных методах осуществляется путем создания зависимости между некоторыми параметрами изображения-контейнера согласно определенному алгоритму. При этом обратное стеганографическое преобразование осуществляется путем изъятия некоторой оценки встроенных данных.

Отсюда предлагается направление для повышения безопасности информационных ресурсов на основе использования методов косвенного стеганографического встраивания.

Анализ существующих методов косвенного стеганографического встраивания

Для успешного сравнительного анализа существующих методов косвенного встраивания рассмотрим стеганографические показатели качества:

1. Относительная стеганографическая емкость $w_{отн}$. Данный показатель используется для оценки эффективности стеганографической системы по удельному объему $w_{встр}$ встраиваемой информации относительно объема $W_{исх}$ изображения-контейнера. Величина $w_{отн}$ относительной стеганографической емкости системы определяется на основе следующей формулы: $w_{отн} = \frac{w_{встр}}{W_{исх}}$.

2. Вероятность $P_{из}$ безошибочного изъятия встроенных данных для авторизированного доступа:

$$P_{из} = \frac{w_{из}}{w_{встр}},$$

где $w_{встр}$ – объем встраиваемой информации, бит; $w_{из}$ – объем безошибочно изъятой информации, бит.

3. Пиковое отношение сигнал-шум h изображения со встроенными данными. Этот показатель характеризует стеганографическую систему с позиции устойчивости к визуальным атакам злоумышленника:

$$h = 20\log_{10}(255/СКО),\ дБ,$$

где $СКО$ – среднеквадратическое отклонение изображения со встроенными данными относительно изображения-контейнера.

4. Вероятность $P_{уст}$ безошибочного изъятия встроенных данных в условиях применения злоумышленником активных атак определяется как отношение объема $w_{встр}$ встроенных данных к объему $w'_{из}$

безошибочно изъятой информации в условиях активных атак:

$$P_{уст} = \frac{w'_{из}}{w_{встр}}$$

и составляет 100%.

5. Пиковое отношение сигнал-шум $h_{авт}$ изображения, полученного в процессе обратного стеганографического преобразования при авторизированном доступе:

$$h_{авт} = 20\log_{10}(255/\sqrt{\sum_{i=1}^{z_{строк}}\sum_{j=1}^{z_{столб}}(a_{i\,j} - a''_{i\,j})^2 / z_{строк}\ z_{столб}})$$

где $a_{i,j}$, $a'_{i,j}$ – элементы соответственно исходного и реконструированного при авторизированном доступе изображений; $z_{строк}\ z_{столб}$ - размер изображения-контейнера.

Методы косвенного стеганографического встраивания условно разделены на две базовые группы, а именно:

1. Методы, для которых требуется прототип изображения-контейнера при стеганографическом изъятии.

2. Методы, для которых не требуется прототипа изображения-контейнера.

Рассмотрим принципы функционирования наиболее распространенных методов, которые используют для косвенного стеганографического изъятия прототип изображения-контейнера.

1. Метод Подильчука. Данный метод предусматривает вычисление порога коэффициента ДКП изображения-контейнера на основе его позиции в матрице. При встраивании анализируются вычисленные пороги. Если значение коэффициента меньше порога, тогда он не изменяется. В противном случае к коэффициенту прибавляется произведение порога и значение элемента скрываемого сообщения. Изъятие встроенной информации осуществляется путем сравнения коэффициентов ДКП стеганограммы и коэффициентов ДКП прототипа исходного изображения-контейнера.

2. Метод Тао. При стеганографическом преобразовании на первом этапе выполняется классификация блоков по шести категориям в зависимости от степени гладкости и наличия контуров. Для каждого блока на основе ключевого правила вычисляются коэффициенты чувствительности к шуму. На следующем этапе блоки упорядочиваются в соответствии с полученными коэффициентами. Энергия встраиваемого элемента определяется этими коэффициентами. Для изъятия встроенных данных выполняется вычитание прототипа изображения-контейнера из принятой стеганограммы и применяются статистические методы проверки гипотез.

3. Алгоритм Кокса. В качестве встраиваемой информации для данного метода используются последовательности вещественных чисел с нулевым средним и единичной дисперсией. Для встраивания применяются несколько АС-коэффициентов ДКП изображения-контейнера с наибольшей энергией. При встраивании осуществляется модификация АС-коэффициентов в соответствии с ключевым правилом встраивания. При изъятии осуществляются обратные операции: определяются коэффициенты ДКП стеганограммы и прототипа изображения-контейнера, находится разность между коэффициентами наибольшей величины.

В отличие от методов, использующих прототип изображения-контейнера при изъятии, методы без учета прототипа обеспечивают изъятие встроенных данных «вслепую». Другими словами, для реализации обратного стеганографического встраивания на основе таких методов не требуется наличие исходного изображения-контейнера.

Среди указанных методов можно выделить следующие:

1. Метод относительной замены величин ДКП (метод Коха и Жао). Одним из наиболее распространенных на сегодня методов. В его алгоритме реализовано разбитие изображения на блоки 8*8 пикселей для применения к каждому из них ДКП. В результате данного преобразования получается матрица 8*8 коэффициентов ДКП. Каждый блок используется для скрытия одного бита данных. Для обеих сторон при организации секретного канала выбираются два конкретных коэффициента ДКП с определенными координатами в массиве коэффициентов. Непосредственно скрытие начинается со случайного выбора блока изображения, предназначенного для кодирования бита данных. Встраивание происходит такой модификацией коэффициентов, чтобы при передаче «0» их разница превышала некоторую положительную величину, а для «1» эта разница делается меньшей по сравнению с некоторой отрицательной величиной. Таким образом, первичное изображение модифицируется за счет внесения изменения в коэффициенты ДКП. После соответствующей коррекции коэффициентов проводится обратное дискретное косинусное преобразование.

2. Метод модификации яркости (метод Куттера-Джордана-Боссена). Встраивание реализуется в канал синего цвета RGB изображения. Цвет был выбран из-за низкой чувствительности человека к его изменению.

Секретный бит M_i встраивается в канал синего цвета путем модификации яркости

$$\lambda_{x,y} = 0.29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0.11448 \cdot B_{x,y}:$$

$$B'_{x,y} = B_{x,y} - \upsilon \cdot \lambda_{x,y} \quad \text{при} \quad m_i = 0$$

и $$B'_{x,y} = B_{x,y} - \upsilon \cdot \lambda_{x,y} \quad \text{при} \quad m_i = 1,$$

где υ - величина, которая определяет энергию встраиваемого сигнала, прямо пропорциональна устойчивости встроенной информации к искажениям.

Для извлечения секретного бита получателю необходимо выполнить предсказание значения первичного не модифицированного пикселя, используя значения соседних пикселей. Авторы метода использовали «крест» пикселей размером 7*7.

3. Метода Бенгама-Мемона-Эо-Юнг. Встраивание осуществляется в спектральные коэффициенты изображения-контейнера путем их модификации. Для этого в спектральной области выбираются три коэффициента ДКП, что позволяет уменьшить визуальные искажения. Для встраивания «0» эти коэффициенты изменяются таким образом, чтобы третий коэффициент стал меньше любого из двух первых. Если необходимо скрыть «1», он делается большим, чем первый и второй коэффициенты. Использование трех коэффициентов ДКП вместо двух уменьшает искажения, которые вносятся в результате встраивания, скрываемого сообщением.

Существующие методы косвенного стеганографического встраивания не обеспечивают в полной мере требований относительно безопасного скрытия данных в изображении. Это обусловлено следующими недостатками:

– низкое значение устойчивости стеганограммы к визуальным атакам злоумышленника. Данный недостаток обусловлен тем, что встраивание скрываемой информации достигается путем модификации элементов представления стеганограммы. Это сопровождается внесением визуальных искажений в изображение и ухудшением его качества. В случае наличия у злоумышленника исходного изображения-контейнера может быть выявлен факт наличия скрытого встраивания в стеганограмме;

– низкая устойчивость встроенных данных к активным атакам злоумышленника. Среди таких атак наиболее распространенными являются компрессионные атаки. Они направлены на устранение психовизуальной избыточности, которая также используется для косвенного стеганографического встраивания информации. Применяя данные атаки, противник способен безвозвратно разрушить встроенное сообщение;

– неудовлетворительное значение стеганографической емкости. Существующие методы встраивания не обеспечивают требуемого объема встраиваемой информации. Данный недостаток обусловлен тем, что увеличение объема встраивания сопровождается увеличением числа модифицированных элементов и как следствие увеличением вносимых искажений в изображение;

– необходимость наличия на приемной стороне прототипа исходного изображения-контейнера для однозначного изъятия встроенной информации.

Существующие недостатки обусловлены тем, что методы используют для косвенного встраивания психовизуальную избыточность изображения.

Основная часть

Для устранения выявленных недостатков косвенного стеганографического встраивания предлагается разработать подход, который позволит использовать для скрытого встраивания структурную избыточность изображения-контейнера. В качестве такого подхода предлагается синтезировать функциональное преобразование $f(\bullet)$ для элементов изображения-контейнера, которое должно обеспечить следующие требования:

1. Функциональное преобразование должно обеспечивать взаимооднозначное кодирование $f(\bullet)$ и декодирование $f^{-1}(\bullet)$ массива A изображения-контейнера при наличии служебной информации Ψ, т.е.

$$C = f(A, \Psi),\ A' = f^{-1}(C, \Psi) \text{ и } A' = A.$$

Здесь A' – массив, восстановленный в результате обратного функционального преобразования $f^{-1}(C)$; Ψ – служебная информация; C – массив, полученный в результате выполнения прямого функционального преобразования.

2. В результате функционального преобразования массива A должна формироваться кодограмма C, которая состоит из двух частей:

– служебной составляющей, содержащей служебные данные Ψ;

– информационной составляющей, содержащей кодовое представление массива A.

3. Значения реконструированных массивов A' и A'' не должны меняться в случае формирования кода при различных значениях служебной информации (Ψ и Ψ'), т.е. $A' = f^{-1}(C, \Psi) = f^{-1}(C', \Psi') = A''$, где A' – массив, реконструированный на основе кода, сформированного с учетом служебных данных Ψ;

A'' – массив, реконструированный на основе кода, сформированного с учетом модифицированных служебных данных Ψ';

C – кодограмма, полученная с учетом служебных данных Ψ;

C' – кодограмма, полученная с учетом служебных данных Ψ'.

Предлагается использовать данное свойство для косвенного стеганографического встраивания.

Тогда процесс встраивания будет включать намеренное изменение служебной информации Ψ на основе ключевого условия. Сформированная кодограмма C', содержащая модифицированные служебные данные Ψ', передается по каналу данных.

При этом на приемной стороне авторизированному пользователю известно условие косвенного встраивания, т.е механизма модификации исходной служебной информации Ψ. В этом случае процесс стеганографического изъятия будет осуществляться путем

анализа значений исходной Ψ и измененной Ψ' служебной информации.

Прямое косвенное стеганографическое преобразование включает следующие этапы:

1. Формирование вектора служебных данных Ψ для массива $A''(2)$ изображения-контейнера.

2. Второй этап предусматривает модификацию вектора служебных данных Ψ с учетом встраиваемого элемента b_ξ на основе ключевого условия: $\Psi' = \Psi + b_\xi$. Здесь b_ξ – элемент скрываемого сообщения $B = \{b_1;...;b_\xi;...;b_\nu\}$, $\xi = \overline{1, \nu}$.

3. Функциональное преобразование массива A с учетом модифицированного вектора служебных данных Ψ' по правилу $f(A)$, т.е. $C = f(A, \Psi')$, где C – сформированное значение кодограммы.

Полученная кодограмма, содержащая в себе информационную составляющую C и служебную составляющую Ψ', передается в канал передачи данных, где может подвергаться атакующим воздействиям.

Обратное косвенное стеганографическое преобразование осуществляется по биполярному принципу для авторизированного и неавторизированного пользователя.

При неавторизированном доступе по правилу $f^{(-1)}(\bullet)$ осуществляется реконструкция исходного массива изображения-контейнера: $A'' = f^{(-1)}(C; \Psi')$.

Здесь A'' – массив исходного изображения, полученный в результате неавторизированного доступа.

Наоборот, обратное косвенное стеганографическое преобразование для авторизованного пользователя осуществляется с учетом ключевого условия изъятия и содержит следующие этапы:

1. На первом этапе по правилу $f^{(-1)}(\bullet)$ реконструируется массив A' исходного изображения контейнера: $A' = f^{(-1)}(C; \Psi')$.

Здесь C – принятая кодограмма, сформированная на передающей стороне с учетом модифицированных служебных данных Ψ'.

2. На втором этапе для реконструированного массива A' по ключевому правилу осуществляется формирование исходного вектора служебных данных Ψ.

3. Третий этап включает косвенное изъятие встроенного элемента b'_ξ скрываемого сообщения $B' = \{b'_1;...;b'_\xi;...;b'_\nu\}$ на основе ключевого условия изъятия при анализе восстановленного Ψ и полученного Ψ' векторов служебных данных: $b'_\xi = \Psi' - \Psi$.

Выводы

Рассмотрена возможность повышения безопасности информационных ресурсов в инфокоммуникационных системах на основе использования методов косвенного стеганографического встраивания.

Приведены основные показатели качества функционирования систем косвенного стеганографического встраивания. Проведен сравнительный анализ наиболее распространенных косвенных стеганографических методов. Определены основные недостатки функционирования таких систем.

Для устранения выявленных недостатков предложен подход, основанный на использовании при косвенном стеганографическом встраивании структурной избыточности представления изображения-контейнера.

Сформулированы требования к синтезированному функционалу. Представлена схема косвенного стеганографического преобразования на основе использования синтезированного функционального преобразования.

Литература: 1. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганографияю М.: Солон-Пресс, 2002. 272 с. **2.** *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288с. **3.** *Тарасов Д.О., Мельник А.С., Голобородько М.М.* Класифікація та аналіз безкоштовних програмних засобів стеганографії // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка". 2010. № 673. С. 365-374. **4.** *Защита* от компьютерного терроризма / А. В. Соколов, О. М. Степанюк // Справочное пособие. БВХ-Петрбург: Арлит. 2002. 496 с. **5.** *Жилкин М.Ю.* Стегоанализ графических данных в различных форматах / М.Ю. Жилкин // Доклады ТУСУРа, 2008. №2 (18). Ч. 1. С.63-64. **6.** *Задирака В.К.* Новые подходы к разработке алгоритмов скрытия информации / В.К. Задирака, Л.Л. Никитенко // Штучный інтелект. 2008. №4. С.353-357. **7.** *Михайличенко О.В.* Применение стеганографических методов сокрытия информации в неподвижных изображениях / О.В. Михайличенко, А.Г. Коробейникова, С.Ю. Каменева // Труды международных научно-технических конференций «Интеллектуальные системы (IEEE AIS'06) и «Интеллектуальные САПР (CAD-2006)». М.: Физмалит, 2006. Т.2. С.511-515.

Поступила в редколегию 17.01.2016

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры автоматизированных систем управления, Харьковский университет Воздушных Сил им. И. Кожедуба. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79. E-mail: barannik_v_v@mail.ru.

Юдин Александр Константинович, д-р техн. наук, профессор, директор института компьютерных информационных технологий Национального авиационного университета. Адрес: Украина, 01000, Киев, пр.Космонавта Комарова, 1.

Фролов Олег Владимирович, соискатель Национального авиационного университета. Адрес: Украина, 01000, Киев, пр.Космонавта Комарова, 1.